

ДОГОВОР

№ КС-129 /19.11.2018 г.

Днес, 19.11.2018 г. в гр. София, между:

1. **АДМИНИСТРАЦИЯТА НА МИНИСТЕРСКИЯ СЪВЕТ** с адрес в гр. София, пощенски код 1594, бул. „Княз Ал. Дондуков“ № 1, БУЛСТАТ 000695025, представлявана от г-н Веселин Чингов, директор на дирекция „Административно и правно обслужване и управление на собствеността“ – упълномощено лице по чл. 7, ал. 1 от Закона за обществените поръчки със Заповед № В-17 от 23.01.2018 г. на министър-председателя и Румяна Славчева Петрова – директор на дирекция „Бюджет и финанси“ в дирекция „Бюджет и финанси“, наричани по-нататък в договора **ВЪЗЛОЖИТЕЛ**, от една страна,

2. **„ДАВИД ХОЛДИНГ“ АД**, с адрес за кореспонденция: гр. Казанлък 6100, ул. „Стара река“ № 2, ДК „Арсенал“, офис 417, тел.: +359 2 4901600, факс: +359 431 62253, ел. адрес: snedev@david.bg, ЕИК:833092882, представлявано от Бальо Динев - изпълнителен директор, наричан по-долу **ИЗПЪЛНИТЕЛ**, от друга страна,

на основание чл. 194, ал. 1 от ЗОП и одобрен Протокол от 18.10.2018 г. на комисия, назначена със Заповед № ФС-104/16.10.2018 г. за получаването, разглеждането и оценката на офертите, . получени след публикуване на обява № 9081440/02.10.2018 г. за обществена поръчка с предмет: „Анализ и отстраняване на констатираните несъответствия в публичния модул и вътрешната среда на ИСУН за програмния период 2007-2013“, се сключи настоящият договор за следното:

I. ПРЕДМЕТ НА ДОГОВОРА

Чл. 1. **ВЪЗЛОЖИТЕЛЯТ** възлага, а **ИЗПЪЛНИТЕЛЯТ** приема да изпълни срещу заплащане дейностите, предмет на обществената поръчка с предмет: „Анализ и отстраняване на констатираните несъответствия в публичния модул и вътрешната среда на ИСУН за програмния период 2007-2013“. Проектът се финансира чрез Бюджетна линия № BG05SFOP001-4.002-0003-C01 „Повишаване на ефективността и ефикасността на Централното координационно звено“ по Оперативна програма „Добро управление“.

Конкретните дейности, предмет на договора са посочени в Техническата спецификация, Техническото предложение и Ценовото предложение на Изпълнителя, представляващи Приложения № 1, № 2 и № 3, неразделна част от договора.

II. ЦЕНА И НАЧИН НА ПЛАЩАНЕ

Чл. 2. (1) Общата цена на договора е 69690,00 (шестдесет и девет шестотин и деветдесет) лева без ДДС и 83 628,00 (осемдесет и три шестотин двадесет и осем) лева с включен ДДС, съгласно Ценовото предложение на ИЗПЪЛНИТЕЛЯ, Приложение № 3, неразделна част от настоящия договор.

Цената включва всички разходи по изпълнение на дейностите и постигане на резултатите по предмета на поръчката, съгласно чл. 1 от настоящия договор.

(2) Плащането се извършва след представяне на двустранно подписан приемо-предавателен протокол за приемане без забележки на изпълнението на всички дейности по чл. 1 и представяне на фактура от ИЗПЪЛНИТЕЛЯ.

За ВЪЗЛОЖИТЕЛЯ приемо-предавателния протокол и фактурата се подписват от отговорните лица по чл. 11 от договора.

(3) Плащанията по чл. 2 ще се извършват по банков път в срок не повече от 30 дни, след представянето на съответните документи по чл. 2, ал. 2 от договора по сметката на ИЗПЪЛНИТЕЛЯ както следва:

Банка: **Обединена българска банка**

BIC: **UBBSBGSF**

IBAN: **BG04UBBS88881000756115**

(4) ИЗПЪЛНИТЕЛЯТ е длъжен да уведомява писмено ВЪЗЛОЖИТЕЛЯ за всички последващи промени по чл. 2, ал. 3 в срок от 3 календарни дни, считано от момента на промяната. В случай, че ИЗПЪЛНИТЕЛЯТ не уведоми ВЪЗЛОЖИТЕЛЯ в този срок, счита се, че плащанията са надлежно извършени.

(5) Договорената цена е окончателна и не подлежи на актуализация за срока на настоящия договор, освен при наличие на основанията, предвидени в чл. 116 от Закона за обществените поръчки.

(6) Когато ИЗПЪЛНИТЕЛЯТ е сключил договор/договори за подизпълнение, ВЪЗЛОЖИТЕЛЯТ извършва окончателно плащане към него, след като бъдат представени доказателства, че ИЗПЪЛНИТЕЛЯТ е заплатил на подизпълнителя/подизпълнителите за изпълнените от тях работи, които са приети по реда на настоящия договор.

III. ПРАВА И ЗАДЪЛЖЕНИЯ НА ИЗПЪЛНИТЕЛЯ

Чл. 3. ИЗПЪЛНИТЕЛЯТ има право:

1. Да иска от ВЪЗЛОЖИТЕЛЯ приемане на изпълнената услуга при условията и сроковете, определени в настоящия договор.

2. Да получи уговореното възнаграждение за изпълнената услуга в размера и по реда, определени в настоящия договор.

Чл. 4. ИЗПЪЛНИТЕЛЯТ се задължава:

1. Да изпълни задълженията си по договора точно (в количествено, качествено и времево отношение), в съответствие с Техническата спецификация и Техническото си предложение да упражнява всичките си права, с оглед защита интересите на ВЪЗЛОЖИТЕЛЯ.

2. При изпълнение на дейностите на настоящата поръчка ИЗПЪЛНИТЕЛЯТ съвместно с ВЪЗЛОЖИТЕЛЯ да изготви план за изпълнение на услугата, който включва описание на конкретната задача, модул, срок за изпълнение, други изисквания, ако е приложимо, съобразно сложността на всяка задача и важност от гледна точка функционирането на системата.

3. Да представи отчет към ВЪЗЛОЖИТЕЛЯ за броя и обхвата на предоставените услуги.

4. При извършване на посочените услуги да се съобразява с процедурата за управление на промените и процедурата за управление на внедряването с цел запазване на наличността на предоставяната от ИСУН услуга и запазване на цялостност и консистентност на данните в нея;

5. При извършване на посочените услуги да се съобразява с изискванията поставени от стандарта за информационна сигурност ISO 27000 и политиката, и процедурите за информационна сигурност въведени и използвани при работа с ИСУН, налични на адрес <http://www.eufunds.bg>.

6. Да изпълнява указанията и изискванията на ВЪЗЛОЖИТЕЛЯ, изразени при съгласуване, одобряване и приемане изпълнението на отделните дейности по договора, да отстранява недостатъци и пропуски и да внася исканите поправки, съответно – да извършва преработка за своя сметка, в срок, определен от ВЪЗЛОЖИТЕЛЯ.

7. Да уведомява писмено ВЪЗЛОЖИТЕЛЯ за всички възникнали трудности при изпълнение на дейностите по договора, които могат да осуетят постигането на крайните резултати, както и за мерките които са взети за отстраняването им.

8. Да не използва по никакъв начин, включително за свои нужди или като я разгласява пред трети лица, каквато и да било информация, станала му известна при или по повод изпълнението на този договор, която ВЪЗЛОЖИТЕЛЯТ няма интерес да бъде разкривана. ИЗПЪЛНИТЕЛЯТ поема задължение да осигури тези действия от всяко лице от екипа си.

9. ИЗПЪЛНИТЕЛЯТ се задължава да предприеме всички необходими мерки за избягване на конфликт на интереси, както и да уведоми незабавно ВЪЗЛОЖИТЕЛЯ относно обстоятелство, което предизвиква или може да предизвика подобен конфликт.

10. Да уведомява ВЪЗЛОЖИТЕЛЯ за всяка промяна в седалището, адреса на управление, банковата сметка и правноорганизационната му форма – преобразуване при условията на чл. 116, ал.1, т.4, б. „б“ или промяна на съдружници в неперсонифицирано дружество, в 3-дневен срок от настъпване на съответното обстоятелство. В случай на правопримство да представи документи от съответните компетентни органи за удостоверяване липсата на обстоятелствата по чл.54 от ЗОП и за доказване на съответствието си с критериите за подбор.

11. Да отстранява за своя сметка допуснатите недостатъци и грешки в процеса на изпълнението на поръчката.

IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА ВЪЗЛОЖИТЕЛЯ

Чл. 5. ВЪЗЛОЖИТЕЛЯТ има право:

1. Да иска от ИЗПЪЛНИТЕЛЯ да изпълни възложените дейности по чл. 1 от настоящия договор в уговорените срокове, без недостатъци и отклонение от уговореното в условията на настоящия договор, Техническата спецификация и Техническото предложение.

2. Да изисква и получава информация за хода на изпълнението на този договор, както и да осъществява текущ контрол.

3. Да дава указания на ИЗПЪЛНИТЕЛЯ, чрез определените лица, които са задължителни за него, по повод изпълнението на възложените дейности и да изисква тяхното доработване и др. в случаите, когато същите са непълни, не съответстват на изискванията му и не са постигнати резултатите за проследяване на изпълнението, съгласно Техническата спецификация.

4. Да задържи съответна част от гаранцията за изпълнение при неизпълнение от страна на ИЗПЪЛНИТЕЛЯ на клаузи на договора и да получи неустойка в размера, определен в раздел X „Неустойки“ от настоящия договор.

5. Да изиска от ИЗПЪЛНИТЕЛЯ да сключи и да му предостави договори за подизпълнение с посочените в офертата му подизпълнители.

Чл. 6. ВЪЗЛОЖИТЕЛЯТ има право да не приеме извършените дейности по чл. 1 от договора, или на част от тях, ако те не съответстват по обем и качество на неговите изисквания и не могат да бъдат коригирани в съответствие с указанията му и действащите правила.

Чл. 7. ВЪЗЛОЖИТЕЛЯТ е длъжен:

1. Да заплати договорената цена в размера и по реда на настоящия договор.
2. Да осигури на ИЗПЪЛНИТЕЛЯ достъп до известната му информация и документация, необходима за изпълнение на услугата.

3. Да не разпространява под каквато и да е форма всяка предоставена му от ИЗПЪЛНИТЕЛЯ информация, имаща характер на търговска тайна, и изрично писмено упомената от ИЗПЪЛНИТЕЛЯ като такава.

4. Да оказва съдействие на ИЗПЪЛНИТЕЛЯ в случай на необходимост.

V. ГАРАНЦИИ ЗА ИЗПЪЛНЕНИЕ

Чл. 8. (1) Преди подписване на договора ИЗПЪЛНИТЕЛЯТ представя гаранция за изпълнение в размер на 5 % (пет процента) от общата стойност на договора по чл. 2, ал. 1 без ДДС, а именно – 3 484,50 лв. (три хиляди четиристотин осемдесет и четири и 0,50) лв.

(2) Гаранцията за изпълнение на договора се представя от ИЗПЪЛНИТЕЛЯ под формата на парична сума/банкова гаранция/застраховка, която обезпечава изпълнението чрез покритие на отговорността на ИЗПЪЛНИТЕЛЯ.

(3) Когато ИЗПЪЛНИТЕЛЯТ е представил гаранция за изпълнение под формата на банкова гаранция, тя трябва да е безусловна, неотменяема, в нея да е записан предмета на договора и да е със срок на валидност минимум 60 календарни дни, след крайния срок на договора. ИЗПЪЛНИТЕЛЯТ предварително съгласува текста на гаранцията на изпълнение, а оригиналът на гаранцията за изпълнение е неразделна част от договора – Приложение № 4.

(4) Когато ИЗПЪЛНИТЕЛЯТ е представил гаранция за изпълнение под формата на застраховка, която обезпечава изпълнението чрез покритие на отговорността на изпълнителя, ВЪЗЛОЖИТЕЛЯТ следва да бъде посочен като трето ползващо се лице по тази застраховка. Застраховката не може да бъде използвана за обезпечение на отговорността на ИЗПЪЛНИТЕЛЯ по друг договор. Текстът на застраховката се съгласува с ВЪЗЛОЖИТЕЛЯ. Застраховката следва да е със срок на валидност минимум 60 календарни дни, след крайния срок на договора;

(5) ВЪЗЛОЖИТЕЛЯТ освобождава гаранцията за изпълнение, без да дължи лихви за периода, през който средствата са престояли законно при него до 30 дни след приемане на изпълнението с подписване на приемателно-предавателен протокол по чл. 2, ал. 2 от договора.

(6) Гаранцията за изпълнение се усвоява от ВЪЗЛОЖИТЕЛЯ, ако договорът бъде прекратен по вина ИЗПЪЛНИТЕЛЯ, както и при частично, забавено или некачествено изпълнение, констатирано по съответния ред.

(7) Гаранцията за изпълнение се задържа от ВЪЗЛОЖИТЕЛЯ, ако в процеса на неговото изпълнение възникне спор между страните, който е внесен за решаване от компетентен съд – до решаване на спора.

(8) ВЪЗЛОЖИТЕЛЯТ има право да усвоява суми по гаранцията за изпълнение при дължими неустойки от страна на ИЗПЪЛНИТЕЛЯ по договора.

(9) В случай на предстоящо изтичане на срока на валидност на учредената банкова гаранция, респ. застраховка ИЗПЪЛНИТЕЛЯТ се задължава да удължи срока на валидност, като в противен случай, ВЪЗЛОЖИТЕЛЯТ има право да усвои сумата по гаранцията при себе си, преди изтичането на валидността ѝ.

VI. УСЛОВИЯ И СРОКОВЕ ЗА ИЗПЪЛНЕНИЕ НА ДОГОВОРА

Чл. 9. Срокът за изпълнение е до 14.12.2018 г.

Чл. 10. Място на изпълнение на поръчката: гр. София, бул. „Дондуков“ № 1.

VII. ОТЧЕТНОСТ И ПРИЕМАНЕ НА ВЪЗЛОЖЕНАТА РАБОТА

Чл. 11. Възложителят и Изпълнителят се съгласяват да определят оторизирани лица по договора, както следва:

а) **ИЗПЪЛНИТЕЛЯТ** оторизира:

Стойчо Недев – Технически директор, e-mail: sn@david.bg, тел.: 490 1600

б) **ВЪЗЛОЖИТЕЛЯТ** определя за оторизирани лица, отговорни за приемането работата по чл. 1 на договора, а именно:

Георги Стратиев, началник отдел „Информационни системи“, тел: 940 3122, g.stratiev@government.bg

в) Промяната на оторизираните лица по тази точка се извършва с писмено уведомление.

Чл. 12. Всички подлежащи на одобрение от страна на Възложителя документи, свързани с изпълнението на договора, се предоставят на ВЪЗЛОЖИТЕЛЯ на хартиен носител (оригинал и копие) на български език.

VIII. СЧЕТОВОДНА ОТЧЕТНОСТ

Чл. 13. ИЗПЪЛНИТЕЛЯТ е длъжен да води точна и редовна документация и счетоводна отчетност, отразяващи изпълнението на договора, използвайки подходяща система за регистрация на документацията. Счетоводните отчети и разходите, свързани с изпълнението на договора, трябва да са в съответствие с изискванията на законодателството и да подлежат на ясно идентифициране и проверка.

Чл. 14. ИЗПЪЛНИТЕЛЯТ е длъжен при поискване от ВЪЗЛОЖИТЕЛЯ да му предоставя достъп до финансовата документация и до документацията, касаеща изпълнението на договора, както и достъп до помещенията на ИЗПЪЛНИТЕЛЯ, в които последната се съхранява. Задължение по предходното изречение ИЗПЪЛНИТЕЛЯТ има и при поискване на проверки от страна на компетентните органи.

IX. ПОВЕРИТЕЛНА ИНФОРМАЦИЯ

Чл. 15. (1) Всички данни, сведения, факти и обстоятелства, свързани със сключването и изпълнението на този договор ще се третира от страните като конфиденциална информация.

(2) Страните се задължават да пазят в тайна, да не разпространяват на трети лица и да опазват от неоторизиран достъп информацията, станала им известна при или по повод изпълнението на задълженията им по настоящия договор, включително и след прекратяването на същия.

(3) Всяка от страните се задължава да информира другата при нарушаване на изискванията за опазване на поверителност на информацията по този договор.

(4) В случай на прекратяване на договора, всяка от страните определя предоставената информация, която другата страна трябва да унищожи. Унищожаването на носителите на информация се извършва по начин, който да не позволява нейното възстановяване. Това се отнася и за информацията, предоставена на електронен носител.

(5) В случай на необходимост от предоставяне на трети лица на поверителна информация, е необходимо изричното и писмено съгласие на другата страна по договора за всеки отделен случай.

X. НЕУСТОЙКИ

Чл. 16. (1) При забава на плащане ВЪЗЛОЖИТЕЛЯТ дължи неустойка на ИЗПЪЛНИТЕЛЯ в размер на 0,5 % от стойността на забавеното плащане за всеки просрочен ден, но не повече от 10 % от тази сума.

(2) При забавено изпълнение на задълженията по договора от страна на ИЗПЪЛНИТЕЛЯ същият заплаща на ВЪЗЛОЖИТЕЛЯ неустойка в размер на 0,5 % от стойността на забавеното изпълнение за всеки просрочен ден, но не повече от 10 % от тази сума.

(3) За некачествено изпълнение или неточно изпълнение на задължения по договора неизправната страна дължи на изправната неустойка в размер на 15 (петнадесет) на сто от цената по договора. Страната, която е понесла вреди от неизпълнението може да търси обезщетение и за по-големи вреди.

(4) ВЪЗЛОЖИТЕЛЯТ може да претендира за нанесени вреди и пропуснати ползи по общия ред, в случай че превишават размера на предвидените неустойки.

XI. ПРЕКРАТЯВАНЕ НА ДОГОВОРА

Чл. 17. Настоящият договор се прекратява:

17.1. С изтичане на срока по чл. 9.

17.2. По взаимно съгласие между страните, изразено в писмена форма

17.3. При виновно неизпълнение на задълженията на една от страните по договора – с 10-дневно писмено предизвестие от изправната до неизправната страна;

17.4. При констатирани нередности и/или конфликт на интереси - с изпращане на едностранно писмено предизвестие от ВЪЗЛОЖИТЕЛЯ до ИЗПЪЛНИТЕЛЯ;

17.5. С окончателното му изпълнение;

17.6. По реда на чл. 118 от Закона за обществените поръчки;

17.7. При преобразуване на ИЗПЪЛНИТЕЛЯ или промяна на съдружниците в неперсонифицирано дружество, ако правопреемникът не отговаря на условията по чл. 116, ал.1, т.4, б. „б“, подбукви „аа“ и „бб“ от ЗОП, договорът се прекратява по право, като ИЗПЪЛНИТЕЛЯТ, съответно правопреемникът дължи обезщетение по общия исков ред.

17.8. Когато са настъпили съществени промени във финансирането на обществената поръчка – предмет на договора, извън правомощията на ВЪЗЛОЖИТЕЛЯ, които той не е могъл или не е бил длъжен да предвиди или да предотврати - с писмено уведомление, веднага след настъпване на обстоятелствата.

17.9. ВЪЗЛОЖИТЕЛЯТ може да прекрати договора без предизвестие, когато ИЗПЪЛНИТЕЛЯТ:

17.9.1. забави изпълнението на някое от задълженията си по договора с повече от 30 работни дни;

17.9.2. не отстрани в разумен срок, определен от ВЪЗЛОЖИТЕЛЯ, констатирани недостатъци;

17.9.3. не изпълни точно някое от задълженията си по договора;

17.9.4. използва подизпълнител, без да е декларирал това в офертата си, или използва подизпълнител, който е различен от този, посочен в офертата му;

17.9.5. бъде обявен в несъстоятелност или когато е в производство по несъстоятелност или ликвидация.

XII. НЕПРЕОДОЛИМА СИЛА

Чл. 18. (1) Страните се освобождават от отговорност за неизпълнение на задълженията си, когато невъзможността за изпълнение се дължи на непреодолима сила. Никоя от страните не може да се позовава на непреодолима сила, ако е била в забава и не е информирала другата страна за възникването на непреодолима сила.

(2) Страната, засегната от непреодолима сила, е длъжна да предприеме всички разумни усилия и мерки, за да намали до минимум понесените вреди и загуби, както и да уведоми писмено другата страна незабавно при настъпване на непреодолимата сила.

(3) Докато трае непреодолимата сила, изпълнението на задължението се спира.

(4) Не може да се позовава на непреодолима сила онази страна, чиято небрежност или умишлени действия или бездействия са довели до невъзможност за изпълнение на договора.

(5) Липсата на парични средства не представлява непреодолима сила.

XIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл.19. Изменение на сключен договор за обществена поръчка се допуска по изключение, при условията на чл. 116 от Закона за обществените поръчки.

Чл. 20. Всички съобщения, предизвестия и нареждания, свързани с изпълнението на този договор и разменяни между ВЪЗЛОЖИТЕЛЯ и ИЗПЪЛНИТЕЛЯ, са валидни, когато са изпратени по пощата (с обратна разписка), по факс, електронна поща или предадени чрез куриер срещу подпис на приемащата страна.

Чл.21. Когато някоя от страните е променила адреса си, без да уведоми за новия си адрес другата страна, съобщенията ще се считат за надлежно връчени и когато са изпратени на стария адрес.

Чл. 22. Всички спорове по този договор ще се уреждат чрез преговори между страните, а при непостигане на съгласие – ще се отнасят за решаване от компетентния съд в Република България.

Чл. 23. За всички неуредени в този договор въпроси се прилагат разпоредбите на действащото законодателство.

Чл. 24. Нито една от страните няма право да прехвърля правата и задълженията, произтичащи от този договор.

Настоящият договор се състави и подписа в два еднообразни екземпляра на български език, един за ИЗПЪЛНИТЕЛЯ и два за ВЪЗЛОЖИТЕЛЯ.

Неразделна част от този договор са:

1. Техническа спецификация на Възложителя (Приложение №1)
2. Техническо предложение (Приложение №2)
3. Ценово предложение (Приложение №3).
4. Гаранция за изпълнение (Приложение № 4)

ВЪЗЛОЖИТЕЛ:

ВЕСЕЛИН ЧИНОВ
ДИРЕКТОР НА ДИРЕКЦИЯ АПОУС

упълномощено лице по чл.7, ал.1 от Закона за обществените поръчки със Заповед № В-17 от 23.01.2018 г. на министър-председателя

.....
чл.2 33ЛД

РУМЯНА ПЕТРОВА
ДИРЕКТОР НА ДИРЕКЦИЯ
„БЮДЖЕТ И ФИНАНСИ“

.....
чл.2 33ЛД

ИЗПЪЛНИТЕЛ:

„ДАВИД Холдинг“ АД

БАЛЪО ДИНЕВ
Изпълнителен директор

.....
чл.2 33ЛД



ЕВРОПЕЙСКИ СЪЮЗ



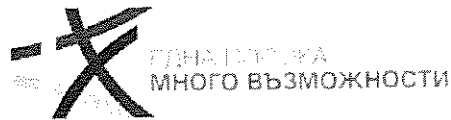
НАУКА
И ОБРАЗОВАНИЕ
МНОГО ВЪЗМОЖНОСТИ

МИНИСТЕРСКИ СЪВЕТ

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

**Анализ и отстраняване на констатираните несъответствия в публичния модул и
вътрешната среда на ИСУН за програмния период 2007-2013**

2018 г.



ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ

I. Въведение и текущо състояние

1. Цел на документа

Документът описва актуалното състояние на информационната система за управление и наблюдение (ИСУН) на Структурните фондове и Кохезионния фонд (СКФ) за програмен период 2007-2013 г., изискванията за изпълнението на поръчката и услугите, които ще бъдат изпълнявани след подписване на договор с изпълнител.

2. Описание на текущото състояние

С цел осигуряването на ефективност и ефикасност при управлението и контрола на средствата от Структурните инструменти на Европейския съюз (ЕС) през програмен период 2007-2013 г. в България се използваше единна информационна система за управление на всички оперативни програми - ИСУН. Системата позволява събиране, записване и съхранение в електронна форма на определени данни от проектно ниво до ниво оперативна програма. Тези данни са необходими за целите на мониторинга, оценката, финансовото управление, проверката и одита на оперативните програми.

Потребители на ИСУН са всички административни структури, участващи в управлението и реализацията на дейностите, финансирани от Структурните инструменти на ЕС в България – Централно координационно звено (ЦКЗ), Одитен орган (ОО), Сертифициращ орган (СО), Управляващи органи на оперативните програми (УО на ОП) и техните Междинни звена (МЗ), кандидати и бенефициенти по оперативните програми и широката общественост чрез осигуряването на свободен достъп до публичния модул на адрес: <https://umispublic.government.bg/> и достъп до модула за електронни услуги на адрес: <https://eumis.government.bg/>.

Основните процеси по кандидатстване за финансиране, отчитане на извършените разходи, верификация и сертификация на плащанията през периода 2007-2013 г. бяха осъществени чрез извършване на действия в системата. Системата осигурява записване и съхранение в компютъризирана форма, както на информацията и данните за проектите и програмите, така и на действията във връзка с управлението им. Тя е основен инструмент за ефективно управление, наблюдение, отчитане и проверки на оперативните програми, както и за обмен на информация с органите на ЕК. Системата гарантира проследимост и прозрачност на управлението на фондовете. В същото време представлява важен инструмент за подобряване на системите за управление и контрол, намаляване на административната тежест за бенефициентите и подобряване на ефикасността на звената, отговорни за управление на средствата от ЕС.

С приключването на програмен период 2007-2013 г. и напредъка в изпълнението на програмите от периода 2014-2020 г. значението на определени модули и



ЕВРОПЕЙСКИ СЪЮЗ



МНОГО ВЪЗМОЖНОСТИ

функционалности на ИСУН, пряко свързани с процесите на кандидатстване, оценка, отчитане и в голяма степен с контрол на проектите, намалява, докато същевременно други елементи и възможности на системата придобиват нарастващо значение. Това са модул „Наблюдение“ и модулът за публична информация на системата, които се използват все по-активно, както от преките потребители, участващи в управлението и реализацията на дейностите, финансирани от Структурните инструменти, така и от широката общественост.

Целта на ИСУН да осигурява ефективност и ефикасност при управлението и контрола на средствата от ЕС към настоящия момент, в който приключва изпълнението на оперативните програми от периода 2007-2013 г., отстъпва на другата основна цел на системата - да осигурява проследимост, публичност и прозрачност на финансираните от ЕС проекти. Дейностите за информиране и публичност, от една страна, представляват нормативно установено задължение на държавите-членки на ЕС, което те трябва да прилагат по отношение на потенциалните бенефициенти, бенефициентите и широката общественост. За изпълнението на това задължение се предприемат множество разнообразни информационни, медийни, рекламно-информационни и комуникационни дейности, насочени към различни целеви групи чрез разнородни комуникационни средства и канали. В допълнение, все по-важно става гражданите и обществото да бъдат информирани и да разпознават финансовия принос на фондовете на ЕС на национално и местно равнище, както и да бъдат осведомени за добавена стойност на предоставената безвъзмездна помощ. В този контекст на разнообразни цели, послания и информационни потоци от изключително значение е да бъде осигурено наличието на един публичен, независим и надежден източник на информация, свободен достъп до който имат всички заинтересовани лица.

ИСУН има водеща роля при изпълнението на целите за публичност и прозрачност на управлението на фондовете от ЕС чрез информацията, която предоставя публичният модул. Поради тази причина е необходимо да бъде осигурена коректна, надеждна и лесно достъпна информация за периода 2007-2013 г. в публичния модул на системата.

Едно от основните предимства на ИСУН е възможността да обработва и обобщава наличните в системата данни, чрез което може да бъде генерирана различна статистическа и друга информация, необходима за вземане на информирани решения, за аналитични и други управленски цели. С напредъка на втория за България програмен период интересът се насочва към постигнатите резултати, реализираните ползи и степента на усвояване на предоставените от ЕС средства. Подобна информация може да бъде генерирана само на базата на наличието на структурирани и надеждни масиви от данни, които са проверени от отговорните за това административни структури. Необходимостта от различни справки по отношение на бенефициентите, крайните ползватели, резултатите и начинът на използване на публичните финансови ресурси от СКФ, е свързана с принципите за прозрачност и публичност, но също така и с осигуряването на надеждни аналитични и статистически данни за целите на предстоящото програмиране и планиране.

За изпълнение на гореописаните цели е необходимо да бъде осигурено наличието на коректни, информативни и лесно достъпни справки за периода 2007-2013 г. в съответния модул на ИСУН.

3. Основни потребители на ИСУН

Макар и с намаляваща интензивност, ИСУН се използва от всички участници в процеса по изпълнение, управление, наблюдение и контрол на средствата от ЕС. С оглед на техните нужди и права за достъп могат да се дефинират 3 основни групи потребители:

- *Вътрешни потребители* – това са служители на административни структури. Въз основа на основните им функции посочената група може да бъде разделена на 2 основни подгрупи потребители:
 - потребители, участващи в управлението и контрола на проекти, финансирани от Структурните инструменти на ЕС в България – УО, СО, ОО. Посочените потребители получават достъп до системата чрез потребителско име и парола, като тези профили се управляват от съответната структура и се контролират от дирекция „Централно координационно звено“ (ЦКЗ) в администрацията на Министерския съвет. Тази категория потребители въвеждат и управляват информация в системата, управляват достъпа до нея в рамките на дадените им правомощия, ползват я за нуждите на техните проверки. Те също така са длъжни да спазват правилата за информационна сигурност, да въвеждат актуална и достоверна информация, както и да проверяват въведената такава от кандидатите и бенефициентите;
 - Потребители от ЦКЗ – тази категория потребители има достъп до цялата система, включително за приложно администриране. Посочените потребители реално не въвеждат информация в ИСУН, но използват въведените данни, като на тази база се подготвят различни анализи и справки. Посочената група потребители са отговорни за правилното въвеждане на информацията в системата, а също така и за управлението на администраторските профили в останалите структури. С оглед изпълнението на посочените функции, основно се използва справочна информация от системата, логове, следене за спазване на сроковете и пълнотата на информацията в ИСУН.
- *Кандидати и бенефициенти* – посочените потребители получават достъп чрез електронен подпис. Тази категория потребители има задължение и отговорност да въвежда своевременно и пълно информацията в рамките на своите правомощия и съобразно предоставените права. Достъпът до системата на кандидатите е автоматизиран, чрез регистрация.
- *Широката общественост* – ползва системата, чрез свободен достъп до информацията, в Публичния модул на ИСУН. Информацията се генерира въз основа въведените в системата данни от останалите потребители.

4. Актуално състояние на ИСУН

Към настоящия момент модулите на системата са следните:

1. Административен модул
2. Регистрация

3. Оценка
4. Договори
5. Управление на проекти
6. Финансов модул
7. Одитен модул
8. Интерфейс със SAP
9. Интерфейс с ИСАК и АКСТЪР-ПОПАЙ
10. Интерфейс с ТГС
11. Модул Наблюдение
12. Нередности и проверки на място
13. Параметри
14. Системна информация
15. Електронни услуги
16. Специализирани инструменти
17. Модул за публична информация
18. Интерфейс с SFC2007.

Наръчникът за работа със системата може да бъде намерен на адрес: <https://umis.government.bg/Help.aspx>.

5. Функционална архитектура

ИСУН притежава централизирана структура, вкл. обща база от данни. Достъпът на потребителите до системата е Web-базиран — чрез стандартен Web-браузер на потребителските работни станции. На потребителските работни станции не е необходимо да бъде инсталиран никакъв специфичен за системата софтуер. Изградени са интерфейси с други информационни системи.

6. Хардуерна и софтуерна платформа

Използваната хардуерна и софтуерна платформа за развитие на системата е посочена в долната таблица.

Хардуерна платформа	Intel – базирана
Операционна система	Microsoft Windows 2003 Server или по-високи версии
База данни	Microsoft SQL Server 2005 или по-високи версии
Софтуерни технологии	ASP.NET технологии за работа в Интернет, Microsoft .NET Framework 1.1, 2.0, 4.0, SOAP, Microsoft .NET Enterprise Services, Windows Workflow Foundation, Microsoft Office Sharepoint Server 2007, или по-високи версии, Microsoft SharePoint Services, XML, JSON, HTML и Microsoft Office, MS SQL Reporting Services, MS SQL Analysis Services,.



ЕВРОПЕЙСКИ СЪЮЗ



РЕПУБЛИКА
БЪЛГАРИЯ
МНОГО ВЪЗМОЖНОСТИ

Посочените в таблицата хардуерни и софтуерни компоненти не са обект на поръчката. Също така не са обект на поръчката всички необходими за достъпа до системата комуникационни компоненти, вкл. защитната стена (Firewall).

II. Изисквания за изпълнение на поръчката

1. Цел и обхват на поръчката

Основната цел на настоящата обществена поръчка е осигуряване поддръжка на системата. Изпълнителят следва да осигури адекватна и целенасочена софтуерна поддръжка и своевременна актуализация на всички работни среди на системата. Услугата включва поддържане и актуализиране на приложението, осигуряващо промени в приложния софтуер, които не могат да бъдат извършени със средствата на системното и приложното администриране на системата, включително:

- Извършване на Анализ на наличната в системата информация и предложение за надграждане на публичния модул на ИСУН 2007-2013
- Отстраняване на открити грешки в приложението. В рамките на определения срок Изпълнителят е длъжен да отстранява откритите грешки;
- Извършване на корекции в базата данни, след искане от страна на Възложителя, поради допуснати от потребителите грешки в минал период, които не могат да бъдат отстранени чрез средствата на потребителския интерфейс.
- Извършване на промени от ниско ниво. Тук се включва: отстраняване на констатираните несъответствия и грешки в публичния модул и във вътрешната среда на ИСУН, които водят до невъзможност за извеждането на коректни справки и информация от системата; след като съвместно с Възложителя извърши детайлен анализ на наличните справки Изпълнителят следва да извърши:
 - премахване на справки, за които не може да бъде генерирана коректна информация;
 - премахване/промяна/преработване на справки, които не са достатъчно информативни, нямат добавена стойност или дублират информация, налична в друга справка;
 - добавяне на нови справки;
 - отстраняване на констатирани несъответствия и грешки в наличните справки;
 - отстраняване на констатирани несъответствия и грешки в публичния модул.
- Извършване на други промени от Ниско ниво: Добавяне на индикатори, параметри, списъци, чек-листи, отчети както и извършване на промени в базата данни, внедряване на нови отчети, процедури и др. при заявена от Възложителя необходимост;

- Извършване на промени от Средно ниво. Тук се включват: промени в съществуващите функционалности и модули на софтуера във връзка с настъпили нормативни промени и/или изисквания на структурите, отговорни за координация, управление и контрол на средствата от Структурните фондове и Кохезионния фонд, които не са свързани с разработването на нови модули на системата, включително добавяне на нови полета в структурата на базата от данни или промяна на заложените в системата алгоритми.
- Консултации по грешки и проблеми с приложния софтуер на системата.

2. Организация на управлението на дейностите.

При изпълнение на дейностите на настоящата поръчка Изпълнителят съвместно с Възложителя ще изготвят план за изпълнение на услугата, който включва описание на конкретната задача, модул, срок за изпълнение, други изисквания, ако е приложимо, съобразно сложността на всяка задача и важност от гледна точка функционирането на системата.

Изпълнителят трябва да представи отчет към Възложителя за броя и обхвата на предоставените услуги по поддръжката.

Срокът за изпълнение на посочената услуга е до 30.11.2018 г.

При извършване на посочените услуги изпълнителят следва да:

- се съобразява с процедурата за управление на промените и процедурата за управление на внедряването с цел запазване на наличността на предоставяната от ИСУН услуга и запазване на цялостност и консистентност на данните в нея;
- се съобразява с изискванията поставени от стандарта за информационна сигурност ISO 27000 и политиката, и процедурите за информационна сигурност въведени и използвани при работа с ИСУН, налични на адрес <http://www.eufunds.bg>.

3. Идентифицирани рискове

Възложителят е идентифицирал следните основни рискове пред коректното функциониране на системата:

- Неправомерен достъп до системата
- Уязвимост към зловреден код;
- Загуба или манипулиране на данни;
- Нарушаване конфиденциалността на чувствителните данни;
- Възможни сривове на системата поради грешни действия на изпълнителя

4. Критерии за подбор.

4.1. За да се гарантира качество на изпълнение при реализиране дейностите на тази поръчка, се изискват специфични познания и опит. Възложителят определя критерии за подбор както следва:

4.1.1. Участниците трябва да прилагат система за управление на качеството, съответстваща на стандарт БДС EN ISO 9001:2015 или еквивалентен, с обхват разработване, внедряване и поддръжка на софтуерни продукти и информационни системи.

4.1.2. Участниците трябва да прилагат система за управление на сигурността на информацията, съответстваща на стандарт БДС EN ISO 27001:2013 или еквивалентен с обхват: разработване, внедряване и поддръжка на софтуерни продукти и информационни системи.

4.1.3. Участникът трябва да прилага система за управление на ИТ услуги, съответстваща на стандарт БДС EN ISO 20000-1:2012 или еквивалентен с обхват управление на ИТ услуги.

4.2. Участниците следва да разполагат с екип от персонал с определена професионална компетентност за изпълнение на поръчката, както следва:

4.2.1. Ръководител на екип:

- **Квалификация:** Ръководителят на екипа притежава сертификат в областта на управлението на проекти (Prince2 Foundation, PMI PMP или еквивалентен);
- **Опит:** Ръководителят на екипа притежава опит като ръководител на най-малко два успешно приключили проекта в областта на информационните технологии, включващи разработване, внедряване и поддръжка на уеб-базирана информационна система.

4.2.2. Бизнес аналитик.

- **Квалификация:** Притежава валиден сертификат в областта на бизнес анализа (IIBA CBAP, PMI/IPMA PBA или еквивалентен);
- **Опит:** Притежава професионален опит в анализ на бизнес процеси за минимум 2 (включително) успешно приключили проекта, включващи разработване и внедряване на уеб-базирана информационна система със СУБД.

4.2.3. Експерт „Програмиране“ 1

- **Квалификация:** Притежава квалификация с придобит сертификат след издържан изпит по системата за обучение на Microsoft или еквивалентно за програмиране на .NET;
- **Опит:** Притежава опит като програмист на най-малко два успешно приключили проекта, включващи разработване, внедряване и поддръжка на уеб-базирана информационна система, разработена върху .NET платформа (.NET framework) със СУБД Microsoft SQL Server.

4.2.4. Експерт „Програмиране“ 2

- **Квалификация:** Притежава квалификация с придобит сертификат след издържан изпит по системата за обучение на Microsoft или еквивалентно в областта на изграждането и управлението на бази данни, работещи върху платформа Microsoft SQL Server;
- **Опит:** Притежава опит като програмист на най-малко два успешно приключили проекта, включващи разработване, внедряване и поддръжка на уеб-базирана информационна система, разработена върху .NET платформа (.NET framework) със СУБД Microsoft SQL Server.

4.2.5. Експерт „Системно администриране“

- **Квалификация:** Притежава квалификация с придобит сертификат след издържан изпит по системата за обучение на Microsoft или еквивалентно в областта на изграждането и управлението на бази данни, работещи върху платформа Microsoft SQL Server;
- **Опит:** Притежава опит като системен администратор в минимум 2 успешно приключили проекта, включващи внедряване и поддръжка на информационна система с база данни базирана върху Microsoft SQL Server.

5. Критерии за възлагане

За изпълнител на обществената поръчка ще бъде избран участникът, предложил **икономически най-изгодната оферта**, която ще бъде определена по критерия **оптимално съотношение качество/цена**, съгласно чл. 70, ал. 2, т. 3 от ЗОП.

Оферти, които не отговарят на минималните изисквания и изискванията на документацията, се отстраняват и не се оценяват.

Комплексната оценка (КО) на офертата на всеки участник се определя по следната формула:

$$КО_n = П1_n \times 0,6 + П2_n \times 0,4, \text{ където}$$

КО_n - комплексна оценка на офертата на n-тия на участник;

П1_n - брой точки по показател „Предложена цена“ на офертата на n-тия участник;

П2_n – брой точки по показател „Техническо предложение“ на офертата на n-тия участник.

Класирането се извършва в низходящ ред, като на първо място се класира офертата, получила най-висока комплексна оценка по посочената формула. В случай, че комплексните оценки на две или повече оферти са равни, при класирането им се прилагат правилата на чл. 58 ал.2 и ал.3 от ППЗОП.



ЕВРОПЕЙСКИ СЪЮЗ



ЕДИНА ПОСТРОЙКА
МНОГО ВЪЗМОЖНОСТИ

Оценките по отделните показатели се представят в числово изражение с точност до втория знак след десетичната запетая.

Показатели за оценка и методика за определяне на комплексната оценка на офертите:

П1 – ПРЕДЛОЖЕНА ЦЕНА

Показател (наименование)	Относителна тежест в комплексната оценка	Максимален възможен брой точки	Символно означение
ПРЕДЛОЖЕНА ЦЕНА	60% (0,60)	100	П1

Показател П1 „Предложена цена” с максимален брой точки - 100 и относителна тежест в комплексната оценка – 0,60.

Максималният брой точки получава офертата с предложена най-ниска цена. Точките на останалите участници се определят в съотношение към най-ниската предложена цена по следната формула:

$$П1_n = Ц_{мин}/Ц_n \times 100, \text{ където:}$$

$Ц_{мин}$ е най-ниска предложена цена;

$Ц_n$ е цената на n -тия участник.

П2 – ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

Показател (наименование)	Относителна тежест в комплексната оценка	Максимален възможен брой точки	Символно означение
ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ	40% (0,40)	100	П2

Показател П2 „Качество” с максимален брой точки – 100 и относителна тежест в комплексната оценка – 0,40.

Точките по втория показател на n -я участник се получават по следната формула:

$П2_n = ПП1_n + ПП2_n$ и се формира като сбор от точките на следните под-показатели:

Под-показател (наименование)	Символно означение	Максимален възможен брой точки
1. Предложение за управление на риска при изпълнение на поръчката	ПП1	40
2. Предложения за подобряване на Публичния модул на ИСУН 2007-2013	ПП2	60
Общ брой точки от всички под-показатели по показател „Качество“:		100

Като под-показатели ПП1 и ПП2 се определят/оценят както следва:

	Под-показатели, формиращи показателя за качество	Точки на Участника
ПП 1	„Описание на подхода за управление на риска при изпълнение на поръчката“. Максимален брой точки 40.	40
ПП 1.1	В допълнение, към техническото предложение за изпълнение на поръчката, участникът е представил механизъм за отговор (предложение за предприемане на действия) за всеки от рисковете, посочени в Техническите спецификации. Посочените действия следва обосноваване да водят до намаляване на влиянието на и/или събдването описания риск и да са в обхвата на възможни за участника действия. Мерки, които не отговарят на тези критерии, няма да бъдат признавани. Забележка: За целите на настоящия критерий „Обосноваване“ означава съдържащо обяснение, демонстриращо как предложената мярка ще повлияе на вероятността за събждане и влиянието на събдването на съответния риск.	40
ПП 1.2	В допълнение, към техническото предложение за изпълнение на поръчката, участникът е предоставил механизъм за отговор (предложение за предприети действия) за 4 от рисковете, посочени в Техническите спецификации. Посочените действия следва обосноваване да водят до намаляване на описания риск и да са в обхвата на възможни за участника действия. Мерки, които не отговарят на тези критерии, няма да бъдат признавани. Забележка: За целите на настоящия критерий „Обосноваване“ означава съдържащо обяснение, демонстриращо как предложената мярка ще повлияе на вероятността за събждане и влиянието на събдването на съответния риск.	20
ПП 1.3	В допълнение, към техническото предложение за изпълнение на поръчката, участникът е предоставил механизъм за отговор (предложение за предприети действия) за 3 от рисковете, посочени в Техническите спецификации. Посочените действия следва обосноваване да водят до намаляване на описания риск и да са в обхвата на възможни за участника действия. Мерки, които не отговарят на тези критерии, няма да бъдат признавани.	10

	Забележка: За целите на настоящия критерий „Обоснован“ означава съдържащо обяснение, демонстриращо как предложената мярка ще повлияе на вероятността за сбъждане и влиянието на сбъждането на съответния риск.	
ПП 1.3	В допълнение, към техническото предложение за изпълнение на поръчката, участникът е предоставил механизъм за отговор (предложение за предприети действия) за по-малко от 3, но поне за 1 от рисковете, посочени в Техническите спецификации. Посочените действия следва обосновано да водят до намаляване на описания риск и да са в обхвата на възможни за участника действия. Мерки, които не отговарят на тези критерии, няма да бъдат признавани. Забележка: За целите на настоящия критерий „Обоснован“ означава съдържащо обяснение, демонстриращо как предложената мярка ще повлияе на вероятността за сбъждане и влиянието на сбъждането на съответния риск.	1
ПП 2	„Предложения за подобряване на Публичния модул на ИСУН 2007-2013“. Максимален брой точки 60.	60
ПП 2.1	Предложението включва описание и обосновка на необходимостта от въвеждане на минимум 3 допълнителни функционалности за подобряване на Публичния модул на ИСУН 2007-2013. Забележка: Липсата на описание или обосновка за необходимостта от въвеждане на предложените допълнителни функционалности ще доведе до тяхното непризнаване.	60
ПП 2.2	Предложението включва описание и обосновка на необходимостта от въвеждане на 2 допълнителни функционалности за подобряване на Публичния модул на ИСУН 2007-2013. Забележка: Липсата на описание или обосновка за необходимостта от въвеждане на предложените допълнителни функционалности ще доведе до тяхното непризнаване.	30
ПП 2.3	Предложението включва описание и обосновка на необходимостта от въвеждане на 1 допълнителна функционалност за подобряване на Публичния модул на ИСУН 2007-2013. Забележка: Липсата на описание или обосновка за необходимостта от въвеждане на предложените допълнителни функционалности ще доведе до тяхното непризнаване.	10



ОДНА ПОСОБА
МНОГО ВЪЗМОЖНОСТИ

чл.2 33ЛД

Приложение № 2

До
Администрация на Министерския съвет
София, бул. „Дондуков“ № 1

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

за участие в обществена поръчка при условията на чл. 20, ал. 3, т. 2 от Закона за обществените поръчки (ЗОП) по реда на Глава Двадесет и шеста за възлагане на обществени поръчки чрез събиране на оферти с обява

От участник:

„ДАВИД Холдинг“ АД,

БУЛСТАТ/ЕИК 833092882, адрес гр. Казанлък, ул. „Стара река“ № 2, ДК „Арсенал“
офис 417,

банкова сметка BG04UBBS88881000756115,

чл.2 33ЛД

представяван от Бальо Атанасов Динев

УВАЖАЕМИ ДАМИ И ГОСПОДА,

Във връзка с обявената от Вас обществена поръчка по реда на Глава Двадесет и шеста ЗОП за възлагане на обществени поръчки чрез събиране на оферти с обява с предмет: „Анализ и отстраняване на констатираните несъответствия в публичния модул и вътрешната среда на ИСУН за програмния период 2007-2013“, представяме нашето техническо предложение за изпълнение на обществената поръчка, както следва: следва (прилага се подробно описание на предложението за изпълнение на поръчката на участника, съобразно Техническата спецификация и изискванията на Възложителя. Техническите предложения на участниците следва да съдържат и предложения, които подлежат на оценяване съобразно методиката за оценка на офертите):

I. Предложение за управление на риска при изпълнение на поръчката

При дефинирането на мерките за намаляване на риска сме приложили най-добрите практики в областта на информационната сигурност - интегриран подход при управлението на риска (Integrated Risk Management). Характерно за този подход е, че той адресира рисковете на различни нива на организацията и от различни гледни точки и като резултат в много случаи една мярка може да намалява вероятността от събъждане и/или влиянието на повече от един риск.

Риск	Мерки за намаляване на риска
1. Неправомерен достъп до системата	<p>Неправомерен достъп до системата е риск, който може да доведе до нарушаване конфиденциалността, целостта и наличността на информацията в системата и респективно да компрометира системата като цяло. Предвид големият и обществено значимото предназначение на системата и съхраняваните в нея данни е голяма вероятността от опити за придобиване на неправомерен достъп до нея.</p> <p>За осигуряване високи нива на защита на информационната система ИСУН 2007-2013 от реализация на риска „Неправомерен достъп до системата“ следва системата да отговаря на следните основни критерии:</p> <ul style="list-style-type: none"> • Да има изградена Ролево базирана сигурност – в системата да са налични роли, които определят достъпа и правата за ползване на обектите, интерфейсите механизми и алгоритмите за обработка на информация в нея. Ролево базираната сигурност трябва да дава на всеки тип потребител на системата права до минимално необходимите му данни и потребителски интерфейси за коректно и безпроблемно изпълнение на операциите. • Средствата за идентификация на потребителите да са надеждно защитени от неправомерен достъп. Криптиране на паролите с използване на силен хеш алгоритъм (SHA 256), не позволяващ възстановяването им. • Да са налични програмни средства за спазване на правилата за формиране на пароли и честотата на смяната им в политиките и процедурите по информационна сигурност. • При разработването на системата да са отчетени известните слабости на използваните средства за разработка и използваните компоненти за изграждане на системата и да са взети мерки за тяхното преодоляване. • Да е осигурена адекватна защита на сървърните компоненти на системата от неправомерен достъп. • Да са реализирани средства за верификация и защита на информацията в алгоритмите за нейната обработка. • Потребителските интерфейси на системата да не допускат неоторизирани потребители до непублични части от системата. • Да са предвидени мерки за защита от хакерски атаки, целящи придобиване на достъп до системата и нейните данни. <p>Една от основните цели на обществената поръчка е Повишаване на сигурността на достъпа и данните в системата. За постигане на тази цел, минимизиране на риска от придобиване на неправомерен достъп до данни и алгоритми в системата, следвайки набелязаните по-горе критерии за осигуряване на висока сигурност, ще предприемем следните мерки:</p> <p>1.1. Анализ на защитата на системата от неправомерен достъп</p> <p>При изпълнение на Анализ на текущото състояние и функционалности на ИСУН 2007-2013, ще бъде извършен анализ на всички компоненти на системата, имащи отношение към осигуряване на защита от неправомерен достъп до системата включващи:</p> <ul style="list-style-type: none"> • Анализ на средствата за идентификация на потребителите;

- Анализ на механизмите за определяне правата на регистрираните потребители;
- Анализ на потребителските интерфейси на системата за откриване на потенциални уязвимости в резултат от използваните технологии за разработка и използване на практики при разработка за минимизиране на уязвимостта;
- Анализ на използваните практики в сорс кода на системата за защита на данните и на достъпа;
- Анализ на събитията, регистриращи се в регистрационните файловете на системата (logs) и тяхното разширение ако е необходимо;
- Анализ на съответствието с утвърдените политики и процедури за информационна сигурност на информационна система ИСУН 2007-2013 и предложения за актуализацията им и в съответствие с най-добрите практики за изграждане и поддръжка на информационни системи, базирани на най-добри практики за информационна сигурност, описаните в ISO 27002:2013 Code of practice конкретно разделите за контрол на достъпа и разработка и поддръжка на софтуер.

В резултат от извършените действия при изпълнение на Услуга 1 ще предоставим информация за текущото ниво на защита на информационната система от неправомерен достъп и ще бъдат предложени конкретни мерки за намаляване на вероятността и/или влиянието от реализацията на този риск. За всяка от предложените мерки ще бъде направена оценка на риска и ще бъдат категоризирани по вероятност и влияние върху информационната система. С цел приоритизиране на дейностите по минимизация на риска и реализиране с по висок приоритет и в по-кратки срокове на защитните мерки с най-голяма вероятност и влияние.

Предложените мерки за намаление на риска, след приемане от Възложителя, ще бъдат реализирани от нас в процеса на изпълнение на Услуга 2 – Разработване на нови функционалности и поддържане на ИСУН 2007-2013. В резултат от изпълнение на мярката ще има актуална оценка на риска „Неправомерен достъп до системата“ с ясна приоритизация, влияние и вероятност на различните сценарии и механизми за неговото събъждане. Оценка на риска ще служи като план за повишаване на сигурността на системата и приоритетно изпълнение в рамките на Услуга 2 на мерки за защита и минимизация на рисковете с най-голямо вероятност и/или влияние върху системата.

Тази мярка ще доведе до значително намаление на риска от неправомерен достъп до системата, тъй като в резултат от нея ще бъдат открити слабите места на системата, които може да се използват за неправомерен достъп, а също и актуализирането на политиките и процедурите за информационна сигурност на системата в съответствие с най-добрите практики.

1.2. Преглед и актуализация на политиките и процедури по сигурност

Ще направим преглед на политиките и процедури по сигурност на информационната система и ще предложим актуализация за тези от тях, които считаме че е необходимо, включително:

- Правила и процедури за контрол на достъп до активите – с цел актуализиране и подобряване на изискванията към потребителските идентификатори, процедурите за предоставяне на права.

- Добавяне на (описаната по-долу) двустепенна идентификация на потребителите с по-големи права (от управляващите органи, ЦКЗ и администраторите на системата), еднократни пароли за външни изпълнители, средства за сигурен обмен на пароли с външни изпълнители и др.
- Описание на ИТ инфраструктурата – актуализация на описанието на ИТ инфраструктурата и отразяване на промените, настъпили от последната редакция от м09.2013г.
- Извеждане описанието на ИТ инфраструктурата в отделен документ с ограничаване на правата за достъп до тази информация до ръководителите на звената, отговорни за поддържането на ИТ инфраструктурата на ИСУН 2007-2013 и лицата и ръководителите на звена, включени в структурата на управление и контрола на информационната сигурност. Целта е минимално разпространяване на информация, която може да се ползва за определяне на потенциални технически уязвимости на изграждащите системата компоненти.
- Преглед и актуализация на политиката за избор на пароли – сложност, честота на смяна, както и включване на задължителна двустепенна идентификация (2FA) за роли с административни права и такива, които биха могли да предизвикат загуба или манипулиране на данни и нарушаване на конфиденциалността на данните. Проверка, че са реализирани механизми, които осигуряват налагането на политиката за избор на пароли.

Актуализацията на политиките и процедурите по сигурността ще позволят в тях да се включат всички нови технически средства за контрол и защита от неправомерен достъп, а изваждането на описанието на ИТ инфраструктурата в отделен документ с контролиран достъп ще намали риска от неправомерен достъп за сметка на откриване на уязвимости от страна на лица, които не са пряко ангажирани с поддръжката ѝ.

Тази мярка намалява риска от неправомерен достъп за сметка на подобряването на политиката и процедурите за информационна сигурност и налагане на правила на потребителите на системата, не позволяващи избор на „слаба“ парола, която би могла да бъде отгатната по метода на социалния инженеринг или чрез груба сила (налучкване).

1.3. Преглед на правата за всяка роля

С цел минимизиране на влиянието на риска от неправомерен достъп до данни, до които съответният потребител не би следвало да има достъп, в рамките на аналитична фаза ще бъде направен преглед на правата всяка от ролите в системата с цел да се установят наличието на твърде високи за конкретната роля права, които не са нужни за изпълнение на ежедневните дейности на дадената роля.

В случай, че се установи превишаване на правата за определени роли, ще предложим намаляване на определени права или в случаите, когато това е приложимо разделяне на някои твърде общи роли (ако съществуват такива) на няколко роли с различни права.

След одобрение на Възложителя ще реализираме, съответните промени в правата и/или ролите.

Тази мярка ще намали влиянието при евентуалната реализация на риска от неправомерен достъп, като ограничи правата за достъп до минимално необходимите за всяка роля.

1.4. Идентифициране на неактивни потребители

Преглед на журналните файлове (logs) на системата и установяване на потребителите, които са вътрешни за системата и не са били активни за дълъг период от време (примерно над 1 месец), за да се установи дали няма потребители, които вече не би следвало да имат достъп до системата, а достъпа им не е отнет.

Индивидуално преглеждане на всички потребители с административни права, за да е сигурно, че не са останали потребителите, които вече не би следвало да имат достъп до системата с административни права.

Тази мярка намалява риска от неправилен достъп до системата на потребители, които не би следвало да имат такъв, но той не е прекратен.

1.5. Централизирано управление на вътрешните потребители

В рамките на аналитичната фаза ще бъде проверено наличието на техническа възможност достъпа на вътрешните за системата потребители да се управляват чрез Active Directory (LDAP), за да се осигури централизирано управление на правата и достъпа им до системата.

При наличие на такава възможност, тя ще бъде реализирана след одобрение от Възложителя.

Тази мярка намалява риска от неправилен достъп до системата на потребители, които не би следвало да имат такъв, но той не е прекратен и не е коригиран в съответствие с променените им роли и отговорности.

1.6. Защита на средствата за идентификация на експертите на Изпълнителя при изпълнението на дейностите по поръчката

При изпълнение на дейностите по поръчката, експертите, които ще имат достъп до информационната система и изграждащите я компоненти ще спазват:

- политиките, процедурите и правилата за информационна сигурност на системата ИСУН 2007-2013, прилагани от Възложителя и описани в актуалната политика;
- политиките, процедурите и правилата за информационна сигурност при разработка и поддръжка на софтуер, разписани в системата за информационна сигурност на Изпълнителя, сертифицирана по стандарт ISO 27001:2013, както и приложимите най-добри практики за информационна сигурност, описаните в ISO 27002:2013 Code of practice и конкретно разделите за контрол на достъпа и разработка и поддръжка на софтуер;
- политиките, процедурите и правилата за информационна сигурност на системата разписани в системата за управление на ИТ услугите за поддръжка на Изпълнителя, сертифицирана по стандарт ISO 20000-1:2011, както и приложимите най-добри практики за информационна сигурност, описани в приложението ISO 20000-2:2012 и конкретно разделите за поддръжка на софтуерни системи;

С цел допълнително намаляване на риска от неправилен достъп до системата ще бъдат приети значително по-високи нива на защита от заложените в текущите правила, като например:

- Отдалечен достъп до компонентите на системата да се осъществява само от утвърдените работни станции на Изпълнителя.

- На всички работни станции на Изпълнителя, утвърдени за достъп до компоненти на информационната система, ще бъдат инсталирани антивирусни решения с активирани автоматични актуализации.
 - Ще се използват само сигурни, предварително утвърдени от Възложителя средства за достъп до компонентите на системата, като VPN клиент и средства за отдалечен достъп, която ще се изисква ежедневно парола или за всеки достъп.
 - Паролите на експертите ще спазват и надхвърлят утвърдените за ИСУН 2007-2013 изисквания за дължина, изисквания за формиране и честота на промяна.
 - Заявяване на отдалечен достъп до системата само, когато е необходимо, като през другото време отдалечения достъп не е активен.
 - Средствата за идентификация на експертите няма да се съхраняват в явен вид на какъвто и да е носител.
 - Поддържане на регистър за достъпа до компоненти на системата, в който всеки експерт ще отразява времето, причината и компонентите, до които е осъществил достъп с цел регистрация, ясна проследимост и последващ анализ на действията на експертите.
 - Ограничаване използването на акаунтите на експертите на Изпълнителя само от конкретни IP адреси.
 - При продължително спиране на работа на експерт по проекта (продължителен отпуск, болест, напускане) ще бъдат предприети мерки за прекратяване на достъпа до информационната система и нейни компоненти. Възложителя ще бъде уведомен за това по надлежен ред преди настъпване на планирано спиране на работа на експерта и не повече от 2 работни дни от настъпване на непланирано събитие (отпуск по болест).
 - Всички експерти на Изпълнителя са подписали декларации за конфиденциалност в съответствие с изискванията на внедрената при Изпълнителя система за управление на сигурността на информацията по стандарт ISO 27001:2013. В допълнение на това при стартиране на проекта ще бъдат подписани и декларации за конфиденциалност (съгласувани с Възложителя), за запазване и неразпространение на информация по проекта, за срока на активно използване на информационната система.
- Изпълнението на описаните действия и изисквания към нашите експерти, осигуряват много висока степен на опазване на информацията, свързана с изпълнение на проекта станала достояние до нашите експерти и минимизират риска от нейното разпространение, в т.ч. и на информация, възможност и/или насоки за реализация на нерегламентиран достъп до системата ИСУН 2007-2013 и изграждащите я компоненти.
- Тази мярка намалява риска от неправомерен достъп до системата чрез използване на данните за достъп на експерти ангажирани с изпълнението на поръчката.

1.7. Приоритизация на докладвани/открити възможности или инциденти за неправомерен достъп до системата

Всички докладвани от Възложителя или открити от Изпълнителя възможности за осигуряване на неоторизиран достъп до информационната система или изграждащите я компоненти в обхвата на действие на

Изпълнителя ще бъдат с най-висок приоритет за изпълнение. Ще се предприемат незабавни мерки за предотвратяване на тези възможности с фокус върху конфиденциалността и целостта на данните и средствата за обработка на информацията.

Докладвани инциденти от Възложителя, даващи възможност за неправомерен достъп до която и да е част от системата, ще бъдат класифицирани като критични и обработвани съгласно утвърдените за информационната система процедури за управление на инциденти, в рамките на сроковете за реакция и възстановяване на ИСУН, посочени в техническото ни предложение.

Неоторизираният достъп до системата е риск с потенциално голямо въздействие и всички грешки в системата или други събития, даващи потенциална възможност или реална събдваемост на този риск е оправдано да са с възможно най-висок приоритет за реакция.

Предложената мярка позволява реакция на инцидент, свързан с неправомерен достъп до системата в много кратко време, което води до намаляване на ефекта от потенциалната или реалната реализация на този риск.

1.8. Сигурност на транспортната среда

Системата ИСУН 2007-2013 е интернет базирана и се използва през стандартни интернет браузъри както от администрацията, така и от бизнеса и гражданите. За да се минимизира риска от неправомерен достъп до данните е необходимо да се осигури не само процес на сигурна идентификация, но и сигурност на данните в транспортната им среда между потребителя и сървърите на системата.

За да постигнем ниска вероятност на риска от неоторизиран достъп до данните на системата, при реализация на промени и нови разработки в системата ще изпълняваме следните мерки за сигурност на транспортната среда:

Достъпа до потребителските интерфейси на системата ще се осъществява само по криптиран (https) канал с цел сигурност и осигуряване на защита на трансферираните данни. Това ще става чрез кодиране като се използват стандартите TLS/SSL (Transport Layer Security) за осигуряване на потвърждаване на идентичността и конфиденциалност на крайните точки при канал за комуникация и AES (Advanced Encryption Standard) с минимум 128-битов ключ за осигуряване на сигурността на съобщенията. За целта на приложния сървър на системата следва да бъде инсталиран и поддържан актуален сървърен цифров сертификат.

Защитата на транспортната среда е един от основните фактори за осигуряване на защита от неправомерен достъп до системата и нейни данни.

Препоръчваме използването на сертификати с разширено валидиране (extended validation (EV) certificates) за сървърите на системата. Като сертификати от най-висок клас, сертификатите с разширено валидиране (EV SSL) активират едновременно и катинарче и зелен идентификационен надпис директно в адресната лента на всички браузъри. EV SSL сертификатите осигуряват най-високото възможно ниво на криптиране и позволяват бързо и ясно идентифициране на организацията, управляваща системата.

Тази мярка намалява риска от прихващане на данните за достъп (име и парола) в транспортните среди между компонентите на системата и потребителите и следователно намалява риска от неправомерен достъп до системата с чужди данни за достъп прихванати в транспортната среда между клиента и системата.

1.12. Следене за уязвимости и обновяване на всички компоненти на системата

Следене на техническата информация от производителя на ключовите конфигурационни елементи на системата (ОС, СУБД, ISS) за възможности за осъществяване на неправомерен достъп до тях. Партньорството с производителя осигурява пълен достъп до техническите бюлетини по сигурността.

Експертите от екипа, отговарящи за администрирането и поддръжката на Microsoft Windows Server и Microsoft SQL Server, ще следят ежедневно за такава информация и в случаите, когато се появи такава, незабавно ще бъде стартиран план за оценка на риска и прилагане на мерки за отстраняването на съответната уязвимост в съответствие с политиката за управление на внедряването (release management).

В случай, че риска от възникване на неправомерен достъп, чрез използване на съответната уязвимост се оцени като висок или критичен, ще бъде приложено незабавно съответното обновяване (security patch) под формата на диференциално внедряване (differential release) в тестовата среда, а след преминаване на успешни тестове и в продукционната среда на системата.

В случай, че риска от възникване на неправомерен достъп, чрез използване съответната уязвимост се оцени като нисък, то съответната уязвимост ще бъде отстранена чрез пакетно внедряване (packaged release), заедно с реализирането на други изменения в системата.

Тази мярка намалява риска от неправомерен достъп до системата, чрез използване на уязвимост (exploit) в нейните компоненти (ОС, Web-сървър ISS, SQL Server).

2. Уязвимост към зловреден код

Зловреден код е всеки софтуерен компонент, действащ без знанието на потребителя и целящ да осигури неправомерен достъп, да наруши конфиденциалността, целостта и наличността на данните и/или да промени поведението на системите. По начина си на проникване, предназначение и въздействие върху информационната система, най-често срещаните видове зловреден код са:

- Вируси (virus)
- Червей (worm)
- Троянски коне (Trojan horse)
- Задна врата (backdoor)
- Шпионски софтуер (spyware)
- Рекламен софтуер (adware)
- Софтуер за запис на клавиши и/или работен плот (Keylogger/screenlogger)
- Фалшив софтуер (rogue)
- Rootkit
- Криптовируси (Ransomware)

За намаляване на уязвимостта на системата към зловреден код е необходимо прилагане на комплекс от мерки за намаляване вероятността и въздействието на всички споменати видове зловреден код. На база наличната информация за системата сме идентифицирали следните мерки за защита:

2.1. Преглед и изготвяне на предложения за актуализация на политиките за сигурност

В процеса на изпълнение на услуга анализа на текущото състояние и функционалности на ИСУН 2007-2013 ще направим цялостен преглед политиката за информационна сигурност в частта ѝ касаеща третирането на уязвимостта към зловреден код и ще изготвим предложения за актуализация на политиката в съответствие с най-добрите практики.

Изпълнението на мярката ще доведе до актуалност и съобразеност на политиките за информационна сигурност на ИСУН 2007-2013 с динамично променящите се заплахи от нови видове зловреден код, начини на проникване, вероятности за тяхната реализация и потенциални въздействия върху системата за целият срок на договора (жизнен цикъл на системата).

2.2. Преглед и оптимизация на инфраструктурата

Ще бъде извършен цялостен преглед на инфраструктурата, върху която работи системата, за наличие на споделени папки (share), които могат да бъдат обект на атака от криптовируси (ransomware). В случай на установяване на такива ще бъде анализирана тяхната необходимост като ще бъдат предложени алтернативни методи с цел намаляване на риска от проникване на зловреден код и минимизиране на въздействието, което може да укаже евентуалното му проникване.

Тази мярка ще намали риска от проникване на зловреден код, който се разпространява чрез споделени папки (share).

2.3. Предоставяне на приложен софтуер без зловреден код

На всички ключови етапи на разработка и тестване на промени в системата при Изпълнителя ще се изпълнява антивирусна проверка, със софтуер с актуални вирусни дефиниции. Като минимум това ще са етапите на компилиране на разработените модули на системата преди вътрешни тестове при Изпълнителя, преди началото и след приключване на вътрешните тестове, тестване на подготвените дистрибутиви за инсталация във всяка от средите на Възложителя. На всеки от тези етапи ще бъде осъществявана проверка и на MD5 hash-сумите на модулите.

С внедряването на тази мярка ще верифицираме, че разработените модули на системата са чисти от вируси (backdoor и др.) и респективно се намаля вероятността за проникване на зловреден софтуер с разработваните от нас промени в системата.

2.4. Използване на Definitive Media Library (DML) за инсталация на софтуер

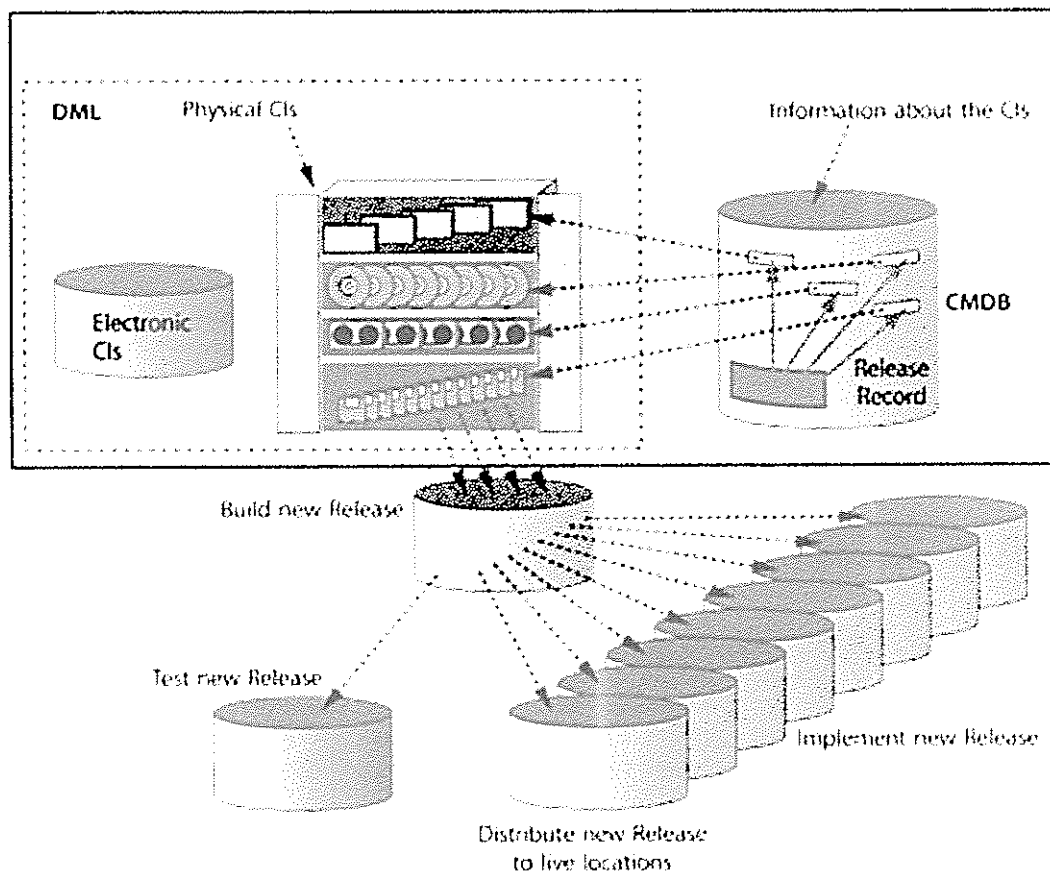
Definitive Media Library (DML), известна още в по-старите версии на ITIL и като Definitive Software Library (DSL), е сигурно защитено хранилище, в което

ще се пазят последните одобрени за употреба в продукционна среда версии на всички софтуерните компоненти на системата.

Този подход гарантира, че до инсталация в продукционна среда ще достига само проверен, тестван и одобрен софтуер, без зловреден код или грешки. Definitive Media Library (DML) съхранява само финалните версии на всички софтуерни компоненти на системата, както разработваните приложения, така и оригиналните инсталационни комплекти на други софтуерни компоненти, като операционни системи и системи за управление на бази данни (в случая Microsoft Windows Server и Microsoft SQL Server), а също и одобрените за инсталация в продукционна среда обновявания (updates, patches).

Използването на Definitive Media Library (DML) заедно с базата данни за управление на конфигурациите (CMDB) ефективно налага практиката да се използват само правилните, одобрени за инсталация в продукционна среда, версии на всички софтуерни компоненти (CIs) на системата, като по-този начин се намалява риска от инсталиране на неodobрен или неработещ правилно софтуер в следствие на грешка на инсталиращия екип на Изпълнителя.

DML and CMDB



Използването на DML не само оптимизира изпълнението на горните процеси, но и намалява риска от проникване на зловреден код, поради инсталиране на непроверен и одобрен софтуер, който съдържа такъв.

2.5. Внедряване на правила за сигурна работа с качвани в системата файлове

Един от възможните сценарии за изпълнение на зловреден код спрямо компоненти на информационната система е чрез качване на файлове във формите на системата, които да се активират на определен принцип (напр. стартиране на зловреден код чрез заявка за получаване на каченият (файл) или се интерпретират грешно от системата, като скриптове за изпълнение.

За намаляване на вероятността от реализация на такъв сценарий, предвиждаме да разработим процедура за сигурна работа с качвани в системата файлове, а след нейното утвърждаване от Възложителя, ще се реализират всички утвърдени програмни и административни мерки.

Принципите, които ще следваме за постигане на сигурна работа с качвани от потребители на системата файлове или външна система, с която е изградена интеграция, са следните:

- Разработка на „Забранен списък“ (black list) със забранени за качване типове файлове. Списъка ще съдържа типове файлови формати, които носят висок риск от внедряване в системата на зловреден код и стандартно не се използват за подаване на необходимата в конкретният бизнес модел информация. Това например са: Изпълними файлове (.exe, .bat, .com и др.), Специални файлове, използвани в компоненти на системата (например: в файловете типове и файлове с наименование *.htaccess, web.config, robots.txt, crossdomain.xml и clientaccesspolicy.xml, могат да позволят на лица, реализиращи атака към системата да променят настройките за сигурност, натоварването на системата и др.
- В аналитичната фаза на проекта ще бъде направен анализ на местата, където е необходимо да се качват външни файлове в системата. За всяко едно място ще се прецени дали е възможно да се определи и списък за допустимите използвани файлове формати за съхранение и обработка на тези типове данни (например: само XLS, само PDF, само PDF или JPG). В резултат от анализа, ще бъде разработен „Разрешен списък“ (white list), съдържащ само разрешените типове файлове. Списъка определя видовете файлове, които могат да се качват от потребителя на дадено място и отхвърля всички файлове, които не съответстват на одобрените типове. Целта е постигане на максимално възможно ниво на сигурност на системата, с прилагане на силно ограничение на типовете файлове прилагани в системата, с което се намалява вероятността от внедряване на зловреден код, без това да създава проблеми в работата на потребителите.
- Определяне и внедряване на правила за използване на средства за валидация на файлове, за да се гарантира, че не се прилагат техники за заобикаляне на списъците със забранени и разрешени файлови типове. Чрез проверка на типа (например използване на втори тип в името на файла – image.jpg.php, или използване на интервали или точки в името на файла).
- Забрана за качване на криптирани с пароли файлове (освен в случаите на криптирани с валиден електронен подпис или с ключ от самата система).
- Определяне максимален размер на единичен файл, който може да бъде качван в системата.
- Определяне максимална дължина на името на файл, който може да бъде качван в системата.

	<ul style="list-style-type: none"> • Проверка на качваните в системата файлове за съвпадение на типа на файла със съдържащите се данни в него. Целта на тази проверка е да се предотврати маскирано качване на файлове със зловреден код и не отговарящи на заложените изисквания в забранения и разрешения списък с файлови типове. • Задължително сканиране на качваните файлове с антивирусен софтуер, изтриване на файлове, в които са открити вирусни дефиниции, изпращане на автоматично уведомление по мейл на потребителя за отхвърляне на файла. • Разработка на конвенция за определяне имена на файлове и автоматично преименуване на качваните файлове съгласно изградената конвенция, с цел намаляване на вероятността от извикване на качен в системата потребителски файл и извикването му с цел активиране на зловреден код. • Качване на файлове само в определен справочник (директория) на сървър на системата, която не е основната за web-сървъра, в нея няма права за изпълнение на файлове (execution) и има активирано антивирусно сканиране в реално време. <p>Предложеният комплекс от мерки за работа с файлове, качвани в системата от потребителите, водят до чувствително намаляване на вероятността от реализация на риска „Уязвимост към зловреден код“.</p> <p>2.6. Премахване на ненужни сървърни услуги и софтуер</p> <p>В процеса на изпълнение на Услуга 1 „Анализ на текущото състояние и функциониране на ИСУН 2007-2013“, при делегиране на права от страна на Възложителя, ще направим анализ на необходимите за нормалната работа на системата сървърни услуги и софтуерни пакети върху сървърите на системата. Ще изготвим доклад с минимално необходимите компоненти, както и пакетите и услугите, работещи върху сървърите на системата, но не са нужни за функционирането на ИСУН 2007-2013 с препоръка всички ненужни пакети да се спрат или деинсталират.</p> <p>С тази мярка се намалява риска от наличие или възникване на уязвимост в някой от софтуерните пакети и сървърни услуги, които не са нужни за функционирането на системата, респективно се намалява вероятността от внедряване и изпълнение на зловреден код в средата на системата.</p>
<p>3. Загуба или манипулиране на данни</p>	<p>Информационна система ИСУН 2007-2013 е съхранява данни за фондовете за европейско финансиране за програмният период 2007-2013г. и загубата или манипулирането на каквато и да е част от данните на системата може да доведе до големи неблагоприятни последици. По тази причина считаме, че риска от „Загуба или манипулиране на данни“ трябва да се сведе до минималното възможно ниво. Поради което, заедно със заложените в политиките и процедурите за сигурност на информационната система изисквания за редундантност на данните (в различни териториални структури) и архивиране и сигурност на архивните копия следва да се набележи, оцени и приложи комплекс от мерки за допълнителна минимизация на риска.</p> <p>На база наличните данни към момента за информационната система и обхвата на възможните дейности за изпълнение в рамките на този проект, сме</p>

идентифицирали следните мерки, които трябва да се приложат за качествено управление и минимизиране на вероятността и ефекта от реализацията на риска „Загуба или манипулиране на данни“:

3.1. Преглед и изготвяне на предложения за актуализация на политиките за сигурност

В процеса на изпълнение на анализа на текущото състояние на ИСУН, след оценка на текущото състояние ще извършим оценка на риска от загуба и манипулиране на данни и ще създадем план за третиране на риска, с който да се постигне възможно най-ниското ниво на този риск.

Специално внимание ще бъде обърнато на процедурите за резервиране на данни и разработка на цялостен план за създаване и съхраняване на резервни копия на данните в съответствие с най-добрите практики за целта. Конкретно забелязани места за подобрения на този етап в настоящата версия на процедурите за Резервиране и архивиране на информацията при Възложителя са:

- Автоматизирано създаване с висока честота на междинни архиви на данните (между две архивирания на лентов магнитен носител) със средствата на СУБД, минимум на 4 часа, в основния и резервния ИЦ. Архивирането на данните в двата ИЦ да не се извършва по едно и също време (например с разминаване от 2 часа).
- Съхраняването на междинните архивите на различни дискови масиви от използваните за нормалната експлоатация на системата. Целта на мярката е да се постигне защита от нарушаване целостта и коректността на данните в системата. А също и въздействието от репликирането в резервния ИЦ на манипулирани данни.
- При изпълнение на тестово възстановяване работоспособността на системата, да се извършва тестово възстановяване на слоя с данни от последен междинен архив.
- В Процедурата за Възстановяване на данни при невнимателно опериране от страна на потребител, да се добави изискване за възстановяване на информацията първо в тестова среда. Извършване оценка на възстановената информация, за ненарушаване целостта на данните въведени и модифицирани в системата от момента на създаване на архивното копие до текущият момент. Едва след това да се прави възстановяване в реална среда.

3.2. Прилагане принципите за сигурна разработка в процеса разработка на нови функционалности

Създаване в рамките на изпълнение на Услуга 1, след анализ на текущото състояние, ще бъдат разработени „Инженерни принципи за разработка на сигурни приложения“, в които се залагат правила за разработка на сигурни софтуерни приложения. При реализация на промени в сорс кода на системата, независимо от модулите, в които се осъществява промяната ще се спазват утвърдените инженерни принципи за разработка на сигурни приложения. Спазването на тези принципи води до еднотипен стил на разработка, базиран на правила, фокусирани върху всички аспекти на сигурността на системата и респективно до ниска вероятност и ниско въздействие при евентуална реализация на определени рискове, в т.ч. и риска за загуба или манипулиране

на данните. В инженерните принципи ще бъдат включени и детайлизирани следните мерки за намаляване на риска от манипулиране и загуба на данни:

3.2.1. Защита от SQL Injection - SQL Injection е една от най-опасните уеб уязвимости и е класирана на първо място в класацията на OWASP за десетте на сериозни уязвимости за сигурността на информационни системи. Посредством SQL Injection може да се промени структурата на SQL запитване на уеб приложение, по начин, който може да доведе до манипулиране, изтриване или извличане на конфиденциални данни. Най-добрата превенция срещу SQL injection е използването на параметрични SQL заявки. За недопускане проявлението на тази уязвимост, при разработка на промени в системата ще се използват само параметрични SQL заявки и няма да се допуска динамично сформирание на SQL заявки в клиентския слой на системата. Използване на готови параметрични заявки е основна предпоставка за минимизация на риска от SQL hijacking, SQL Injection и други методи за вмешателство в данните и гарантира че атакуващите няма променят поведението на SQL заявките от клиентския слой на системата.

Осигуряването на защита срещу SQL Injection намаля риска от загуба или манипулиране на данни в системата.

3.2.2. Няма да се дава детайлна информация за системните грешки

Логическите грешки, свързани с поведението на потребителя или подадените от него данни ще дават ясна и конкретна информация за неправилното действие и/или данни, а също и възможните начини на корекция, когато това е приложимо.

При настъпване на системна грешка, обаче няма да се извеждат технически детайли за грешките, тъй като тази информация може да помогне на лица със злонамерена активност за откриване на възможности за разкриване на уязвимост, атаки с цел изтриване или манипулиране на данни.

Техническите детайли за дадена системна грешка не говорят нищо и не са от полза на средностатистическия потребител на системата, а непоказването им ще намали риска от идентифициране на уязвимост и използването ѝ за изтриване или манипулиране на данни.

3.2.3. Транзакционен принцип на работа с данните

При разработка на промени в системата ще се обръща особено внимание за гарантиране целостта на логически свързани данни, като записа на данни ще се извършва винаги на транзакционен принцип. Използването на транзакционен принцип на работа няма да позволи логически свързани данни да бъдат частично променени, с което да се наруши логическата цялост и консистентност на данните и намалява вероятността от загуба и манипулиране на данните в системата в следствие на възникнали технически проблеми.

При изтриване на данни системата ще проверява дали данните, подлежащи на изтриване не са използвани в други данни и в случай, че това е така няма

да позволява да бъдат изтривани. Това важи за ключови данни, като списъци и номенклатури, чието изтриване би могло да доведе загуба на данни или манипулиране на данните в системата в следствие на изтриването на първичните данни и подмяната им с други.

Прилагането на транзакционен принцип на работа с данните осигурява интегритета им намалява риска от загуба на данни в следствие неуспешно завършване на транзакция.

3.2.4. Използване на защитени канали за комуникация между отделните слоеве на системата и при обмен на данни с потребители и външни системи

Достъпа до интерфейсите на системата, включително нови или променяни модули, интерфейси и др. програмни единици, предназначени за интеракция с потребителите ще се осъществява само по https канал с цел сигурност и осигуряване на защита на трансферираните данни. Това ще става чрез кодиране като се използват стандартите TLS/SSL (Transport Layer Security) за осигуряване на потвърждаване на идентичността и конфиденциалност на крайните точки при канал за комуникация и AES (Advanced Encryption Standard) с минимум 128-битов ключ за осигуряване на сигурността на съобщенията.

Обмена на данни с външни системи и приложения ще се изпълнява по защитени канали за комуникация, гарантиращи висока степен на защита на данните от неоторизиран достъп, на транзакционен принцип гарантиращ целостта на данните. При проектирането на интерфейси за обмен на данни с всяка отделна външна система ще бъдат прилагани най-високите възможни изисквания за конфиденциалност на данните, в зависимост от технологичните интерфейси и възможности на отделната външна система. При проектирането на интерфейси за обмен на данни с ИСУН 2007-2013, който да бъде използван за външни системи ще бъде прилагано криптиране на данни с двойка ключове (публичен и частен), което ще гарантира, че данните, изпратени от ИСУН 2007-2013 не са манипулирани и могат да бъдат прочетени само от външната система, за която са предназначени и обратно при обмен в другата посока. Този метод няма да се прилага за изцяло публични данни.

Тези мерки за защита на данните са с цел намаляване на вероятността от манипулиране и/или загуба на данни в процеса на трансфер на тези данни между отделните слоеве на системата или при обмен с други системи.

3.3. Гарантиране автентичност на модулите на системата

Подписване с цифров сертификат на всички модули на системата (Assembly signing), работещи в реалната среда с цел предотвратяване и идентификация на манипулирани програмни единици.

В резултат от прилагането на тази мярка се минимизира риска от неоторизирана промяна на програмния код на системата, с която би могло да бъде извършена изтриване или манипулиране на данни в системата.

3.4. Следене и регистриране действията на администраторите в системата

Всички действия, извършвани от администраторите на системата ще бъдат регистрирани с цел възможност за проследимост и проверка при необходимост. Това важи както за действията, извършвани през потребителския интерфейс на системата, така и действията по администрацията на системата на ниско ниво – база данни и файлове.

Системата за регистрация (logs) ще бъде организирана така, че нито един от администраторите да няма възможност да изтрива регистрациите на собствените си действия. Това се постига с ограничаване на правата върху местата, където се съхраняват системните журнали (логове).

Тази мярка позволява да се намали риска от несанкционирано изтриване или манипулиране на данни от страна на администраторите на системата.

3.5. Защита от зловреден код

Един от най-честите причини за загуба на данни е внедряване на зловреден код в приложението или средата на изпълнение на информационната система, поради което прилагането на всички мерки за третиране на риска „Уязвимост към зловреден код“ пряко намаляват вероятността за реализация на риска от загуба на данни.

3.6. Защита от неправилен достъп

Един от причини за загуба или манипулиране на данни е чрез неправилен достъп до информационната система, поради което прилагането на всички мерки за третиране на риска „Защита от неправилен достъп“ пряко намаляват вероятността за реализация на риска от загуба или манипулиране на данни.

3.9. Налагане на механизми за контрол на правата на потребителите

При разработването на системата ще бъде приложен принципа за проверка, че потребителя е идентифициран и валидиран, че ролята му има достатъчно права за изпълнение на операциите по промяна или изтриване на данни. Този подход ще позволи намаляването на риска от загуба или манипулиране на данни, чрез използване уязвимости като XSS (Cross Site Scripting) и CSRF (Cross Site Request Forgery), като за избягването им ще се използва CSRF маркер (token) и криптирани параметри в URL на заявките.

Тази мярка намалява вероятността за реализация на риска от загуба или манипулиране на данни за сметка на превишаване на правата на потребител или изпълнение на заявка от неидентифициран потребител, чрез използване на уязвимости в системата.

4. Нарушаване конфиденциалността на чувствителните данни

Нарушаване конфиденциалността на чувствителните данни е риск с голямо въздействие. Предвид големият брой потребители и обществено значимото предназначение на системата и съхраняваните в нея данни е голяма вероятността от опити за придобиване на съхраняваните в нея чувствителни данни. Чувствителни данни са всички данни, поддържани в системата, до които не трябва да се осигурява публичен достъп без надлежна

идентификация на потребител и данни, до които даден потребител няма право на достъп според предоставените му права.

При изпълнение на договора планираме като минимум да прилагаме следните мерки за намаляване на вероятността за реализация на риска:

4.1. Достъп на потребителите до минимално необходимите им данни, интерфейси и функции за обработка на информацията

При проектиране и реализация на промени в ИСУН 2007-2013 ще бъде спазван принципа за делегиране на права на потребителите само до минимално необходимите им данни и функционалности. За всеки нов обект в системата ще се прави анализ за ролите, в които следва да бъде включено използването му и минимално необходимите права върху обекта за всяка роля.

В процеса на разработка на промени в системата при необходимост ще бъдат създавани нови роли, за да се спазва принципа за достъп на потребителите до минимално необходимите им данни. За всяка нова роля ще се предоставя на Възложителя **Карта за правата на достъп** - детайлно описание на правата върху обектите в системата (четене, запис, промяна и т.н.), а така също и предложения за актуализация на формуляра „Заявка за създаване/промяна/закриване на потребителски профил“.

Прилагането на принципа за делегиране на права на потребителите само до минимално необходимите им данни и функционалности, намалява риска от нарушаване на конфиденциалността на чувствителни данни за сметка на получаване на достъп до данни, които не са нужни за пряката работа на съответната роля.

4.2. Анализ на съществуващите роли и права за достъп

В рамките на изпълнението на анализа на състоянието ще бъде направен преглед на правата всяка от ролите в системата с цел да се установят наличието на твърде високи за конкретната роля права, които не са нужни за изпълнение на ежедневните дейности на дадена роля. Ако бъдат открити права за достъп до данни, които не са нужни за нормалната работа на съответната роля, ще бъде предложено на възложителя техните права да бъдат актуализирани.

Тази мярка намалява риска от нарушаване на конфиденциалността на чувствителни данни за сметка на ненужни или неактуални роли, както и завишени права за достъп до данни, ненужни за дадена роля.

4.3. Анализ на неактивни потребители на системата

Преглед на журналните файлове (logs) на системата и установяване на потребителите, които са вътрешни за системата и не са били активни за дълъг период от време (над 1 месец), за да се установи дали няма потребители, които вече не би следвало да имат достъп до системата, а достъпа им не е отнет.

Индивидуално преглеждане на всички потребители с административни права, за да е сигурно, че не са останали потребителите, които вече не би следвало да имат достъп до системата.

При възможност достъпа на вътрешните за системата потребители да се управлява чрез Active Directory (LDAP), за да се осигури централизирано управление на правата и достъпа им до системата.

Този подход минимизира риска от нарушаване конфиденциалността на чувствителните данни, до които потребителите вече не би трябвало да имат достъп (например поради промяна на длъжността им).

4.4. Преглед и актуализация на политиката за пароли

Преглед и актуализация на политиката за избор на пароли – сложност, честота на смяна, както и включване на задължителна двустепенна идентификация (2FA) за роли с административни права и такива, които биха могли да предизвикат нарушаване на конфиденциалността на чувствителни данните.

Извършване на проверка, че са реализирани механизми, които осигуряват реалното налагане (enforcement) на политика за избор на пароли. Това е особено важно за служебни потребители и поддържащи екипи, включително този на изпълнителя.

Тази мярка намалява риска от нарушаване конфиденциалността на чувствителните данни, чрез налучкването на пароли за достъп, базирани на често използвани логически модели за формиране на парола или на основата на социален инженеринг.

4.5. Криптиране на чувствителни данни, съхранявани в системата

В рамките на Услуга 1 – Анализ на текущото състояние ще бъдат анализирани данните, които се съхраняват в системата и ще бъде направена оценка дали някои от тях са конфиденциални и следва да бъдат криптирани. Ако се установи наличието на такива данни те ще бъдат криптирани с използването на силен криптографски алгоритъм (AES 128). Криптирането ще се осъществява в слоя на приложния сървър на системата, като така към базата данни тези данни ще бъдат прехвърляни и съхранявани само в криптиран вид.

Криптирането на чувствителни данни и съхраняването и прехвърлянето им само в криптиран вид намалява риска от нарушаване конфиденциалността на чувствителните данни, тъй като дори даден потребител да прихване или да се сдобие неправомерно с такива данни те не могат да бъдат прочетени и са неизползваеми.

4.6. Криптиране на данните за идентификация

Данните за идентификация на потребителите са най-чувствителните данни, чиято конфиденциалност трябва да бъде запазена. Всички пароли ще бъдат съхранявани в криптиран вид. За криптиране на паролите ще се използва силен хеш алгоритъм (SHA 256), непозволяващ възстановяването им. Този подход ще гарантира, че никой, дори потребителите имащи пълни

административни права върху всички компоненти на системата, няма да може да декриптира паролата на друг потребител и да осъществи достъп от негово име.

Прилагането на силни еднопосочни алгоритми за криптиране надеждно защитава идентификационните данни на потребители и намаля риска от нарушаване конфиденциалността на чувствителните данни в случая паролите за достъп.

4.7. Защита на конфиденциалните данни в транспортната среда на системата (публичен интернет)

Системата ИСУН 2007-2013 е интернет базирана и се използва през стандартни интернет браузъри като от администрацията, така и от бизнеса и гражданите. За да се минимизира риска от нарушаване конфиденциалността на чувствителните данни е необходимо не само процес на сигурна идентификация, но и осигуряване на сигурност на данните в транспортната им среда между потребителя и сървърите на системата. За да гарантираме ниска вероятност на риска за нарушаване на конфиденциалността на чувствителни данни в системата, при реализация на промени и нови разработки в системата, достъпа до интерфейсите на системата от потребителите ще се осъществява само по https канал с цел сигурност и осигуряване на защита на трансферираните данни. Това ще става чрез кодиране като се използват стандартите TLS/SSL (Transport Layer Security) за осигуряване на потвърждаване на идентичността и конфиденциалност на крайните точки при канал за комуникация и AES (Advanced Encryption Standard) с минимум 128-битов ключ за осигуряване на сигурността на съобщенията. За целта на приложния сървър на системата следва да бъде инсталиран сървърен цифров сертификат.

Прилагането на тази мярка намалява риска от нарушаване конфиденциалността на чувствителните данни, като защитава всички данни, които обменят потребителите със системата, включително най-чувствителната информация – данните за идентификация на потребителя от прихващането ѝ при комуникация в публичния интернет.

4.8. Защита на данните между Възложителя и Изпълнителя

Прилагане на мерки за превенция на риска от прихващане на обменяни чувствителни данни между Възложителя и Изпълнителя:

- Изпращане на данни за идентификация в средите на Възложителя в криптиран вид и/или по различни канали за комуникация (напр. по мейл в криптиран файл, а ключ за декриптиране чрез SMS от предварително определен номер(а) до предварително регистриран номер(а));
- Използване на еднократни пароли за достъп до компоненти на продуктивната система;
- Използване на двустепенна авторизация (2FA) с честота на изпращане на код за достъп – 1 ден за достъп до среди и компоненти, в които не се изисква ежедневна работа;

- Изпращане на други чувствителни данни за структура, архитектура и топология на системата, IP адреси, DNS имена в криптиран вид. За превенция срещу узнаване на потенциални уязвимости и набелязване на цели за атака от злонамерени лица.

Целта на мярката е да се осигури защита на чувствителната информация, която ще се обменя между Възложителя и Изпълнителя и която би могла да доведе до достъп и/или разкриване на чувствителни данни.

Прилагането на тази мярка намалява риска от нарушаване конфиденциалността на чувствителните данни, като защитава чувствителната информация, която се съхранява в системата – данните за идентификация на специалистите на Изпълнителя за получаване на достъп до системата и нейните компоненти в повечето случаи с администраторски права.

4.9. Защита от опити за налучкване на паролата

Един от методите за нарушаване конфиденциалността на чувствителни данни е чрез налучкване на паролата на даден потребител по метода на социалния инженеринг. В случаите, когато злонамереното лице познава навиците на потребител на системата, има информация за факти от личния му живот, дати, имена и друга лична информация, знае негова парола за достъп до друга система или логиката, по които потребителя обикновено избира паролите си, то може да се опита да налучка паролата му за системата и това да доведе до нарушаване на конфиденциалността на чувствителни данни.

В този случай защитата с код за сигурност не е достатъчна, защото при този метод не се генерират автоматизирано пароли по метода на грубата сила (brute force), а атакуващия пробва да налучка паролата, като ръчно въвежда и кода за защита. Това създава неудобство, но не и реална защита от налучкване на парола по метода на социалния инженеринг.

Системата следва да регистрира такива събития в журналния файл, а в случаите, когато става въпрос за служебен или административен потребител, системата следва да изпраща и уведомление по имейл до друг (различен от заключения) административен потребител.

Прилагането на тази мярка намалява риска от нарушаване конфиденциалността на чувствителните данни чрез отгатване (налучкване) на паролата на потребител на системата по метода на социалния инженеринг.

4.10. Защита от зловреден код

Един от честите методи за нарушаване конфиденциалността на чувствителни данни е чрез внедряване на зловреден код в системите и средата на изпълнение на информационната система, поради което прилагането на всички мерки за третиране на риска „Уязвимост към зловреден код“ пряко влияят за намаляване на вероятността за реализация и въздействието на риска „Нарушаване конфиденциалността на чувствителни данни“.

Конкретно приложими за намаляването на риска от нарушаване конфиденциалността на чувствителни данни са използването на подписан код

	<p>на приложните модули, в който липсват задни вратички (back doors) и DML за всички компоненти на системата.</p>
<p>5. Възможни сринове на системата поради грешни действия на изпълнителя</p>	<p>Предвид обхвата на оказваните услуги в рамките на обществената поръчка, потенциална реализация на риска от сринове на информационна система ИСУН 2007-2013 поради грешни действия на Изпълнителя може да доведе до сериозни последици.</p> <p>Базирайки се на нашия над 20 годишен опит в изграждане и поддържане на критични за бизнеса на клиентите ни, информационни системи, внедрените системи за управление сигурността на информацията по стандарт ISO 27001:2013 и Управление на ИТ услуги по стандарт ISO 20000-1:2011, за намаляване на вероятността и евентуалните последици при реализация на риск „Възможни сринове на системата поради грешни действия на изпълнителя“, ще прилагаме следният комплекс от мерки:</p> <p>5.1. Изпълнение на действията от компетентен и опитен персонал Всяко от действията по изпълнение на договора ще бъде извършвано от компетентен за конкретното действие персонал, притежаващ опит, знания и умения за изпълнение на действието и сертификати за преминали обучения за процесите/системите/средите в обхвата на изпълнение на действието. Няма да се допуска изпълнение на действия и/или дейности от недостатъчно подготвени за съответните действия служители. Възложителя е поставил високи изисквания за компетентност и опит, като всички предложени от нас експерти отговарят на най-високите поставени критерии, а в определени области ги надхвърлят с познания и умения, директно водещи до намаляване риска от сринове на системата, поради грешни действия на изпълнителя.</p> <p>Ръководителят и един от членовете на екипа на Изпълнителя, притежават сертификат ITIL Foundation, гарантиращ задълбочени познания за набора от добри практики за управление на ИТ услуги – ITIL 2011, което позволява използване на знанията при изпълнение на услугите по развитие и поддръжка на системата и води до намаляване на риска от възможни сринове в системата поради грешни действия на изпълнителя.</p> <p>Прилагането на мярката намалява както вероятността, така и последиците от реализация на риска, поради високото ниво на компетентност на предлаганите от нас експерти, недопускане за изпълнение на дейности от неподготвен за конкретната дейност персонал и доказани познания по най-добрите практики за управление на ИТ услуги ITIL 2011.</p> <p>Предложения за изпълнение на поръчката екип е изпълнявал поддръжка на информационната система ИСУН 2007-2013 и има опит в това.</p> <p>5.2. Начално обучение на екипа на изпълнителя Всички експерти от екипа на Изпълнителя познават в детайли процедурите за поддръжка и информационна сигурност на съответните внедрени системи за управление сигурността на информацията по стандарт ISO 27001:2013 и Управление на ИТ услуги по стандарт ISO 20000-1:2011. Ръководителят на екипа е представител на ръководството, а един от членовете е мениджър на</p>

внедрените при Изпълнителя системи за управление сигурността на информацията по стандарт ISO 27001:2013 и Управление на ИТ услуги по стандарт ISO 20000-1:2011.

Допълнително на всички експерти, ангажирани с изпълнение на поръчката, преди започване на работа, ще бъде проведено допълнително обучение за:

- Опресняване на знанията, свързани с процедурите за осигуряване на непрекъсваемост на бизнеса и управление на измененията при Изпълнителя с акцент върху практическото им прилагане при изпълнение на настоящата поръчка за всеки отделен експерт.
- Запознаване с наличните процедури при Възложителя за информационна сигурност и процедурите за работа на звено за техническа подкрепа. Акцент върху ролите и отговорностите на всеки експерт от екип на Изпълнителя за всяка конкретна процедура, дефинирани в документите на Възложителя.
- Нови най-добри практики от набора от добри практики за управление на ИТ услуги – ITIL, които са приложими при изпълнение на услугите по развитие и поддръжка на системите и водят до намаляване на риска от възможни сринове в системата.

Предвиждаме обучението на експертите да включва:

- Запознаване с процеса за управление на промените (change management), както и интегрирането му със съответната процедура при Изпълнителя за практическото му прилагане при изпълнение на поръчката. Акцента ще е върху създаването и изпълнението на планове за възстановяване на системата към предишно състояние (roll-back план).
- Запознаване с процеса за управление на внедряването (release management) политиката за управление на внедряванията (Release Policy), както и интегрирането им със съответната процедура при Изпълнителя за практическото им прилагане при изпълнение на поръчката. Тук акцента ще бъде върху създаването и изпълнението на планове за внедряване на нова и променена функционалност на системата, като целта ще бъде да се пакетират максимален брой промени в едно внедряване (release) с цел минимизиране на риска при всяко едно внедряване.
- Запознаване с процеса за управление на конфигурациите (configuration management), както и интегрирането му със съответната процедура при Изпълнителя за практическото му прилагане при изпълнение на поръчката. Тук акцента ще е върху гарантиране актуалността и интегритета на данните в базата за управление на конфигурацията (CMDB) на всички среди на системата (тестова, продукционна, за разработка и публичен тест) и поддържането на актуална версия на CMDB при Изпълнителя.
- Запознаване с процеса за управление на проблемите (problem management), както и интегрирането му със съответната процедура при Изпълнителя за практическото му прилагане при изпълнение на поръчката. Акцент върху анализа на досегашни сринове на системата, поради грешни действия на изпълнителя, ако има данни за такива.
- Запознаване с процеса за управление на достъпността (availability management), както и интегрирането му със съответната процедура при

изпълнителя за практическото му прилагане при изпълнение на поръчката. Тук акцента ще е върху плана за наличността, изискванията за актуалните нива на наличност и дефинираните метрики и отчети.

- Запознаване с процеса за управление на външните доставчици (supplier management), както и интегрирането му със съответната процедура при Изпълнителя за практическото му прилагане при изпълнение на поръчката. Тук акцента ще е върху изискванията към Изпълнителя като доставчик на ИТ услуги.
- Запознаване с процеса за управление на непрекъснатостта (IT service continuity management), както и интегрирането му със съответната процедура при изпълнителя за практическото му прилагане при изпълнение на поръчката. Тук акцента ще е върху актуалните планове за непрекъснатост на системата и възстановяване от бедствия и аварии, изготвените анализи на рисковете и дейностите по управлението на рисковете, наличните механизми за непрекъснатост на услугите.

Прилагането на мярката намалява както вероятността, така и последствията от реализация на риска, поради високото ниво на компетентност на предлаганите от нас експерти и недопускане за изпълнение на дейности от неподготвен за конкретната дейност персонал.

5.3. Разделяне на отговорностите по проектиране, разработка, тестване и поддръжка на системата

За да се постигне високо ниво на сигурност в процесите по разработка на нови функционалности на системата планираме да прилагаме подход за ясно разделяне на отговорностите, правата и ролите за всеки етап на процеса. Там където е възможно за всеки етап ще се определят различни отговорни експерти за изпълнение на етапа. Като единствено предвиждаме изключение за тестването на промените, в който задължително ще се включват и експертите проектирали промените – с цел оценка съответствието на реализацията с разработените технически задания за реализация.

Включването на достатъчен брой експерти в изпълнението на задачата с ясни отговорност е предпоставка за своевременно откриване на потенциални проблеми и реализация на механизми за тяхното отстраняване, което намалява вероятността от реализация на риска от сринове на системата поради грешни действия на изпълнителя.

5.4. Непрекъснато усъвършенстване на експертите в екипа

Непрекъснатото усъвършенстване знанията и уменията на експертите от екипа на Изпълнителя е ключов фактор за намаляване на вероятността и въздействието от възможни грешни действия от страна на екипа на изпълнителя.

За постоянното намаляване на нивото на този риск, предвиждаме провеждане на обучения на нашите експерти на планирани интервали от време. Към настоящият момент планираме провеждането на следните видове обучения:

- Встъпително обучение за запознаване на експертите с политиките и процедурите за сигурност на информационната система ИСУН 2007-2013. Обучението ще се проведе преди начало на работата на експертите по изпълнение на договора.
- Обучения за нови уязвимости, заплахи и рискове за информационната система и нейни ключови компоненти. Целта на обучението е да се запознаят експерти от екипа на Изпълнителя с нови заплахи за сигурността на информационната система и/или нейни компоненти, в резултат от използваните технологии за разработка, архитектурни и технически решения или други фактори. Обучението ще акцентира върху технологичните решения и средствата за справяне с тези заплахи и тяхната превенция. Обученията ще се провеждат на регулярни интервали от време не по-дълги от 6 месеца или при възникване на нови заплахи и уязвимости за информационната система или конкретни нейни конфигурационни елементи.
- Тематични обучения по групи експерти за вътрешен трансфер на знания за информационната система ИСУН 2007-2013, придобити по време на изпълнение на договора. Обученията ще се провеждат на регулярни интервали от време не по-дълги от 3 месеца през първата година и 6 месеца за периода след първата година.

Тази мярка намалява риска като осигурява непрекъснатото усъвършенстване знанията и уменията на експертите от екипа на Изпълнителя, което ще доведе до намаляване на вероятността и въздействието от възможни грешни действия от страна на екипа на изпълнителя.

5.5. Пакетиране на няколко промени в едно внедряване (packaged release)

Всяка промяна в продукционната среда създава риск от срив на системата. С цел минимизиране на този риск при създаването и изпълнение на планове за внедряване (release management) на нова и променена функционалност на системата, ще се стараем да се пакетират максимален брой промени в едно внедряване (packaged release) с цел минимизиране на риска от срив при всяко едно внедряване. Особено важен е този подход при внедряването на няколко логически свързани промени, което подобрява потребителското преживяване (user experience) при използването на нови функционалности, но и значително намалява риска от сринове в системата.

Предвиждаме да реализираме този подход, чрез анализ и оценка дали дадена заявена промяна може да се пакетира с други подобни промени по следните критерии:

- Промяната не е спешна. Пакетират се само стандартни и нормални промени.
- Намаляване на риска за другите промени, при пакетиране с тях.
- Намаляване на общото време за изпълнение на промените при комбинирането им.
- Намаляване натоварването на екипите на Изпълнителя и Възложителя в следствие намаляване на общото време тестване и внедряване на промените при пакетирането им.
- Времето на постъпване заявката е съобразено с планиране на внедряванията според „Политиката за внедряване“.

Подхода за пакетиране на внедрявания (packaged release) е особено подходящ при пускане на нови версии на приложната част на системата (full release) или части от системата, решаващи конкретни проблеми (пачове - differential releases), заедно с нови версии (full releases) или пачове (differential releases) на ключови конфигурационни компоненти (CI – Configuration items) като операционна система, сървър за база данни, web сървър и т.н. Този подход няма да се прилага за спешни промени.

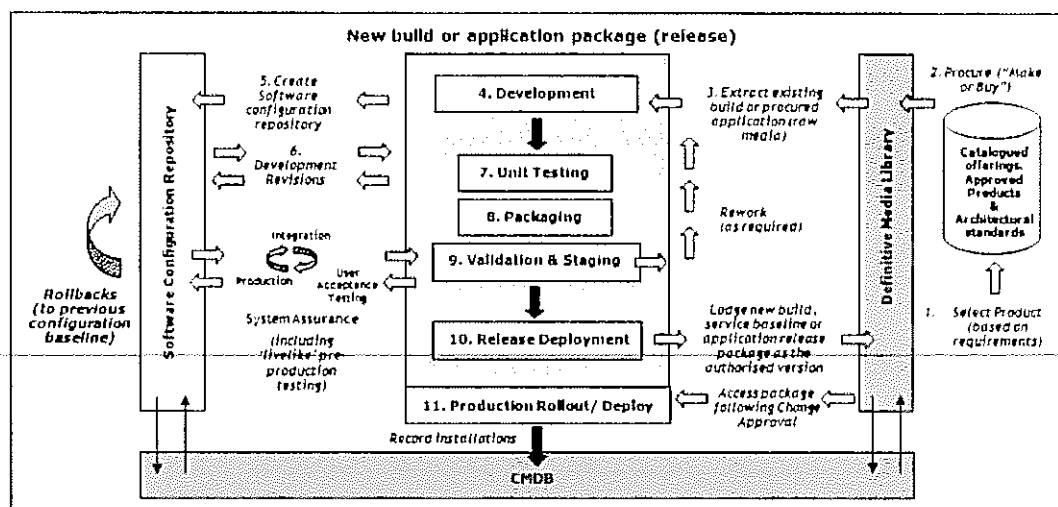
Пакетирането на няколко промени в едно внедряване (packaged release) води до намаляване на възможностите за грешка, поради по-малкия брой случаи, в които се извършват потенциално опасни действия в продукционната среда и намалява риска от сринове на системата поради грешни действия на изпълнителя.

5.6. Използване на Definitive Media Library (DML) за внедряване, за възстановяване на услугата и справяне с аварии

Definitive Media Library (DML), известна още в по-старите версии на ITIL и като Definitive Software Library (DSL), е сигурно защитено хранилище, в което се пазят последните одобрени за употреба в продукционна среда версии на софтуера.

Този подход гарантира, че до инсталация в продукционна среда ще достига само проверен, тестван и одобрен софтуер, без зловреден код или грешки. Definitive Media Library (DML) съхранява само финалните версии на всички софтуерни компоненти на системата, както разработваните приложения, така и оригиналните инсталационни комплекти на други софтуерни компоненти, като операционни системи и системи за управление на бази данни (в случая Microsoft Windows Server и Microsoft SQL Server), а също и одобрените за инсталация в продукционна среда обновявания (updates, patches).

Използването на Definitive Media Library (DML) и CMDB в контекста на процеса по управление на внедряването (release management) е илюстрирано на следната диаграма:



Използването на Definitive Media Library (DML) заедно с базата данни за управление на конфигурациите (CMDB) ефективно налага практиката да се използват само правилните, одобрени за инсталация в продукционна среда, версии на всички софтуерни компоненти (CIs) на системата, като по-този начин се намалява риска от инсталиране на неodobрен или неработещ правилно софтуер в следствие на грешка на инсталиращия екип на Изпълнителя.

Добра практика е освен софтуерните компоненти в Definitive Media Library (DML) да се съхраняват и асоциирани с тях елементи, като лицензна информация или ключове и документация. По този начин се гарантира, че се поддържат актуални не само софтуерните компоненти, но и цялата свързана с тях информация, което намалява вероятността за грешки. Софтуера, съхраняван в DML се управлява в съответствие с процесите за управление на измененията и внедряването и се регистрира в CMDB.

Съгласно набора най-добри практики ITIL, DML подпомага:

- Процеса за управление на внедряването (Release and Deployment), като осигурява централизирано място за съхранение на всички одобрени за инсталиране в продукционна среда софтуерни пакети и компоненти.
- Процесите за управление на достъпността и непрекъснатостта (Availability and Service Continuity), като осигурява проверен и сигурен източник за инсталиране на всички софтуерни компоненти на системата по време на процедурите по възстановяване на услугата (service restoration) и възстановяване от аварии (Disaster recovery).

Използването на DML не само оптимизира изпълнението на горните процеси, но и намалява риска от срив системата, поради инсталиране на неodobрен или неработещ правилно софтуер в следствие на грешка на инсталиращия екип на Изпълнителя, като ефекта е особено силен, когато се изпълняват процедурите по възстановяване на услугата (service restoration) и възстановяване от аварии (Disaster recovery), тъй като обичайно те се изпълняват под стрес при неработеща система и съответно вероятността за грешки е по-висока.

5.7. Регистриране на действията по изпълнение на договора

Ще бъде създаден индивидуален за ИСУН 2007-2013 регистър на извършваните от екипа на Изпълнителя действия по поддръжка на системата. В регистъра ще се отразяват всички действия на експертите по поддръжка, включително: достъп до информационни активи на ИСУН 2007-2013, дейности по отстраняване на настъпили събития и/или инциденти и др.

Целта на мярката е да осигурим пълна проследимост на действията на нашите експерти, коректността на работата им и спазването на политиките и процедурите по сигурност на информационната система, както и на разработените и утвърдени детайлни работни инструкции.

Регистрираните действия ще бъдат обект на регулярен преглед и анализ и са основа за взимане на превантивни и коригиращи действия, за намаляване на риска от сринове на системата вследствие на действие или бездействие на експерти на Изпълнителя.

5.8. Анализ на досегашни сринове на системата

Доколкото системата е действаща и нейната поддръжка се осъществява в продължение на повече от година, и в момента в съответствие с процедурите за работа на звеното за техническа подкрепа, всички възникнали до момента проблеми би следвало да се регистрират.

Предвиждаме да направим анализ на досегашните сринове на системата поради грешни действия на изпълнителя, ако има данни за такива, като изследваме причините довели до срыв в системата и набележим конкретни мерки за предотвратяването сринове по аналогични причини в бъдеще.

Ще бъде направен преглед и анализ на:

- Актуалните планове за непрекъснатост на ИСУН и възстановяване от бедствия и аварии и изготвянето на препоръки за подобрене и актуализация.
- Актуалните анализи за въздействието на бедствията и аварията върху бизнес операциите и обновяване на планове за възстановяване.
- Наличните анализи на рисковете и предприетите дейности по управлението им и изготвянето на препоръки за подобрене и актуализация.
- Преглед на наличните механизми за непрекъснатост на услугите и резултатите от тестването им или реалното им прилагане и изготвянето на препоръки за подобрене и актуализация.

В резултат на натрупания опит ще предложим актуализация на съответните процедури и/или добавяне на нови механизми за непрекъснатост на услугите или подобряването им.

Целта на мярката е да се направят изводи от евентуалните досегашни сринове в системата и да се набележи комплекс от коригиращи и превантивни мерки, чието изпълнение ще намали на риска от сринове на системата в следствие на експерти на Изпълнителя.

II. Предложения за подобряване на Публичния модул на ИСУН 2007-2013

Предложение	Описание и обосновка
1. Добавяне на ЕИК/Булстат	<p>Описание: Предложената промяна включва добавяне и визуализиране на наличния в системата единен идентификационен код (ЕИК) или Булстат номера на организациите бенефициенти, партньори или изпълнители по проектите, финансирани със средствата от Структурните фондове и Кохезионния фонд (СКФ) в България. Предложената промяна ще обхване всички таблици, съдържащи информация за посочените оператори.</p> <p>Обосновка: Предложената промяна е необходима с оглед предоставянето на възможност за извършване на коректни справки и последващото обработване на наличната, в публичния модул на ИСУН, информация. Данните за организациите, представени в публичния модул на ИСУН, не предоставят възможност за извършване на последваща обработка и анализ поради липсата на единен уникален идентификатор на субекта. Визуализирането на ЕИК и Булстат номера на икономическите субекти ще повиши допълнително публичността и прозрачността при усвояването на средствата, предоставени от ЕС.</p>
2. Актуализация на данните в публичния модул	<p>Описание: Текущата функционалност на публичния модул на ИСУН за актуализиране на данните в системата изисква намесата на квалифицирано техническо лице (ИТ експерт), което да инициира описаното действие. В тази връзка предложената промяна включва възможност за актуализация на данните в публичния модул със средствата на потребителския интерфейс от оторизирано/и за целта лице/а (например потребител от Централното координационно звено), без да е необходимо ангажирането на ИТ експерт, който да зарежда съответния скрипт за опресняване на данните в системата.</p> <p>Обосновка: Предложената промяна се обосновава с необходимостта от текуща актуализация на данните в публичния модул на ИСУН, което представлява повтарящо се действие и след първоначалното разработването на приложния скрипт за актуализация, не следва да се изисква специализирана намеса от страна на ИТ експерт. Предложената промяна ще улесни възможността за актуализация на данните и в извънредни случаи.</p>
3. Функционалност за отворени данни	<p>Описание: Публикуването на публичната информация в отворен формат е задължение за организациите от публичния сектор съгласно Директива 2013/37/ЕС на Европейския парламент и на Съвета от 26 юни 2013</p>

	<p>година за изменение на Директива 2003/98/ЕО относно повторната употреба на информацията в общественния сектор. Директивата се транспонира с изменения и допълнения на Закона за достъп до обществената информация и съответните подзаконовни нормативни актове. Текущата функционалност на публичния модул на ИСУН не предоставя възможност за осигуряване на пълен открит достъп до публичните данни в ИСУН и има както икономически ефекти, така и по-широко обществено значение. Част от тях са генериране и реализация на</p>
	<p>бизнес идеи с помощта на отворените набори от данни. Според оценка на Европейската комисия, предоставянето на открит достъп до данните и възможност за повторното им използване в европейски мащаб, може да донесе икономически облаги на държавите - членки на ЕС, на стойност приблизително 40 милиарда евро годишно. Предложената функционалност ще осигури възможност за предоставяне в структуриран вид (машинночетим формат) на пълния набор от данни от публичния модул на ИСУН.</p> <p>Обосновка: Предложената промяна се обосновава с оглед необходимостта от осигуряване на коректни пълни данни за изпълнението на програмите финансирани по Структурните фондове и Кохезионния фонд (СКФ) в България за програмния период 2007-2013 и осигуряването на законоустановеното ниво на публичност и прозрачност при управлението на средствата от ЕС. Към момента информацията от публичния модул на ИСУН извежда частично в зависимост от ограниченията на таблицата, която се визуализира в системата.</p>
<p>4. Информация за кандидати</p>	<p>Описание: Предложената промяна включва добавяне и визуализиране на информация за организациите кандидати по програмите, финансирани от Структурните фондове и Кохезионния фонд (СКФ), в публичния модул на ИСУН. Предложената промяна ще обхване кандидатите по всички 7 програми от програмния период 2007-2013.</p> <p>Обосновка: Предложената промяна се обосновава с липсата на данни за кандидатите по програмите, финансирани от ЕС. Наличието на посочените данни в публичния модул на ИСУН ще допринесе за повишаване на възможностите за анализ на информацията и активността на различните организации, съответно тяхната успеваемост при кандидатстване.</p>



чл.2 33ЛД

ОДНА ПОРЪЧКА
МНОГО ВЪЗМОЖНОСТИ

Декларираме, че сме съгласни с клаузите на приложения проект на договор.

Срокът на валидност на настоящата оферта е 60 дни след изтичане на срока за подаване на офертите.

Прилагам подробен график, с конкретизирани срокове за изпълнение на всяка дейност и поддейност от настоящата поръчка.

Приложение: ГРАФИК за изпълнение на поръчката.

ПОДПИС и ПЕЧАТ:

чл.2 33ЛД

Бальо Динев (име и фамилия)

Изпълнителен директор (длъжност на представляващия участника)

Дата: 05.10.2018г.

чл.2 33ЛД

чл.2 33ЛД



ЕВРОПЕЙСКИ СЪЮЗ



НАЦИОНАЛНА АГЕНЦИЯ
ЗА РЕГИОНАЛНО РАЗВИТИЕ
МНОГО ВЪЗМОЖНОСТИ

Приложение № 3

До
Администрация на Министерския съвет
София, бул. „Дондуков“ № 1

ЦЕНОВО ПРЕДЛОЖЕНИЕ

От участник: „ДАВИД Холдинг“ АД,
БУЛСТАТ/ЕИК 833092882, адрес гр. Казанлък, ул. „Стара река“ № 2, ДК „Арсенал“
офис 417

банкова сметка BG04UBBS88881000756115,
представяван от Бальо Атанасов Динев

УВАЖАЕМИ ДАМИ И ГОСПОДА,

Във връзка с обявената от Вас обществена поръчка по реда на Глава Двадесет и шеста от ЗОП с предмет: „Анализ и отстраняване на констатираните несъответствия в публичния модул и вътрешната среда на ИСУН за програмния период 2007-2013“,

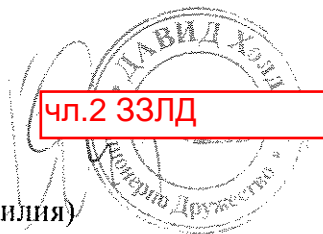
представяме нашата ценова оферта за изпълнение на обществената поръчка, както следва:

Общата предлагана от нас цена за изпълнение на поръчката възлиза на 69 690.00 (шестдесет и девет хиляди и шестстотин и деветдесет) лева без ДДС или 83 628.00 (осемдесет и три хиляди шестстотин двадесет и осем) лева с ДДС.

Декларирам, че посочената цена е крайна и включва всички разходи по изпълнение на поръчката.

Срокът на валидност на настоящата оферта е 3 (три) месеца след изтичане на срока за подаване на офертата

ПОДПИС и ПЕЧАТ:



Бальо Динев (име и фамилия)

Изпълнителен директор (длъжност на представляващия участника)

Дата: 05.10.2018г.

Плащане от/към бюджета

Документ ID: 17512205 Статус дата: 19/10/2018 15:35:28
 Референция: BSRBC1345144

Статус: Одобрен

Платете на - име на получателя:	
Администрация на Министерски съвет	
IBAN на получателя:	BIC на получателя:
BG38BNBG96613300157901	BNBNBGCS
При банка - име на банката на получателя (попълва се автоматично):	Вид плащане*
БЪЛГАРСКА НАРОДНА БАНКА	
*попълва се автоматично за сметки на администратори на приходи и на Централния бюджет	

ПРЕВОДНО НАРЕЖДАНЕ

за плащане от/към бюджета	Валута:	Сума в лева:
	BGN	3484.50

Словом:

Три хиляди четиристотин осемдесет и четири и 50 ст.

1	Вид плащане:	Сума:
		3484.50

Основание за плащане / внасяне - вид данък, такса, осигуровка, мито, лихва...:

Гаранция за изпълнение на договор

Още пояснения:

по Заповед ФС-104/15.10.2018

Вид и номер на документ, по който се плаща:

9

Дата на документа:

Период, за който се отнася плащането:

От:

До:

Задължено лице - наименование на юр. лице/трите имена на физ. лице 30 символа:

Давид Холдинг АД

ЕИК/код по БУЛСТАТ на задълж. лице:

В33092882

ЕГН на задълженото лице:

ЛНЧ на задълженото лице:

Наименование - име на наредителя:

ДАВИД ХОЛДИНГ АД

IBAN на наредителя:

BG04UBBS88881000756115

Валута:

BGN

BIC на наредителя:

UBBSBG33

Платежна система:

БИСЕРА

Вид плащане:

Дата на изпълнение:

За суми над 100 хил. лева преводът се насочва към RINGS, независимо от Вашия избор.

Статус: Дата на статус: Роль: Потребител

Създаден: 19/10/2018 15:32:23 А Йонко ДИМОВ ЙОНКОВ

Подписан: 19/10/2018 15:35:27 А Йонко ДИМОВ ЙОНКОВ

Схеми на подписи: А