



ЕВРОПЕЙСКИ СЪЮЗ



**ДОГОВОР  
ЗА ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНА ПОРЪЧКА**  
№ МС-88 / 01.07.2019 г.

Подписите са  
заличени на  
основание чл. 36а,  
ал. 3 от ЗОП

Днес, 01.07.....2019 г., в гр. София, между:

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

и

**„ДАВИД ХОЛДИНГ“ АД**, със седалище и адрес на управление: гр. Казанлък 6100, СТАРА РЕКА, Дом на културата Арсенал № 2, ет. 4, ап. 417, ЕИК 833092882, представлявано от БАЛЪО АТАНАСОВ ДИНЕВ, в качеството на изпълнителен директор, наричано за краткост **ИЗПЪЛНИТЕЛ**, от друга страна,  
(**ВЪЗЛОЖИТЕЛЯТ** и **ИЗПЪЛНИТЕЛЯТ** наричани заедно „**Страните**“, а всеки от тях поотделно „**Страна**“)

на основание чл. 112 и следващите от раздел II, Глава Тринадесета от ЗОП и във връзка със Заповед № ФС-57 от 30.05.2019 г. на директора на дирекция „Административно и правно обслужване и управление на собствеността“, за определяне на изпълнител на обществената поръчка с предмет: „**Осигуряване на поддръжка на ИСУН за програмния период 2007-2013**“ по бюджетна линия BG05SFOP001-4.005-0005 „Повишаване на ефективността и ефикасността на ЦКЗ 2019-2021 г.“, финансирана по Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд,

се сключи настоящият договор (**„Договора/договорът“**) за следното:

## I. ПРЕДМЕТ НА ДОГОВОРА.

**Чл. 1.** (1) **ВЪЗЛОЖИТЕЛЯТ** възлага, а **ИЗПЪЛНИТЕЛЯТ** приема да предостави срещу възнаграждение и при условията на този договор следните услуги: осигуряване на поддръжка на ИСУН за програмния период 2007-2013, наричани за краткост „Услугите“.

(2) **ИЗПЪЛНИТЕЛЯТ** се задължава да предостави услугите в съответствие с Техническата спецификация, Техническото предложение на **ИЗПЪЛНИТЕЛЯ** и Ценовото предложение на **ИЗПЪЛНИТЕЛЯ**, съставляващи съответно Приложения № 1, 2 и 3 към този Договор (**„Приложенията“**) и представляващи неразделна част от него.

**Чл. 2.** В срок до 10 (десет) дни от датата на сключване на договора, но най-късно преди започване на неговото изпълнение, **ИЗПЪЛНИТЕЛЯТ** уведомява **ВЪЗЛОЖИТЕЛЯ** за името, данните за контакт и представителите на подизпълнителите, посочени в офертата на **ИЗПЪЛНИТЕЛЯ**. **ИЗПЪЛНИТЕЛЯТ** уведомява **ВЪЗЛОЖИТЕЛЯ** за всякакви промени в предоставената информация в хода на изпълнението на договора в срок до 10 (десет) дни от настъпване на съответното обстоятелство. (ако е приложимо)

## II. СРОК НА ДОГОВОРА. СРОК И МЯСТО НА ИЗПЪЛНЕНИЕ.

**Чл. 3.** Договорът влиза в сила от датата на сключването му.

**Чл. 4.** Срокът за изпълнение на Услугите е до 31.12.2021 г.

**Чл. 5.** Мястото на изпълнение на договора е Република България, гр. София, Администрация на Министерския съвет, Централно координационно звено.

### **III. ЦЕНА, РЕД И СРОКОВЕ ЗА ПЛАЩАНЕ.**

**Чл. 6. (1)** За предоставяне на Услугите, ВЪЗЛОЖИТЕЛЯТ се задължава да плати на ИЗПЪЛНИТЕЛЯ обща цена в размер 296 280,00 (двеста деветдесет и шест хиляди двеста и осемдесет) лв. без ДДС и 355 536,00 (триста петдесет и пет хиляди петстотин тридесет и шест) лева с ДДС (наричана по-нататък „Цената“ или „Стойността на Договора“), изчислена на база на абонаментната цена за услугата за 1 месец, съгласно Ценовото предложение на ИЗПЪЛНИТЕЛЯ, съставляващо Приложение № 3, за срока по чл. 4.

(2) В Цената по ал. 1 са включени всички разходи на ИЗПЪЛНИТЕЛЯ за изпълнение на Услугите и за неговите подизпълнители (ако е приложимо). ВЪЗЛОЖИТЕЛЯТ не дължи заплащането на каквито и да е други разноски, направени от ИЗПЪЛНИТЕЛЯ.

(3) Цената, посочена в ал. 1 е крайна за изпълнение на договора и не подлежи на промяна, освен в случаите, предвидени в ЗОП.

**Чл. 7. (1)** ВЪЗЛОЖИТЕЛЯТ плаща на ИЗПЪЛНИТЕЛЯ цената по този Договор на тримесечна база в срок до 30 (тридесет) дни след двустранно подписване на приемо-предавателен протокол за изтеклото тримесечие, с който се удостоверява, че предоставената услуга е извършена качествено и в срок, и след представяне на фактура.

(2) ВЪЗЛОЖИТЕЛЯТ плаща на ИЗПЪЛНИТЕЛЯ последното плащане в срок до 30 (тридесет) дни след двустранно подписване на окончателния приемо-предавателен протокол, съгласно чл. 27, ал. 5 от Договора, с който се удостоверява, че предоставената услуга е извършена качествено и в срок, и след представяне на фактура.

(3) За ВЪЗЛОЖИТЕЛЯ протоколите по ал. 1 и 2 и фактурите се подписват от отговорните лица, съгласно чл. 27, ал. 7 от настоящия Договор.

(4) При извършване на плащанията ВЪЗЛОЖИТЕЛЯТ има право да прихване от дължимата сума, дължими от ИЗПЪЛНИТЕЛЯ неустойки за забавено или неточно изпълнение и/или други изискуеми суми.

**Чл. 8. (1)** Всички плащания по този Договор се извършват в лева чрез банков превод по следната банкова сметка на ИЗПЪЛНИТЕЛЯ:

ТИТУЛЯР: ДАВИД ХОЛДИНГ АД  
БАНКА: ОББ АД  
IBAN: BG04 UBBS 8888 1000 7561 15  
BIC: UBBSBGSF

(2) ИЗПЪЛНИТЕЛЯТ е длъжен да уведомява писмено ВЪЗЛОЖИТЕЛЯ за всички последващи промени по ал. 1 в срок от 3 работни дни (три работни) дни, считано от момента на промяната. В случай че ИЗПЪЛНИТЕЛЯТ не уведоми ВЪЗЛОЖИТЕЛЯ в този срок, счита се, че плащанията са надлежно извършени.

### **V. ГАРАНЦИЯ ЗА ИЗПЪЛНЕНИЕ**

**Чл. 9. (1)** При подписването на този Договор, ИЗПЪЛНИТЕЛЯТ представя на ВЪЗЛОЖИТЕЛЯ гаранция за изпълнение в размер на 5 % (пет на сто) от Стойността на Договора без ДДС, а именно 14 814,00 (четирнадесет хиляди осемстотин и

четирнадесет) лева („Гаранцията за изпълнение“), която служи за обезпечаване на изпълнението на Договора.

**Чл. 10.** (1) В случай на изменение на Договора, извършено в съответствие с този Договор и приложимото право, включително когато изменението е свързано с индексирание на Цената, ИЗПЪЛНИТЕЛЯТ се задължава да предприеме необходимите действия за привеждане на Гаранцията за изпълнение в съответствие с изменените условия на Договора, в срок до 5 (пет) работни дни от подписването на допълнително споразумение за изменението.

(2) Действията за привеждане на Гаранцията за изпълнение в съответствие с изменените условия на Договора могат да включват, по избор на ИЗПЪЛНИТЕЛЯ:

1. внасяне на допълнителна парична сума по банковата сметка на ВЪЗЛОЖИТЕЛЯ, при спазване на изискванията на чл. 11 от Договора; и/или;

2. предоставяне на документ за изменение на първоначалната банкова гаранция или нова банкова гаранция, при спазване на изискванията на чл. 12 от Договора; и/или

3. предоставяне на документ за изменение на първоначалната застраховка или нова застраховка, при спазване на изискванията на чл. 13 от Договора.

**Чл. 11.** Когато като Гаранция за изпълнение се представя парична сума, сумата се внася по следната банкова сметка на ВЪЗЛОЖИТЕЛЯ:

Банка: БНБ

BIC: BNBGBGSD

IBAN: BG38BNBG96613300157901

**Чл. 12.** (1) Когато като гаранция за изпълнение се представя банкова гаранция, ИЗПЪЛНИТЕЛЯТ предава на ВЪЗЛОЖИТЕЛЯ оригинален екземпляр на банкова гаранция, издадена в полза на ВЪЗЛОЖИТЕЛЯ, която трябва да отговаря на следните изисквания:

1. да бъде безусловна и неотменяема банкова гаранция, във форма, предварително съгласувана с ВЪЗЛОЖИТЕЛЯ и да съдържа задължение на банката - гарант да извърши плащане при първо писмено искане от ВЪЗЛОЖИТЕЛЯ, деклариращ, че е налице неизпълнение на задължение на ИЗПЪЛНИТЕЛЯ или друго основание за задържане на Гаранцията за изпълнение по този Договор;

2. да бъде със срок на валидност за целия срок на действие на Договора плюс 60 (шестдесет) дни след крайния срок на Договора, като при необходимост срокът на валидност на банковата гаранция се удължава или се издава нова.

(2) Банковите разходи по откриването и поддържането на Гаранцията за изпълнение във формата на банкова гаранция, както и по усвояването на средства от страна на ВЪЗЛОЖИТЕЛЯ, при наличието на основание за това, са за сметка на ИЗПЪЛНИТЕЛЯ.

**Чл. 13.** (1) Когато като Гаранция за изпълнение се представя застраховка, ИЗПЪЛНИТЕЛЯТ предава на ВЪЗЛОЖИТЕЛЯ оригинален екземпляр на застрахователна полица, издадена в полза на ВЪЗЛОЖИТЕЛЯ, в която ВЪЗЛОЖИТЕЛЯТ е посочен като трето ползващо се лице (бенефициер), която трябва да отговаря на следните изисквания:

1. да обезпечава изпълнението на този Договор чрез покритие на отговорността на ИЗПЪЛНИТЕЛЯ;

2. да бъде със срок на валидност за целия срок на действие на Договора плюс 60 (шестдесет) дни след крайния срок на Договора.

(2) Разходите по сключването на застрахователния договор и поддържането на валидността на застраховката за изисквания срок, както и по всяко изплащане на застрахователно обезщетение в полза на ВЪЗЛОЖИТЕЛЯ, при наличието на основание за това, са за сметка на ИЗПЪЛНИТЕЛЯ.

**Чл. 14.** (1) ВЪЗЛОЖИТЕЛЯТ освобождава Гаранцията за изпълнение в срок до 30 (тридесет) дни след приключване на изпълнението на Договора и окончателно му приемане в пълен размер, ако липсват основания за задържането от страна на ВЪЗЛОЖИТЕЛЯ на каквато и да е сума по нея.

(2) Освобождаването на Гаранцията за изпълнение се извършва, както следва:

1. когато е във формата на парична сума – чрез превеждане на сумата по банковата сметка на ИЗПЪЛНИТЕЛЯ, посочена в чл. 8 от Договора;

2. когато е във формата на банкова гаранция – чрез връщане на нейния оригинал на представител на ИЗПЪЛНИТЕЛЯ или упълномощено от него лице;

3. когато е във формата на застраховка – чрез връщане на оригинала на застрахователната полица/застрахователния сертификат на представител на ИЗПЪЛНИТЕЛЯ или упълномощено от него лице /изпращане на писмено уведомление до застрахователя.

(3) Гаранцията или съответната част от нея не се освобождава от ВЪЗЛОЖИТЕЛЯ, ако в процеса на изпълнение на Договора е възникнал спор между Страните относно неизпълнение на задълженията на ИЗПЪЛНИТЕЛЯ и въпросът е отнесен за решаване пред съд. При решаване на спора в полза на ВЪЗЛОЖИТЕЛЯ той може да пристъпи към усвояване на гаранциите.

**Чл. 15.** ВЪЗЛОЖИТЕЛЯТ има право да задържи съответна част и да се удовлетвори от Гаранцията за изпълнение, когато ИЗПЪЛНИТЕЛЯТ не изпълни някое от неговите задължения по Договора, както и в случаите на лошо, частично и забавено изпълнение на което и да е задължение на ИЗПЪЛНИТЕЛЯ, като усвои такава част от Гаранцията за изпълнение, която съответства на уговорената в Договора неустойка за съответния случай на неизпълнение.

**Чл. 16.** ВЪЗЛОЖИТЕЛЯТ има право да задържи Гаранцията за изпълнение в пълен размер, в следните случаи:

1. при пълно неизпълнение, в т.ч. когато изпълнението на договора не отговаря на изискванията на ВЪЗЛОЖИТЕЛЯ, и разваляне на Договора от страна на ВЪЗЛОЖИТЕЛЯ на това основание;

2. при прекратяване на дейността на ИЗПЪЛНИТЕЛЯ или при обявяването му в несъстоятелност.

**Чл. 17.** Във всеки случай на задържане на Гаранцията за изпълнение, ВЪЗЛОЖИТЕЛЯТ уведомява ИЗПЪЛНИТЕЛЯ за задържането и неговото основание. Задържането на Гаранцията за изпълнение изцяло или частично не изчерпва правата на ВЪЗЛОЖИТЕЛЯ да търси обезщетение в по-голям размер.

**Чл. 18.** Когато ВЪЗЛОЖИТЕЛЯТ се е удовлетворирил от Гаранцията за изпълнение и Договорът продължава да е в сила, ИЗПЪЛНИТЕЛЯТ се задължава в срок до 10 (десет) дни да допълни Гаранцията за изпълнение, като внесе усвоената от ВЪЗЛОЖИТЕЛЯ сума по сметката на ВЪЗЛОЖИТЕЛЯ или предостави документ за изменение на първоначалната банкова гаранция или нова банкова гаранция, съответно застраховка, така че във всеки момент от действието на Договора размерът на Гаранцията за изпълнение да бъде в съответствие с чл. 9 от Договора.

**Чл. 19.** ВЪЗЛОЖИТЕЛЯТ не дължи лихва за времето, през което средствата по Гаранцията за изпълнение са престояли при него законосъобразно.

## **V. ПРАВА И ЗАДЪЛЖЕНИЯ НА СТРАНИТЕ**

**Чл. 20.** Изброяването на конкретни права и задължения на Страните в този раздел от Договора е неизчерпателно и не засяга действието на други клаузи от Договора или

от приложимото право, предвиждащи права и/или задължения на която и да е от Страните.

**Чл. 21. ИЗПЪЛНИТЕЛЯТ има право:**

1. да получи възнаграждение в размера, сроковете и при условията по чл. 6 – 8 от Договора;

2. да иска и да получава от ВЪЗЛОЖИТЕЛЯ необходимото съдействие за изпълнение на задълженията по този Договор, както и всички необходими документи, информация и данни, пряко свързани или необходими за изпълнение на Договора.

**Чл. 22. ИЗПЪЛНИТЕЛЯТ се задължава:**

1. да предостави Услугите и да изпълнява задълженията си по този Договор в уговорените срокове и качествено, в съответствие с Договора и Приложенията;

2. да информира своевременно ВЪЗЛОЖИТЕЛЯ за всички пречки, възникващи в хода на изпълнението на работа, да предложи начин за отстраняването им, като може да поиска от ВЪЗЛОЖИТЕЛЯ указания и/или съдействие за отстраняването им;

3. да изпълнява всички законосъобразни указания и изисквания на ВЪЗЛОЖИТЕЛЯ;

4. да пази поверителна Конфиденциалната информация, в съответствие с уговореното в чл. 40 от Договора;

5. да не възлага работата или части от нея на подизпълнители, извън посочените в офертата на ИЗПЪЛНИТЕЛЯ освен в случаите и при условията, предвидени в ЗОП; *(ако е приложимо)*

6. да сключи договор/договори за подизпълнение с посочените в офертата му подизпълнители в срок от 10 (десет) дни от сключване на настоящия Договор. В срок до 3 (три) дни от сключването на договор за подизпълнение или на допълнително споразумение за замяна на посочен в офертата подизпълнител ИЗПЪЛНИТЕЛЯТ изпраща копие на договора или на допълнителното споразумение на ВЪЗЛОЖИТЕЛЯ заедно с доказателства, че са изпълнени условията по чл. 66, ал. 2 и 14 ЗОП *(ако е приложимо)*.

7. да участва във всички работни срещи, свързани с изпълнението на този Договор;

8. 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;

9. да допуска ВЪЗЛОЖИТЕЛЯ и лица, упълномощени от него, както и всички компетентни органи, съгласно действащото законодателство да проверяват или одитират по всяко време документите и сметките, свързани с дейността по договора.

10. 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, одитна проследимост и проверка;

11. при поискване от ВЪЗЛОЖИТЕЛЯ, органите по чл. 9 и 11 от ЗУСЕСИФ, Европейската комисия или Европейската сметна палата, както и други национални или европейски органи и институции с контролни или регулаторни функции, 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;

12. да съхранява всички документи, свързани с изпълнението на договора за срок от една година след закриването на оперативната програма или за период от три години след годината, през която е извършено частично закриване. Сроковете спират да текат в

случай на съдебни процедури или по искане ВЪЗЛОЖИТЕЛЯ, или на посочените в предходната алинея институции;

13. при всички дейности, за които е приложимо, ИЗПЪЛНИТЕЛЯТ следва да осигурява публичност и информираност по отношение на финансирането на настоящия договор. ИЗПЪЛНИТЕЛЯТ следва да използва емблемата на ЕС във всички обяви или публикации, свързани с договора. ИЗПЪЛНИТЕЛЯТ е длъжен да оповести, че договорът е получил финансиране от Европейския социален фонд (ЕСФ) чрез Оперативна програма „Добро управление” (ОПДУ). Изготвените материали следва ясно да отразяват финансовия принос на ОПДУ, спазвайки горните изисквания. Финансовият принос на ОПДУ следва да бъде ясно демонстриран по подходящ начин при изпълнението на всяка една от дейностите по проекта. Приложението следва ясно да демонстрира ролята на ОПДУ за изграждането на системата и да визуализира всички изискуеми логотипа, както и надписите показващи финансовия принос на ЕС.

14. при изпълнение на предмета на поръчката да се съобрази с изискванията за визуална идентификация, определени в „Единен наръчник на бенефициента за прилагане на правилата за информация и комуникация 2014-2020“, публикуван на следния интернет адрес:

<https://www.eufunds.bg/index.php/bg/programen-period-2014-2020/operativni-programi-2014-2020/operativna-programa-dobro-upravlenie-2014-2020/narachnici-rakovodstva-pravila/item/14878-iziskvaniya-za-informatziya-i-publichnost>

**Чл. 23. ВЪЗЛОЖИТЕЛЯТ има право:**

1. да изисква и да получи изпълнението на предмета на договора в уговорения срок, количество и качество;

2. да контролира изпълнението на поетите от ИЗПЪЛНИТЕЛЯ задължения, в т.ч. да иска и да получава информация от ИЗПЪЛНИТЕЛЯ през целия Срок на Договора, или да извършва проверки, при необходимост и на мястото на изпълнение на Договора, но без с това да пречи на изпълнението;

3. да изисква, при необходимост и по своя преценка, обосновка от страна на ИЗПЪЛНИТЕЛЯ на изготвените от него доклади или съответна част от тях;

3. с писмено мотивирано искане да поиска замяна, ако прецени, че даден експерт от персонала на ИЗПЪЛНИТЕЛЯ, който ще отговаря за изпълнение на Услугите, работи неефективно или не изпълнява задълженията си по Договора;

4. да изисква от ИЗПЪЛНИТЕЛЯ преработване или доработване на всеки от докладите, в съответствие с уговореното в чл. 27, ал. 4 от Договора.

**Чл. 24. ВЪЗЛОЖИТЕЛЯТ се задължава:**

1. да приеме изпълнението, когато отговаря на договореното, по реда и при условията на този Договор;

2. да заплати на ИЗПЪЛНИТЕЛЯ Цената в размера, по реда и при условията, предвидени в този Договор;

3. да предостави и осигури достъп на ИЗПЪЛНИТЕЛЯ до информацията, необходима за изпълнение на предмета на Договора, при спазване на относимите изисквания или ограничения съгласно приложимото право;

4. да пази поверителна Конфиденциалната информация, в съответствие с уговореното в чл. 40 от Договора;

5. да оказва съдействие на ИЗПЪЛНИТЕЛЯ във връзка с изпълнението на този Договор, включително и за отстраняване на възникнали пречки пред изпълнението на Договора, когато ИЗПЪЛНИТЕЛЯТ поиска това;

6. да освободи представената от ИЗПЪЛНИТЕЛЯ Гаранция за изпълнение, съгласно клаузите на чл. 9-19 от Договора.



## VI. ЕКИП НА ИЗПЪЛНИТЕЛЯ

**Чл. 25.** ИЗПЪЛНИТЕЛЯТ е длъжен да осъществява дейностите – предмет на договора с експертите от списъка на персонала, който ще изпълнява поръчката и/или на членовете на ръководния състав, които ще отговарят за изпълнението.

**Чл. 26.** (1) За работата, действията и бездействията на екипа на ИЗПЪЛНИТЕЛЯ, във връзка с изпълнението на договора, ИЗПЪЛНИТЕЛЯТ отговаря като за своя работа, действия и бездействия, като пред ВЪЗЛОЖИТЕЛЯ, така и пред трети лица. ИЗПЪЛНИТЕЛЯТ носи отговорност за качеството на експертите, които предлага на разположение на ВЪЗЛОЖИТЕЛЯ.

(2) ИЗПЪЛНИТЕЛЯТ няма право да заменя и/или да допуска оттеглянето или замяната на експертите.

(3) Оттегляне на експерт се допуска само по сериозни здравословни или други причини, които не позволяват на експерта да продължи да работи по изпълнението на поръчката.

(4) В случая по ал. 3, ИЗПЪЛНИТЕЛЯТ е длъжен своевременно да осигури нов професионална квалификация, съответстваща на изискванията на възложителя, посочени в обявлението за обществена поръчка. В случаите на неодобрение от ВЪЗЛОЖИТЕЛЯ на предложен експерт, ИЗПЪЛНИТЕЛЯТ предлага на негово място друга кандидатура.

(5) Оттеглянето, замяната и привличането на експерти е допустимо само с писмено съгласие на ВЪЗЛОЖИТЕЛЯ.

(6) При никакви обстоятелства замяната на експерти и привличането на допълнителни експерти (включително и спомагателен персонал) не е основание за искане и получаване на каквото и да е друго допълнително плащане, извън цената по чл. 4.

(7) По време на изпълнение на Договора и с писмено мотивирано искане, ВЪЗЛОЖИТЕЛЯТ може да поиска замяна, ако прецени, че даден експерт работи неефективно или не изпълнява задълженията си по Договора.

(8) При възникнали допълнителни разходи от замяната на експерт, разходите и отговорността се понасят от ИЗПЪЛНИТЕЛЯ.

## VII. ПРЕДАВАНЕ И ПРИЕМАНЕ НА ИЗПЪЛНЕНИЕТО

**Чл. 27.** (1) За отчитане на извършените дейности, ИЗПЪЛНИТЕЛЯТ изготвя доклади на период от 3 месеца, описващи всички извършени дейности по поддръжката за отчетния период, с приложена версия на продукта на CD/DVD/Flash memory носител в заредима фаза, както и напълно документиран и актуален сорс-код, стандартен съпътстващ софтуер, ако е необходим за нормалната работа на системата, и пълна техническа документация, ако през отчетния период е извършена промяна на версията на ИСУН.

(2) Докладите по ал. 1 следва да съдържат:

1. Брой предоставени услуги по поддръжка;
2. Описание на предоставените услуги;
3. Информация за неразрешени искания, ако е приложимо.

(3) Междинните доклади по ал. 1 се приемат от ВЪЗЛОЖИТЕЛЯ с двустранен, предавателно-приемателен протокол, с който се удостоверява, че предоставената услуга е извършена качествено.

(4) ВЪЗЛОЖИТЕЛЯТ има право:

1. да приеме изпълнението, когато отговаря на договореното;

2. да поиска преработване и/или допълване на докладите в определен от него срок, като в такъв случай преработването и/или допълването се извършва в указан от ВЪЗЛОЖИТЕЛЯ срок и е изцяло за сметка на ИЗПЪЛНИТЕЛЯ. Когато бъдат установени несъответствия на изпълнението с уговореното или бъдат констатирани недостатъци, ВЪЗЛОЖИТЕЛЯТ може да откаже приемане на изпълнението до отстраняване на недостатъците, като даде подходящ срок за отстраняването им за сметка на ИЗПЪЛНИТЕЛЯ, който не може да бъде по-дълъг от 5 (пет) работни дни;

3. да откаже да приеме изпълнението при съществени отклонения от договореното в случай че констатираните недостатъци са от такова естество, че не могат да бъдат отстранени в рамките на срока за изпълнение по Договора и резултатът от изпълнението става безполезен за ВЪЗЛОЖИТЕЛЯ.

(5) Окончателното приемане на изпълнението на Услугите по този Договор се извършва с подписване на окончателен Приемо-предавателен протокол, подписан от Страните в срок до 1 (един) месец след изтичането на срока на Договора. В случай че към този момент бъдат констатирани недостатъци в изпълнението, те се описват в окончателния приемо-предавателен протокол и се определя подходящ срок за отстраняването им или налагането на санкция, съгласно чл. 28 – 32 от Договора.

(6) Приемо-предавателните протоколи се подписват от представители на ВЪЗЛОЖИТЕЛЯ и ИЗПЪЛНИТЕЛЯ в два оригинални екземпляра – по един за всяка от Страните.

(7) Лицата, които ще подписват приемо-предавателните протоколи и ще контролират изпълнението на Договора са, както следва:

за ИЗПЪЛНИТЕЛЯ: Стойчо Недев Стойчев, Технически директор ДАВИД Холдинг АД, тел. 0888 573709, e-mail: [snedev@david.bg](mailto:snedev@david.bg)

за ВЪЗЛОЖИТЕЛЯ: Севдалина Иванова - главен сътрудник по УЕПП, Отдел „Информационни системи” Дирекция „Централно координационно звено”, Администрация на Министерския съвет, тел.: 02/9402969, e-mail: [s.ivanova@government.bg](mailto:s.ivanova@government.bg)

## VIII. САНКЦИИ ПРИ НЕИЗПЪЛНЕНИЕ

**Чл. 28.** При просрочване изпълнението на задълженията по този Договор, неизправната Страна дължи на изправната неустойка в размер на 0,5 % (нула цяло и пет на сто) от цената на Договора за всеки ден забава, но не повече от 10 % (десет на сто) от стойността на договора.

**Чл. 29.** При констатирано лошо или друго неточно или частично изпълнение на отделна дейност или при отклонение от изискванията на ВЪЗЛОЖИТЕЛЯ, посочени в Техническата спецификация, ВЪЗЛОЖИТЕЛЯТ има право да поиска от ИЗПЪЛНИТЕЛЯ да изпълни изцяло и качествено съответната дейност, без да дължи допълнително възнаграждение за това. В случай че и повторното изпълнение е некачествено, ВЪЗЛОЖИТЕЛЯТ има право да задържи гаранцията за изпълнение и да прекрати договора.

**Чл. 30.** При разваляне на Договора поради виновно неизпълнение на някоя от Страните, виновната Страна дължи неустойка в размер на 10 % (десет на сто) от Стойността на Договора



**Чл. 31.** ВЪЗЛОЖИТЕЛЯТ има право да удържи всяка дължима по този договор неустойка чрез задържане на сума от Гаранцията за изпълнение, като уведоми писмено ИЗПЪЛНИТЕЛЯ за това.

**Чл. 32.** Плащането на неустойките, уговорени в този Договор, не ограничава правото на изправната страна да търси реално изпълнение и/или обезщетение за понесени вреди и пропуснати ползи в по-голям размер, съгласно приложимото право.

### **VIII. ПРЕКРАТЯВАНЕ НА ДОГОВОРА**

**Чл. 33.** Този Договор се прекратява:

1. с изтичане на срока на Договора;
2. с изпълнението на всички задължения на Страните по него;
3. при настъпване на пълна обективна невъзможност за изпълнение, за което обстоятелство засегнатата Страна е длъжна да уведоми другата Страна в срок до 5 (пет) работни дни от настъпване на невъзможността и да представи доказателства;
4. при прекратяване на юридическо лице – Страна по Договора без правопримство, по смисъла на законодателството на държавата, в която съответното лице е установено;
5. при условията по чл. 5, ал. 1, т. 3 от ЗИФОДРЮПДРКТЛТДС.

**Чл. 34.** Договорът може да бъде прекратен

1. по взаимно съгласие на Страните, изразено в писмена форма;
2. когато за ИЗПЪЛНИТЕЛЯ бъде открито производство по несъстоятелност или ликвидация – по искане на всяка от Страните.

**Чл. 35.** (1) Всяка от Страните може да развали Договора при виновно неизпълнение на съществено задължение на другата страна по Договора, при условията и с последиците съгласно чл. 87 и сл. от Закона за задълженията и договорите, чрез отправяне на писмено предупреждение от изправната Страна до неизправната и определяне на подходящ срок за изпълнение. Разваляне на Договора не се допуска, когато неизпълнената част от задължението е незначителна с оглед на интереса на изправната Страна.

(2) За целите на този Договор, Страните ще считат за виновно неизпълнение на съществено задължение на ИЗПЪЛНИТЕЛЯ всеки от следните случаи:

1. когато ИЗПЪЛНИТЕЛЯТ не е започнал изпълнението на Услугите в срок до 10 (десет) дни, считано от датата на влизане в сила;
2. ИЗПЪЛНИТЕЛЯТ е прекратил изпълнението на Услугите за повече от 10 (десет) дни;
3. ИЗПЪЛНИТЕЛЯТ е допуснал съществено отклонение от Условията за изпълнение на поръчката, Техническата спецификация и Техническото предложение.

(3) ВЪЗЛОЖИТЕЛЯТ може да развали Договора само с писмено уведомление до ИЗПЪЛНИТЕЛЯ и без да му даде допълнителен срок за изпълнение, ако поради забава на ИЗПЪЛНИТЕЛЯ то е станало безполезно или ако задължението е трябвало да се изпълни непременно в уговореното време.

**Чл. 36.** ВЪЗЛОЖИТЕЛЯТ прекратява Договора в случаите по чл. 118, ал. 1 от ЗОП, без да дължи обезщетение на ИЗПЪЛНИТЕЛЯ за претърпени от прекратяването на Договора вреди, освен ако прекратяването е на основание чл. 118, ал. 1, т. 1 от ЗОП. В последния случай, размерът на обезщетението се определя в протокол или споразумение, подписано от Страните, а при непостигане на съгласие – по реда на клаузата за разрешаване на спорове по този Договор.

**Чл. 37.** Във всички случаи на прекратяване на Договора, освен при прекратяване на юридическо лице – Страна по Договора без правопримство:

1. ВЪЗЛОЖИТЕЛЯТ и ИЗПЪЛНИТЕЛЯТ съставят констативен протокол за извършената към момента на прекратяване работа и размера на евентуално дължимите плащания; и

2. ИЗПЪЛНИТЕЛЯТ се задължава:

а) да предаде на ВЪЗЛОЖИТЕЛЯ всички документи, изготвени от него в изпълнение на Договора до датата на прекратяването; и

б) да върне на ВЪЗЛОЖИТЕЛЯ всички документи и материали, които са собственост на ВЪЗЛОЖИТЕЛЯ и са били предоставени на ИЗПЪЛНИТЕЛЯ във връзка с предмета на Договора.

## Х. ОБЩИ РАЗПОРЕДБИ

### Дефинирани понятия и тълкуване

**Чл. 38.** (1) Освен ако са дефинирани изрично по друг начин в този Договор, използваните в него понятия имат значението, дадено им в ЗОП, съответно в легалните дефиниции в Допълнителните разпоредби на ЗОП или, ако няма такива за някои понятия – според значението, което им се придава в основните разпоредби на ЗОП.

(2) При противоречие между различни разпоредби или условия, съдържащи се в договора и приложенията, се прилагат следните правила:

1. специалните разпоредби имат предимство пред общите разпоредби;

2. разпоредбите на приложенията имат предимство пред разпоредбите на Договора.

### Спазване на приложими норми

**Чл. 39.** При изпълнението на Договора, ИЗПЪЛНИТЕЛЯТ [и неговите подизпълнители] е длъжен [са длъжни] да спазва[т] всички приложими нормативни актове, разпоредби, стандарти и други изисквания, свързани с предмета на Договора, и в частност, всички приложими правила и изисквания, свързани с опазване на околната среда, социалното и трудовото право, приложими колективни споразумения и/или разпоредби на международното екологично, социално и трудово право, съгласно Приложение № 10 към чл. 115 от ЗОП.

### Конфиденциалност

**Чл. 40.** (1) Всяка от Страните по този Договор се задължава да пази в поверителност и да не разкрива или разпространява информация за другата Страна, станала ѝ известна при или по повод изпълнението на Договора („Конфиденциална информация“). Конфиденциална информация включва, без да се ограничава до: обстоятелства, свързани с търговската дейност, техническите процеси, проекти или финанси на Страните, както и ноу-хау, изобретения, полезни модели или други права от подобен характер, свързани с изпълнението на Договора. Не се смята за конфиденциална информацията, касаеща наименованието на изпълнения проект, стойността и предмета на този Договор, с оглед бъдещо позоваване на придобит професионален опит от ИЗПЪЛНИТЕЛЯ.

Дефиниция: Конфиденциална информация включва, без да се ограничава до: всякаква финансова, търговска, техническа или друга информация, анализи, съставени материали, изследвания, документи или други материали, свързани с бизнеса, управлението или дейността на другата Страна, от каквото и да е естество или в каквато и да е форма, включително, финансови и оперативни резултати, пазари, настоящи или потенциални клиенти, собственост, методи на работа, персонал, договори, ангажименти, правни въпроси или стратегии, продукти, процеси, свързани с документация, чертежи, спецификации, диаграми, планове, уведомления, данни, образци, модели, мостри, софтуер, софтуерни приложения, компютърни устройства или други материали или

записи или друга информация, независимо дали в писмен или устен вид, или съдържаща се на компютърен диск или друго устройство.

(2) С изключение на случаите, посочени в ал. 3 на този член, Конфиденциална информация може да бъде разкривана само след предварително писмено одобрение от другата Страна, като това съгласие не може да бъде отказано безпричинно.

(3) Не се счита за нарушение на задълженията за неразкриване на Конфиденциална информация, когато:

1. информацията е станала или става публично достъпна, без нарушаване на този Договор от която и да е от Страните;

2. информацията се изисква по силата на закон, приложим спрямо която и да е от Страните; или

3. предоставянето на информацията се изисква от регулаторен или друг компетентен орган и съответната Страна е длъжна да изпълни такова изискване;

В случаите по точки 2 или 3 Страната, която следва да предостави информацията, уведомява незабавно другата Страна по Договора.

(4) Задълженията по този член се отнасят както до ИЗПЪЛНИТЕЛЯ, така и до всички негови подразделения, контролирани от него фирми и организации, всички негови служители и наети от него физически или юридически лица, като ИЗПЪЛНИТЕЛЯТ отговаря за изпълнението на тези задължения от страна на такива лица.

(5) Задълженията, свързани с неразкриване на Конфиденциалната информация остават в сила и след прекратяване на Договора на каквото и да е основание.

#### Публични изявления

**Чл. 41.** ИЗПЪЛНИТЕЛЯТ няма право да дава публични изявления и съобщения, да разкрива или разгласява каквато и да е информация, която е получил във връзка с извършване на Услугите, предмет на този Договор, независимо дали е въз основа на данни и материали на ВЪЗЛОЖИТЕЛЯ или на резултати от работата на ИЗПЪЛНИТЕЛЯ, без предварителното писмено съгласие на ВЪЗЛОЖИТЕЛЯ, което съгласие няма да бъде безпричинно отказано или забавено.

#### Авторски права

**Чл. 42.** (1) Страните се съгласяват, на основание чл. 42, ал. 1 от Закона за авторското право и сродните му права, че авторските права върху всички документи и материали, и всякакви други елементи или компоненти, създадени в резултат на или във връзка с изпълнението на Договора, принадлежат изцяло на ВЪЗЛОЖИТЕЛЯ в същия обем, в който биха принадлежали на автора. ИЗПЪЛНИТЕЛЯТ декларира и гарантира, че трети лица не притежават права върху изготвените документи и други резултати от изпълнението на Договора, които могат да бъдат обект на авторско право.

(2) В случай че бъде установено с влязло в сила съдебно решение или в случай че ВЪЗЛОЖИТЕЛЯТ и/или ИЗПЪЛНИТЕЛЯТ установят, че с изготвянето, въвеждането и използването на документи или други материали, съставени при изпълнението на този Договор, е нарушено авторско право на трето лице, ИЗПЪЛНИТЕЛЯТ се задължава да направи възможно за ВЪЗЛОЖИТЕЛЯ използването им:

1. чрез промяна на съответния документ или материал; или

2. чрез замяната на елемент от него със защитени авторски права с друг елемент със същата функция, който не нарушава авторските права на трети лица; или

3. като получи за своя сметка разрешение за ползване на продукта от третото лице, чиито права са нарушени.

(3) ВЪЗЛОЖИТЕЛЯТ уведомява ИЗПЪЛНИТЕЛЯ за претенциите за нарушени авторски права от страна на трети лица в срок до 10 (десет) дни от узнаването им. В

случай че трети лица предявят основателни претенции, ИЗПЪЛНИТЕЛЯТ носи пълната отговорност и понася всички щети, произтичащи от това. ВЪЗЛОЖИТЕЛЯТ привлича ИЗПЪЛНИТЕЛЯ в евентуален спор за нарушено авторско право във връзка с изпълнението по Договора.

(4) ИЗПЪЛНИТЕЛЯТ заплаща на ВЪЗЛОЖИТЕЛЯ обезщетение за претърпените вреди и пропуснатите ползи вследствие на окончателно признато нарушение на авторски права на трети лица.

#### Прехвърляне на права и задължения

**Чл. 43.** Никоя от Страните няма право да прехвърля никое от правата и задълженията, произтичащи от този Договор, без съгласието на другата Страна. Паричните вземания по Договора могат да бъдат прехвърляни или залагани съгласно приложимото право.

#### Изменения

**Чл. 44.** Този Договор може да бъде изменян само с допълнителни споразумения, изготвени в писмена форма и подписани от двете Страни, в съответствие с изискванията и ограниченията на ЗОП.

#### Непреодолима сила

**Чл. 45.** (1) Никоя от Страните по този Договор не отговаря за неизпълнение, причинено от непреодолима сила. За целите на този Договор, „непреодолима сила“ има значението на това понятие по смисъла на чл. 306, ал. 2 от Търговския закон.

(2) Не може да се позовава на непреодолима сила Страна, която е била в забава към момента на настъпване на обстоятелството, съставляващо непреодолима сила.

(3) Страната, която не може да изпълни задължението си поради непреодолима сила, е длъжна да предприеме всички действия с грижата на добър стопанин, за да намали до минимум понесените вреди и загуби, както и да уведоми писмено другата страна в срок до 3 дни от настъпването на непреодолимата сила, като посочи в какво се състои непреодолимата сила и възможните последици от нея за изпълнението на Договора. При неуведомяване се дължи обезщетение за настъпилите от това вреди.

(4) Докато трае непреодолимата сила, изпълнението на задълженията на свързаните с тях насрещни задължения се спира.

#### Нисщожност на отделни клаузи

**Чл. 46.** В случай че някоя от клаузите на този Договор е недействителна или неприложима, това не засяга останалите клаузи. Недействителната или неприложима клауза се замества от повелителна правна норма, ако има такава.

#### Уведомления

**Чл. 47.** (1) Всички уведомления между Страните във връзка с този Договор се извършват в писмена форма и могат да се предават лично или чрез препоръчано писмо, по куриер, по факс, електронна поща.

(2) За целите на този Договор данните и лицата за контакт на Страните са както следва:

1. За ВЪЗЛОЖИТЕЛЯ:

Адрес за кореспонденция: гр. София, пощенски код 1594, бул. „Княз Ал. Дондуков“

№ 1

Тел.: 02/9402969

e-mail: s.ivanova@government.bg

Лице за контакт: Севдалина Иванова - главен сътрудник по УЕПП, Отдел „Информационни системи“ Дирекция „Централно координационно звено“, Администрация на Министерския съвет

**2. За ИЗПЪЛНИТЕЛЯ:**

Адрес за кореспонденция: гр. Казанлък, пощенски код 6100, ул. „Стара река“ 2, етаж 4, офис 417

Тел.: 02/490-1600 Факс: 0431 / 6-22-53

e-mail: [info@david.bg](mailto:info@david.bg)

Лице за контакт: Стойчо Недев Стойчев, Технически директор ДАВИД Холдинг АД, тел. 0888 573709, e-mail: [snedev@david.bg](mailto:snedev@david.bg)

**(3) За дата на уведомлението се счита:**

1. датата на предаването – при лично предаване на уведомлението;
2. датата на пощенското клеймо на обратната разписка – при изпращане по пощата;
3. датата на доставка, отбелязана върху куриерската разписка – при изпращане по куриер;
4. датата на приемането – при изпращане по факс;
5. датата на получаване – при изпращане по електронна поща.

(4) Всяка кореспонденция между Страните ще се счита за валидна, ако е изпратена на посочените по-горе адреси (в т.ч. електронни), чрез посочените по-горе средства за комуникация и на посочените лица за контакт. При промяна на посочените адреси, телефони и други данни за контакт, съответната Страна е длъжна да уведоми другата в писмен вид в срок до 3 (три) дни от настъпване на промяната. При неизпълнение на това задължение всяко уведомление ще се счита за валидно връчено, ако е изпратено на посочените по-горе адреси, чрез описаните средства за комуникация и на посочените лица за контакт.

(5) При преобразуване без прекратяване, промяна на наименованието, правноорганизационната форма, седалището, адреса на управление, предмета на дейност, срока на съществуване, органите на управление и представителство на ИЗПЪЛНИТЕЛЯ, същият се задължава да уведоми ВЪЗЛОЖИТЕЛЯ за промяната в срок до 3 работни (три работни) дни от вписването ѝ в съответния регистър.

**Език**

**Чл. 48. (1)** Този Договор се сключва на български език.

(2) Българският език е задължителен за използване при съставяне на всякакви документи, свързани с изпълнението на Договора, в т.ч. уведомления, протоколи, отчети и др., както и при провеждането на работни срещи. Всички разходи за превод, ако бъдат необходими за ИЗПЪЛНИТЕЛЯ или негови представители или служители, са за сметка на ИЗПЪЛНИТЕЛЯ.

**Приложимо право**

**Чл. 49.** Този Договор, в т.ч. Приложенията към него, както и всички произтичащи или свързани с него споразумения, и всички свързани с тях права и задължения, ще бъдат подчинени на и ще се тълкуват съгласно българското право.

**Разрешаване на спорове**

**Чл. 50.** Всички спорове, породени от този Договор или отнасящи се до него, включително споровете, породени или отнасящи се до неговото тълкуване, недействителност, изпълнение или прекратяване, както и споровете за попълване на празноти в Договора или приспособяването му към нововъзникнали обстоятелства, ще

се уреждат между Страните чрез преговори, а при непостигане на съгласие – спорът ще се отнася за решаване от компетентния български съд.

Екземпляри

**Чл. 51.** Този Договор е изготвен и подписан в 2 (два) еднообразни екземпляра – един за ИЗПЪЛНИТЕЛЯ и един за ВЪЗЛОЖИТЕЛЯ.

Приложения:

**Чл. 52.** Към този Договор се прилагат и са неразделна част от него следните приложения:

Приложение № 1 – Техническа спецификация;

Приложение № 2 – Техническо предложение на ИЗПЪЛНИТЕЛЯ;

Приложение № 3 – Ценово предложение на ИЗПЪЛНИТЕЛЯ;

Приложение № 4 – Списък на персонала, който ще изпълнява поръчката и/или на членовете на ръководния състав, които ще отговарят за изпълнението;

Приложение № 5 – Гаранция за изпълнение.

**ЗА ВЪЗЛОЖИТЕЛЯ:**

.....  
**ВЕСЕЛИН ЧИНОВ**  
**ДИРЕКТОР НА ДИРЕКЦИЯ**  
**„АДМИНИСТРАТИВНО И ПРАВНО**  
**ОБСЛУЖВАНЕ И УПРАВЛЕНИЕ**  
**НА СОБСТВЕНОСТТА“,**  
упълномощен със Заповед № В-17/ 23.01.2018  
г. на министър-председателя, да изпълнява  
функциите на възложител по чл. 7, ал. 1 от ЗОП

.....  
**РУМЯНА ПЕТРОВА**  
**ДИРЕКТОР НА ДИРЕКЦИЯ**  
**„БЮДЖЕТ И ФИНАНСИ“**

**ИЗПЪЛНИТЕЛЯ:**

.....  
**БАЛЪО ДИНЕВ**  
**ИЗПЪЛНИТЕЛЕН ДИРЕКТОР**



## 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.

Дейностите, свързани с поддръжка на информационната система, използвана през периода 2007-2013, са изключително важни за гарантиране на надеждността и точността на информацията в нея и ако не са налични, биха възникнали грешки в данните за изпълнението на оперативните програми. Наличието на грешна информация и ненадеждна система за съхранение на данните в електронна форма е нарушение на нормативните изисквания на ЕС и може да доведе до санкции от страна на ЕК. В тази връзка, въпреки затихващите функции на ИСУН за периода 2007-2013 г., осигуряването на текуща поддръжка на системата е задължително условие за успешното окончателно приключване на оперативните програми и гаранция за качеството и надеждността на съхраняваните данни.

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 се поддържат по подходящ и коректен начин.

За да може ИСУН да осигурява проследимост, публичност и прозрачност на финансираните от ЕС проекти, е необходимо да бъде гарантирана надеждността и точността на информацията в системата. За изпълнението на това задължение е необходимо да бъде осигурено наличието на безпроблемно функционираща информационна система за предходния програмен период.

### **3. Основни потребители на ИСУН**

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 със следните информационни системи:

- Счетоводната система SAP, обслужваща Сертифициращия орган;
- Информационните системи ИСАК и АКСТЪР-ПОПАЙ и информационните системи, обслужващи програмите за трансгранично сътрудничество;
- SFC 2007.

## **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,.

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 за срок до края на 2021 г. Услугата се предоставя на абонаментен принцип. Възложителят ще заплаща месечна абонаментна такса на Изпълнителя, като последният се задължава да извършва целия обхват на посочените по-долу дейности за срока на договора. 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:

- Отстраняване на открити грешки в приложението. В рамките на определения срок Изпълнителят е длъжен да отстранява откритите грешки;
- Извършване на корективни дейности (в т.ч. и 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, и дейности при инциденти;
- Дейности по приложно администриране;
- Дейности по системното администриране, които следва да бъдат извършвани от оторизирани ИТ специалисти - системни администратори. Предвид развитието на технологиите и появата на облачни услуги под системно администриране се разбира администриране на операционните системи на ниво виртуални машини. Системното администриране включва цялостен мониторинг и управление на всички информационни ресурси, определени за системата;
- Извършване на промени от ниско ниво. Тук се включва: отстраняване на констатираните несъответствия и грешки в публичния модул и във вътрешната среда на ИСУН, добавяне на индикатори, параметри, списъци, чек-листи, отчети и справки, 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;
- Изпълняване на функциите на трето ниво на поддръжка съгласно „Процедури за работа на звено за техническа подкрепа“ (Help desk).

Изпълнителят следва да осигури адекватна и целенасочена софтуерна поддръжка, своевременна реакция и отстраняване на възникнали проблеми и възстановяване на системата до работното ѝ състояние – 24/7/365.

## 2. Предоставяне на услугата

В таблицата по-долу са описани различните приоритети и времената за реакция и отстраняване на открити грешки в приложението:

<b>Приоритет</b>	<b>Описание</b>	<b>Време на реакция</b>	<b>Време за възстановяване на ИСУН</b>
Критичен	Това е инцидент с критичен бизнес	30 минути	До 4 часа

	импакт. Достъпът до ИСУН е невъзможен. Изисква максимално бързо възстановяване на функционалността. Бизнесът не може да използва основната функционалност на ИСУН.		
Висок	Това е инцидент със среден бизнес импакт. Достъпът до ИСУН е възможен. Част от функционалността на ИСУН не е достъпна. Бизнесът може да използва основната функционалност на системата.	2 часа	Следващия работен ден
Нисък	Това е инцидент с нисък бизнес импакт. Засегната е до една институция потребител на ИСУН. Всички функции на ИСУН работят без проблем.	4 часа	3 работни дни

В рамките на посочения срок Изпълнителят е длъжен да отстранява откритите грешки.

Изпълнителят трябва да има внедрена и сертифицирана система за управление на сигурността на информацията, съответстваща на стандарт ISO 27001:2013 или еквивалентен обхват разработване, внедряване и поддръжка на софтуерни продукти и информационни системи, като към предложението за изпълнение на поръчката е необходимо да се представи копие на посочения сертификат.

Изпълнителят трябва да има внедрена и сертифицирана система за управление на ИТ услуги, съответстваща на стандарт БДС EN ISO 20000-1:2012 или еквивалентен с обхват разработване и поддръжка на софтуерни продукти и информационни системи за външни клиенти, като към предложението за изпълнение на поръчката е необходимо да се представи копие на посочения сертификат.

При изпълнение на дейностите по поддръжка Изпълнителят следва да се съобразява с изискванията на „Процедури за работа на звено за техническа подкрепа“ и 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>.

Комплектът на документацията при предаване на услугата на електронен носител включва:

1. Версия на продукта в заредима фаза, както и напълно документиран и актуален сорс-код. Представените документация и сорс-код следва да позволяват по-нататъшно развитие усъвършенстване на продукта с или без участие на Изпълнителя.
2. Стандартен съпътстващ софтуер, ако е необходим за нормалната работа на системата.
3. Пълна техническа и експлоатационна документация на системата.

По време на изпълнението на услугата Изпълнителят следва да предоставя актуализирана документация и кодове на продукта с настъпилите промени с означен номер на версията.

Изпълнителят трябва да осигури за своя сметка гаранционна поддръжка за период от 24 месеца след приемане на работата на Изпълнителя.

При необходимост, по време на гаранционния период трябва да бъдат осъществявани дейности по осигуряване на експлоатационната годност на софтуера и ефективното му използване от Възложителя, в случай че настъпят явни отклонения от нормалните експлоатационни характеристики.

### **3. Период на изпълнение**

Срокът за изпълнение на посочената услуга е до 31.12.2021 г.

### **4. Мерки за публичност и информираност**

При всички дейности, за които е приложимо, Изпълнителят следва да осигурява публичност и информираност по отношение на финансирането на настоящия договор. Изпълнителят следва да използва емблемата на ЕС във всички обяви или публикации, свързани с договора. Изпълнителят е длъжен да оповести, че договорът е получил финансиране от Европейския социален фонд (ЕСФ) чрез Оперативна програма „Добро управление” (ОПДУ). Изготвените материали следва ясно да отразяват финансовия принос на ОПДУ, спазвайки горните изисквания. Финансовият принос на ОПДУ следва да бъде ясно демонстриран по подходящ начин при изпълнението на всяка една от дейностите по проекта. Приложението следва ясно да демонстрира ролята на ОПДУ за изграждането на системата и да визуализира всички изискуеми лога, както и надписите показващи финансовия принос на ЕС.

### **5. Отчитане на предоставените услуги**

Отчитането на дейностите по предоставянето на услугата следва да отговаря на утвърдените правила и процедури за управлението на ОПДУ.

За отчитане на извършените дейности Изпълнителят изготвя доклади на период от 3 месеца, описващи всички извършени дейности по поддръжката за отчетния период, с приложена версия на продукта на CD/DVD/Flash memory носител в заредима фаза, както и напълно документиран и актуален сорс-код, стандартен съпътстващ софтуер, ако е необходим за нормалната работа на системата, и пълна техническа документация, ако през отчетния период е извършена промяна на версията на ИСУН. Докладите следва да съдържат:

- о Брой предоставени услуги по поддръжка;
- о Описание на предоставените услуги;
- о Информация за неразрешени искания, ако е приложимо.

Междинните доклади се приемат от Възложителя с двустранен, предавателно-приемателен протокол, с който се удостоверява, че предоставената услуга е извършена качествено.

### **6. Идентифицирани рискове**

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

1. Неправомерен достъп до системата
2. Уязвимост към зловреден код;
3. Загуба или манипулиране на данни;
4. Нарушаване конфиденциалността на чувствителните данни;
5. Възможни сринове на системата поради грешни действия на изпълнителя

ДО  
МИНИСТЕРСКИ СЪВЕТ  
гр. София, бул. „Княз Ал. Дондуков“ № 1

**ПРЕДЛОЖЕНИЕ ЗА ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА  
В СЪОТВЕТСТВИЕ С ТЕХНИЧЕСКИТЕ СПЕЦИФИКАЦИИ И  
ИЗИСКВАНИЯТА НА ВЪЗЛОЖИТЕЛЯ**

в процедура за възлагане на обществена поръчка с предмет:  
**„Осигуряване на поддръжка на ИСУН за програмния период 2007-2013“.**

от „ДАВИД Холдинг“ АД (наименование на участника), ЕИК/БУЛСТАТ: 833092882, представлявано от Бальо Атанасов Динев (трите имена) в качеството на Изпълнителен директор (длъжност, или друго качество), адрес гр. Казанлък, ул. „Стара река“ 2, офис 417, телефон 02 490 1600 факс 0431 62253, електронна поща [info@david.bg](mailto:info@david.bg),

**УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,**

С настоящото Ви представяме нашето предложение за изпълнение на обявената от Вас процедура за възлагане на обществена поръчка с предмет: „Осигуряване на поддръжка на ИСУН за програмния период 2007-2013“.

Съгласяваме се да изпълним поръчката съгласно всички изисквания на Техническата спецификация на възложителя и документацията за обществена поръчка.

При подготовката на настоящата оферта сме спазили всички изисквания на възложителя за нейното изготвяне.

1. Срокът за изпълнение на услугата е до 31.12.2021 г.

2. С оглед успешното изпълнение на услугата, предмет на поръчката, заявяваме че:

2.1. Участникът, когото представлявам има внедрена система за управление на сигурността на информацията по стандарт ISO 27001:2013 или еквивалентен с обхват, съгласно изискванията на възложителя, посочени в Техническата спецификация.

2.2. Участникът, когото представлявам има внедрена и сертифицирана система за управление на IT услуги, съответстваща на стандарт БДС EN ISO 20000-1:2012 или еквивалентен с обхват разработване и поддръжка на софтуерни продукти и информационни системи за външни клиенти.

3. С настоящото, представяме нашето предложение за изпълнение на обществената поръчка, както следва:

**3.1. Описание на подхода за управление на риска при изпълнение на поръчката:**

**Подход за управление на риска**

Формално, управлението на риска е процес, при който се изследва, анализира и проследява развитието на съществуващите рискове с цел да се намали негативния ефект от евентуалното им настъпване или пък да се предостави възможност за възползване от техният настъпване. Управлението на риска има за цел да бъде проактивно – да работи с вредите / възможностите много преди те да станат реалност.

Стефанка Байкова - Димитрова



Голяма част от рисковете, които могат да сполетят едно начинание е възможно да бъдат предвидени. Те се наричат известни рискове. Това са и тези рискове, които могат да бъдат управлявани. Остава и една част, които няма как да бъдат предвидени. Такива рискове се наричат неизвестни. Такива рискове могат да бъдат контролирани само с техники като предвиждане на финансов, времеви или материален резерв.

Управлението на риска е итеративен процес, продължаващ през целия период на изпълнение на проекта, включващ идентифициране, анализиране, реагиране и контрол на рисковете по проекта. То включва максимизиране на вероятността и последствията от благоприятни събития и минимизиране на вероятността и последствията от нежелателни за проекта събития.

Управлението на риска изследва рисковете и тяхното потенциално влияние върху проекта и формулира множество от действия, които елиминират или намаляват, доколкото е възможно, това влияние. Използването на доказана методология за управление на проекта и разработката, както и средства за осигуряване на качеството помагат да се преодолеят много от генеричните рискове за проекта. За управлението и преодоляването на рисковете скипът на Изпълнителя ще приложи методология, включваща следните задължителни стъпки:

- Идентифициране на рисковете, колкото се може по-рано в жизнения цикъл на проекта;
- Оценка и приоритизиране на рисковете;
- Планиране на намаляването на рисковете и непредвидените събития;
- Мониторинг на рисковете през целия жизнен цикъл.

### **Роли и отговорности в екипа по управление на риска в проекта**

#### **Инициатор**

Инициаторът на риск е този, който първоначално идентифицира риска и съобщава за него на Ръководителя на проекта. Инициаторът е отговорен за:

- Максимално ранно идентифициране на риска;
- Изпращане на съобщение за риск;
- Предоставяне на допълнителна информация за съответния риск при необходимост;
- Следене на предпоставки и признаци за поява на съответните нежелани събития.

Всеки участник в проекта може да съобщи за риск, т.е. да бъде в ролята на „Инициатор на риск“. Това може да стане по един от следните начини:

- Чрез съобщение по електронна поща с обратна разписка, изпратено до Ръководителя на проекта със Subject: Risk с кратко описание на риска > и Body: свободно описание, което може да съдържа предложение за стойности на атрибутите на риска;
- Директен запис в Регистър на рисковете, когато инициатор е Ръководителят на проекта;
- Съобщение по време на среща на проектните скипи, което е протоколирано като риск.

### Риск мениджър

Риск мениджър е роля в конкретния проект съвместявана от Ръководителя на проекта. Риск мениджърът е отговорен за:

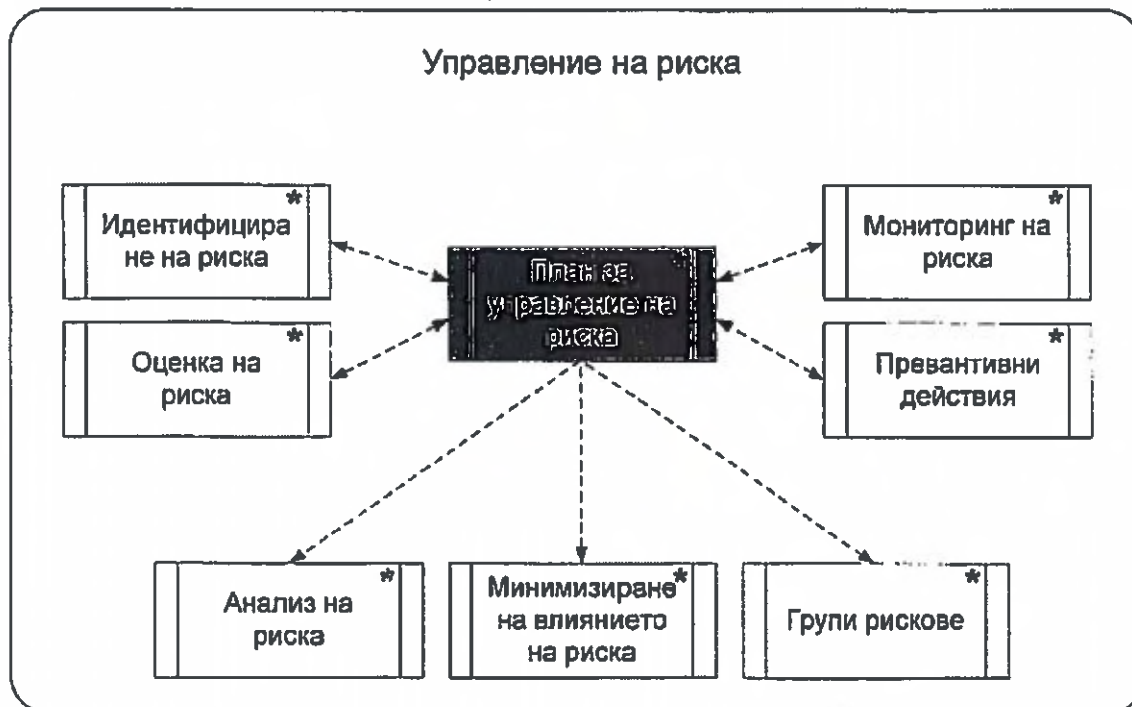
- Максимално ранно идентифициране на риска;
- Получаване на съобщенията за рискове и оценка на тяхната релевантност за проекта;
- Регистриране на рисковете в Регистъра на рисковете;
- Оценка и анализ на рисковете;
- Комуникация на рисковете с ръководството на проекта, когато това е необходимо;
- Комуникацията на решенията на ръководството на проекта с работните групи;
- Мониторинг на действията спрямо рисковете.

### Отговорник

Определеният отговорник за риск:

- Извършва или контролира планираните действия срещу риска;
- Следи за появата на признаци за съответните нежелани събития.
- Информира ръководителя на проекта за промени в обстоятелства и фактори, които влияят на риска.

На следващата фигура са представени основните компоненти на управлението на риска при изпълнение на проекта:



Рисковете са идентифицирани в началото на проекта и непрекъснато ще се поддържат актуални докато проекта е в ход. Ръководителят на проекта и екипа ще следят хода на проекта, неговото текущо състояние, и това, което предстои и ще преоценяват потенциалните заплахи и възможности.



ЕВРОПЕЙСКИ СЪЮЗ



ЕДНА ПОСОКА  
МНОГО ВЪЗМОЖНОСТИ

## Методика за управление на риска

Предлаганата методика PRINCE2 осигурява ефективното управление на риска, което е много важно за успеха на проекта. От ключово значение е да има ангажираност и от Възложителя, и от Изпълнителя за идентифицирането и контролирането на рисковете на проекта. Дори когато всички ресурси на Възложителя и Изпълнителя са наясно с всички възможни рискове, това не означава, че последствията от тях са определени и категорични и не е изключено, въпреки всички предприети мерки, те да окажат негативно влияние върху прогреса и/или качеството на проекта. Ето защо, тази тема изисква специално внимание от всички заинтересовани страни през всички фази на проекта и следва да бъде разглеждана на всички срещи за обсъждане на статуса на проекта. Трябва да се осигури, че всички заинтересовани страни са информирани навреме относно вероятността за поява на рискове за проекта и относно възможните (планирани) мерки за реакция в случай на проявление - за елиминиране или минимизиране на неблагоприятния им ефект.

**Планиране управлението на риска** - процес за определяне на подхода и дейностите по управление на риска. Важно е да се планират и последващите процеси по управление на риска, за да има съизмеримост между нивото, вида и прозрачността на управление на риска, от една страна и самия риск и важността на проекта за организацията, от друга.

**Идентифициране на риска** - определяне на рисковете, които могат да повлияят на проекта, и документиране на техните характеристики в Регистъра на рисковете. Участници в процеса на определяне на риска са: основният екип на проекта, екипът по управление на риска, специалисти от други звена на фирмата, клиенти, крайни потребители, други ръководители на проекти и външни експерти. Идентифицирането на риска е итеративен процес. Първата итерация може да се осъществи от част от екипа на проекта или от екипа по управление на риска. Целият екип на проекта и основните заинтересовани лица могат да осъществят втората итерация. Щом бъде идентифициран даден риск, се разработят и дори внедряват прости и ефективни мерки за преодоляването му.

**Качествен анализ на риска** - оценка на вероятността за проявление и ефекта от даден риск. Този процес приоритизира рисковете според вероятността им за проявление и евентуалното им въздействие (ефект) върху целите на проекта. Качественият анализ на риска е един от начините за определяне важността на идентифицираните рискове и насочване на усилията към справяне с тях. Времето за реакция може да е критичен фактор при някои рискове. Оценката на качеството на наличната информация също спомага при преоценката на риска. Качественият анализ за оценка на вероятностите и ефекта на рисковете използва различни методи и средства.

**Количествен анализ на риска** - приложение на мощни статистически и други количествени методи за анализ на най-важните рискове за проекта. В този процес се използват методи като симулации "Монте Карло", дърво на решенията, експертни оценки, анализ на чувствителността и други с цел получаване на количествени оценки за вероятността от проявлението на даден риск и на ефекта му върху срока, бюджета или характеристиките на продукта на проекта. Тези оценки са основа за избор на стратегия и

за планиране на адекватни действия за реакция в случай на проявление на всеки риск.

**Планиране на реакция на риска** - разработване на варианти и определяне на действия, които увеличават възможностите и намаляват заплахите за осъществяване на целите на проекта. Този процес включва възлагане на отговорности на отделни лица или звена във връзка с планираните дейности относно рисковете, както и използването на други необходими ресурси. Този процес гарантира адекватна реакция на идентифицираните рискове в случай на тяхното проявление.

**Следене и контролиране на риска** - проследяване на идентифицираните рискове, наблюдаване на остатъчни рискове и откриване на нови рискове. Този процес служи за осъществяване на планираните действия за реакция на риска и за оценка на тяхната ефикасност. Той се изпълнява многократно в хода на проекта. С времето рисковете се променят, появяват се нови, някои очаквани рискове не се проявяват. Доброто наблюдение и контрол на рисковете дава информация, която подпомага взимането на адекватни решения за предотвратяване на неблагоприятните рискове и за използване на всички благоприятни фактори и условия.

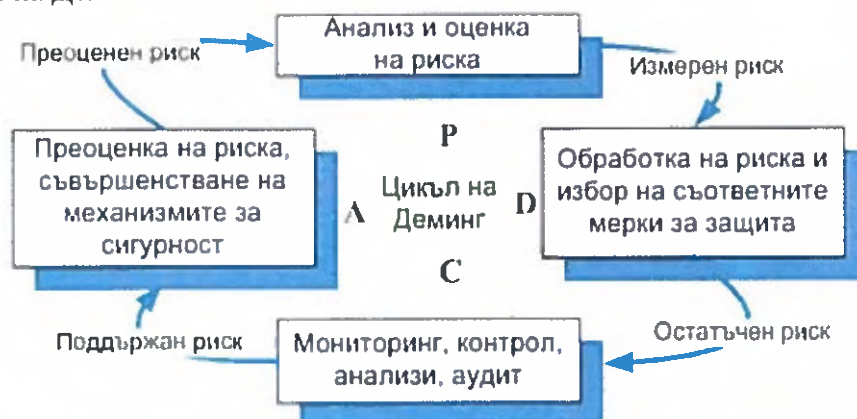
Контролът на риска може да включва избор на алтернативна стратегия, прибягване до резервен план, извършване на коригиращи действия или препланиране на проекта. Ръководителят на проекта и ръководителят на екипа за риска периодично получават информация за ефективността на плана и наличието на неочаквани въздействия и взаимно съответните мерки в хода на проекта.

**Ключови фактори за успех** - успешното управление на риска изисква:

- Достъп до надеждна и актуална информация за рисковете
- Регулярна оценка и анализ на критичните рискове
- Непрекъснато следене и контролиране на ефекта от предприетите действия за реакция на рисковете
- Осигуряване на баланс между процесите за управление на риска и останалите процеси за управление на проекта.

#### Процес на управление на риска

Предлаганият от нас подход включва процес на итеративно управление на риска с непрекъснато подобряване по време на целия проект. Този процес е известен още като „Цикъл на Деминг“.





### Идентифициране на рисковете

Идентифицирането на рискове е процес, при който се определят възможните източници на рискове, а самите рискове се идентифицират и описват. Източниците на рискове в контекста на всеки проект могат да бъдат разделени в две основни групи:

- **Външни рискове** - обикновено произлизат от бизнес средата, в която функционират участниците в проекта (имат икономически, социален, политически или технологически характер), от висшия мениджмънт (пр. промяна в собствеността на организацията, промяна в бизнес целите и стратегиите, вътрешна нестабилност и конфликти и т.н.) и от клиентите на проекта (пр. липса на заинтересованост и ангажираност, организационно културни различия т.н.). Наричат се външни, защото проектния екип (в това число и проектния мениджмънт) не може пряко да им влияе. Идентифицирането на външните рискове е най-успешно при наличието на задълбочен анализ на външната (макросреда и микросреда) и вътрешната среда (висш мениджмънт, финансови/човешки ресурси и т.н.) на ниво организация.
- **Вътрешни рискове** - свързани са със самия проект и типа задачи, които се изпълняват в него. Тези рискове са малко или много под контрола на проектния екип (проектния мениджър) и с възрастта на организацията и натрупването на опит, значително намаляват. Например такива рискове могат да са резултат от неяснота в ролите и отговорностите вътре в екипа, липсата на дисциплина и ред, липсата на управленски качества и познания, липсата на мотивация (риск от текучество), внедряването на нова технология и т.н.

Идентификация на потенциалните случаи и уязвимости на проекта, които могат да имат негативен ефект на работата или плановите, е основата на стратегията за управление на риска. Екипът на Изпълнителя ще използва следните добри практики за идентифициране на риска:

- Определяне на риска на базата на целите - определят се целите на проекта, а всички събития или обстоятелства, които могат частично или напълно да застрашат постигането на тези цели, се определят като рискове;
- Определяне на риска на базата на сценарии - разиграват се различни сценарии за развитието на определено събитие или изпълнението на определен процес. Всяко събитие, което предизвиква реализирането на нежелан резултат, се третира като риск;
- Разговори с експерти в различните области на проекта и представители на Възложителя - на база добри практики се разработва въпросник, от отговорите на който се извличат рисковете, които трябва да се контролират.

Веднъж идентифицирани, рисковете се документират в Регистъра на рисковете. Той съдържа детайли за всички рискове, тяхната оценка, собственици и статус в хода на проекта.

**Идентификация на рисковете и предпоставките, които могат да окажат влияние върху изпълнението на поръчката**

Разработването на софтуерни решения е сред най-рисковите начинания, които трябва да се управляват разумно и много внимателно. Много технологични проекти и проекти за разработка на приложен софтуер често надхвърлят първоначалния бюджет,

краен срок или обхват поради неадекватното управление на риска или недостатъчно внимание, ангажираност и приоритизиране на съпътстващите разработката рискове.

Считаме, че правилният подход за управление и изпълнение на проекти, свързани с вграждането и интегрирането на информационни системи е да се открие навреме всеки един риск, за да може той да се контролира в рамките на проекта и да се минимизира неговото въздействие върху цялостното изпълнение.

В това отношение методологията PRINCE2 се допълва от методологията за разработка RUP, като се залага на ранното минимизиране на риска като съществена част от управлението на проекта. За целта вместо да се пренебрегват или скриват рисковете, те се оценяват, управляват и контролират, за да не могат да причинят неочаквано надхвърляне на разходите, обхвата или срока на проекта.

По-долу са описани типични основни рискове при софтуерните разработки, за да се подпомогне процеса по тяхното управление:

- Надхвърляне на заложения обхват;
- Честа промяна на изискванията;
- Лошо управление на очакванията на потребителите;
- Непълнени очаквания за проекта;
- Липсваща функционалност;
- Недостатъци на хардуерната конфигурация, например капацитет, възможности и др.;
- Неправилно описан обхват, неидентифицирани базови функционалности или софтуерни интерфейси;
- Липса на ясна отчетност, отговорност и контрол за изпълнение;
- Недостиг на човешки ресурси;
- Липса на ангажираност при управлението на проекта в някоя от страните;
- Липса на приоритети при изпълнение на задачите;
- Липса на разбиране за позите от проекта;
- Липсата на процес за измерване на резултатите и за измерване на ползата от реализацията;
- Напускане на ключови експерти за проекта;
- Пропуски или загуби в развойната/тестовата среда;
- Закъснение при доставката и конфигурирането на хардуера за системата, което влияе върху внедряването на софтуерната разработка;

Поради спецификата на проекта могат да се очакват допълнително следните рискове:

- Промяна в нормативната уредба;
- Недобра комуникация между екипите на Възложителя и Изпълнителя по време на аналитичните етапи на изпълнение на проекта.
- Затруднения в работата на възложителя по време на първоначалния период след пускането в действие на новите разработки.
- Трудности при осигуряване на експлоатационна и тестова среда.

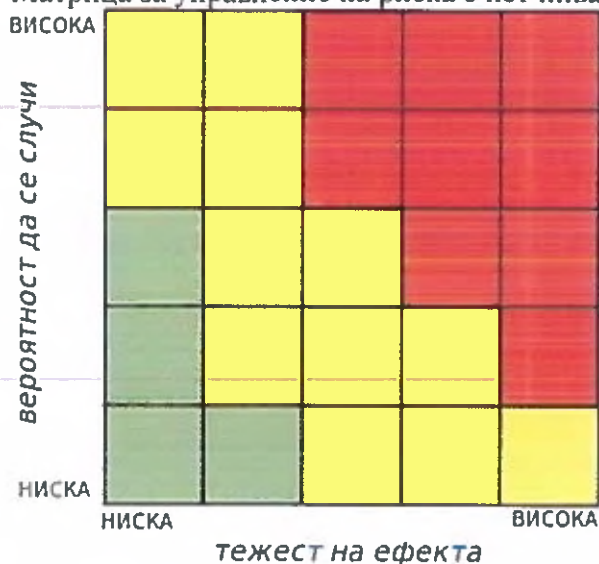
За да се минимизира възможността от проява на тези рискове, трябва управлението на риска да бъде отговорност на всички един член на работния екип, а от Ръководителя на проекта се очаква да следи за проявление на риска и да го докладва

навреме пред Заинтересованите страни, с цел намаляване на въздействието му върху успеха на проекта.




### Анализ на рисковете

Анализът и оценката на рисковете е процес, при който рисковете се анализират с цел да се определят вероятността те да се случат и евентуалните последиците върху проекта. Целта е да се постави количествена оценка на всеки риск на база, на която те да бъдат приоритизирани (за целите на модифицирането им). Важно е да се отчете факта, че конкретния момент на настъпване на риска има значение върху последиците, които ще окаже. Използвайки тези два показателя се въвежда т.нар. матрица за оценка на степента на риска.

Матрица за управление на риска с пет нива на всяко от измеренията.



#### ЛЕГЕНДА:

-  рискът може да бъде пренебрегнат
-  рискът трябва да бъде анализиран
-  рискът трябва да бъде управляван

Оценката, която се получава като резултат от тези два показателя се нарича влияние на риска. Съществуват два подхода за оценяването на рисковете: отгоре-надолу и отдолу-нагоре. При подхода отгоре - надолу се разработва списък на потенциалните рискови фактори. Оценката е на база предишен опит. Стремешът е да се определят потенциалните връзки между отделните рискове, моментите на тяхното настъпване и възможните последици. Това дава възможност да се вземат предварителни действия за да се предотврати или намали влиянието на риска. При подхода отдолу - нагоре рисковете се анализират детайлно на най-ниското ниво. Оценяват се алтернативните критични пътища и се изчисляват времетраенето и продължителността с цел да се осигури възможност на ръководителите да заложат буфери, с помощта на които биха посрещнали негативните последици от реализирането на рискове. На практика този подход предполага невъзможност на ръководителя да предвиди риска и да предприеме



превантивни управленски действия за избягването му.

В конкретния проект, считаме за подходящо да се приложи подхода за оценка на риска отгоре – надолу. На база сериозния си опит при реализиране на аналогични проекти сме разработили списък на потенциалните рискови фактори. Целта е да се определят потенциалните връзки между отделните рискове, моментите на тяхното настъпване и възможните последици. Този подход дава възможност да се вземат предварителни действия за да се предотврати или намали влиянието на риска.

Анализа на рисковете се извършва в две направления – качествено и количествено.

### Качествен и количествен анализ на риска

Рисковете се оценяват въз основа на възможността да се случат и въздействието, което биха имали върху целите на проекта:

- Възможността е оценената вероятност да се появи риска
- Въздействието е оцененият ефект или резултат от появата на риска

Въздействието се оценява въз основа на:

- време
- разходи
- качество
- обхват
- ползи
- хора/ресурси

За оценка на вероятността за проявление на рисковете е възприета следната скала

- Малка - вероятност за проявление до 30 %
- Средна - вероятност за проявление над 30 % до 70 %
- Висока - вероятност за проявление над 70 %

За оценка на ефекта на рисковете е възприета следната скала:

- Слаб
- Среден
- Голям
- Критичен

### План за реакция на рисковете

Изборът на действие е баланс между множество фактори и почива на избрана стратегия. За идентифицираните и оценени рискове се предвиждат действия за реакция на риск целящи увеличаване на възможностите и намаляване на заплахите за целите на проекта. Те целят да се осигури внимание върху рисковете с най-висок приоритет чрез включително на ресурси и дейности в бюджета, графика и плана за управление на проекта. Планират се действия, за които разходите са по-приемливи от риска, който контролират. Действията за реакция на риска се описват в Регистъра на рисковете заедно с оценките за разходите и отговорностите за тяхното предприемане. Те се основават на избрана стратегия измежду изложените по-долу.

Подходът за управление на риска зависи от неговия приоритет:

- Риските с **нисък приоритет**. Рискът е малък, защото е малко вероятно да се прояви и/или ще има малко влияние върху успеха на проекта. Риск мениджърът наблюдава тези рискове да не преминат в жълтата или червената зона на матрицата.
- Риските със **среден приоритет**. Рискът е среден, защото може да се прояви и/или може да има отрицателно влияние върху успеха на проекта. Тези рискове се наблюдават непрекъснато, като се прилагат действия за контролирането им, с цел да не преминат в зоната с висок приоритет.
- Риските с **висок приоритет**. Рискът е голям, защото е с голяма вероятност да се прояви и/или ще има голямо отрицателно влияние върху успеха на проекта. Спрямо рисковете, попаднали в зоната с висок приоритет, задължително се предприемат мерки и се управляват активно.

### Стратегии за негативни рискове или заплахи

В настоящия проект, в съответствие с избраната методология управление на проекта PRINCE2, ще прилагаме четири основни стратегии за третиране на риска:

#### Избягване

Промени в плана на проекта за елиминиране на риска или за защита на целите на проекта от ефекта му - намаляване на обхвата, добавяне на ресурси, удължаване на срока, избягване на нови подходи или непознати подизпълнители и др.

#### Прехвърляне

Прехвърляне на последиците от риска върху трета страна, заедно с отговорността на реакцията, т.е. отговорността за управлението му - управление на финансовия риск (договори с трета страна, застраховане, гаранции и др.).

#### Смекчаване

Намаляване на вероятността или ефекта на неблагоприятно рисково събитие до приемливи граници - превантивни действия за предотвратяване или смекчаване на проблема; ранни действия за атакуване на причините, на обоснована цена.

#### Приемане

Приемането се отнася само до тези рискове, чието избягване, смекчаване или прехвърляне е невъзможно или неоправдано. Ще бъдат използвани следните варианти на приемане на риска:

- Активно приемане - разработен план за действие при непредвидени обстоятелства, в случай че се наложи.
- Пасивно приемане - без планирани действия; проектният екип се справя с риска, когато и както се прояви.
- Резерв за непредвидени обстоятелства - резерв от време, пари, ресурси.
- План за действие при провал - неуспешна стратегия, риск с голям ефект.

Конкретният подход (реакция), който Изпълнителя ще приложи за управление на риска ще бъде избран в зависимост от естеството на риска и неговия приоритет.

### Мерки за превенция на рисковете и намаляване на негативните последици

Съгласно предложената методология PRINCE2 и RUP, мерките за управление на риска са свързани с управлението на следните процеси:

- **Планиране:** Оценката на риска е най-ефективния начин да се хване и ограничи въздействието му. Затова ефективното планиране на риска ще позволи да се дефинират възможните области, в които рискът може да се прокрадне или задълбочи.
- **Качествено изпълнение:** Преглеждането на очакваните услуги/резултати спрямо договореното още по време на Встъпителната фаза е начин да се изградят поточно очакванията за проекта и да се гарантира, че изпълнението и обхвата се управляват и са коректно заложени в архитектурата на системата.
- **Изпълнение на очакванията и постите ангажменти:** Разговорите със заинтересованите страни (спонсори, клиенти, възложители, потребители) още в началото на проекта подпомага разбиранията им за очакванията по отношение на целите на проекта, обхвата и ресурсите.
- **Разширение на обхвата:** Осигурява се непрекъснат фокус върху контролирано разширяването на обхвата на проекта откъм функционалност, организация, бизнес процеси, технологии, доставчици или работен екип.
- **Управление на проекта:** Извършва се ежеседмичен анализ на работния график от екипа и ръководителя на проекта.
- **Проследяване на изискванията:** Всички изисквания следва да бъдат категоризирани и да бъдат номерирани, за да са лесни за проследяване. Категоризираните изисквания, с които се определя обхвата на проекта (това са критичните изисквания) трябва да бъдат подписани от съответните заинтересовани страни.
- **Техническо управление на риска:** Определя се дали при управлението на риска не се налага помощ от специалист.
- **Управление на промените:** Определя се дали всяка промяна може да намери място в текущата разработка.

### Планиране и ресурсно обезпечение

В настоящия проект, в съответствие с избраната методология управление на проекта PRINCE2, ще прилагаме следните подходи за ефективно планиране и ресурсно обезпечение на риска:

- Определяне на количеството и типа ресурси, необходими за извършване на споменатите дейности;
- Разработване на подробен план за действие;
- Потвърждение на желанието за извършване на дейностите, идентифицирани по време на оценка на рисковете
- Получаване на одобрение от ръководството
- Определяне и възлагане на задачи на ресурси за извършване на определените дейности
- Ресурсите, необходими за дейностите по избягване, смекчаване и прехвърляне на рисковете, следва да се финансират от бюджета на проекта.

### Следене и контролиране на риска

Изпълнителят ще обърне специално внимание на мониторинга и отчитането на

дейностите по рисковете. Някои от дейностите ще включват наблюдение на идентифицираните рискове за промени в техния статус, а други ще включват:

- Проверка, че планираните дейности имат очаквания ефект;
- Проверка за вторични или остатъчни рискове и планиране на действия за тях;
- Наблюдение за ранни сигнали за поява на нови рискове;
- Моделиране на тенденции за прогнозиране на рискове;
- Проверка, че цялостното управление на риска се прилага ефективно.

### Мониторинг на риска

Мониторинг на риска е процес, при който систематично се следят и оценяват представените действия за справяне с риска и се развиват бъдещи опции, които са подходящи за справянето с тези рискове. За ефективен контрол на управление на рисковете по време на изпълнението на проекта се извършва регулярен мониторинг на рисковете и по-точно на статуса на риска и резултата от него при действието по справяне с риска.

### Обосновка за използвания подход

Подходът, който ще прилагаме за идентифициране, анализиране и реагиране на рисковете по проекта съответства напълно на Системата за управление на качеството на ДАВИД Холдинг АД. Той е насочен към максимизиране на вероятността и ефекта от благоприятните събития и минимизиране на вероятността и ефекта от неблагоприятните за проекта събития. Причината за избора на този подход е, че той е използван в продължение на повече от 20 години в проекти за разработване и внедряване на комплексни софтуерни системи. В този период той е доказал своята приложимост в тази област, което е гаранция за навременното идентифициране и контролирането на рисковете в проекта.

### Списък с идентифицирани рискове

В „Регистър на рисковете“ е представен списък на предварително идентифицираните рискове с оценка на въздействието (ефекта), вероятността и действия за реакция. След иницирането на проекта и в хода на неговото изпълнение Регистърът на рисковете ще бъде допълван и актуализиран въз основа на новата информация за средата и продукта на проекта. Той ще бъде неразделна част от Плана за управление на риска, а в хода на изпълнение на проекта решенията и действията за управление на рисковете ще бъде докладвани с отчетите за напредъка на проекта.

За всеки идентифициран риск предлагаме да се поддържа следната информация:

- Идентификатор - служи за идентифициране на риска. Обикновено се използва уникален номер (ID) или наименование;
- Описание - кратко текстово описание на риска;
- Вероятност - индикатор за вероятно проявление на риска, съгласно следното деление:
  - Висока вероятност (В) - над 0,7;
  - Средна вероятност (С) - между - 0,3 и 0,7;
  - Ниска вероятност (Н) - под 30%;
- Ефект - индикатор за относителни влияния върху проекта - като закъснения спрямо времевия график или спрямо заложения бюджет:
  - Малък (М)



- Среден (С)
- Голям (Г)
- Критичен (К)
- Подход за третиране - описание на предложения подход за редуциране на въздействието на риска;
- План - само за рискове, които реално се проявяват се създава се план на действие. Той съдържа информация как ще се реагира на проявлението на риска (например, предлага се алтернативно решение, намалява се функционалността и т.н.)

Взимайки в предвид описаните процеси по управление на риска и описания подход за категоризиране и оценяване на рисковете, предлагаме списъкът с рискове да се поддържа в табличен вид и да се допълва итеративно.

### Мерки за намаляване на предварително идентифицираните рискове

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

#### 1. Неправомерен достъп до системата

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 прогнозен брой потребители (над 25000) и обществено значимото предназначение на системата и съхраняваните в нея данни е голяма вероятността от опити за придобиване на неправомерен достъп до нея.

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:

- 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.

Една от целите 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 механизъм за отговор (предложение за предприемане на действия). За всяка предложена мярка за намаляване на риска сме дали обяснение, демонстриращо как предложената мярка ще повлияе на вероятността за събъждане или влиянието на събъждането на съответния риск.

**Предвиждаме следните мерки за намаляване на риска:**

#### **1.1. Анализ на защитата на системата от неправомерен достъп**

Ще бъде извършен анализ на всички компоненти на системата, имащи отношение към осигуряване на защита от неправомерен достъп до системата включващи:

- 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 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. Оценката на риска ще служи като план за повишаване на сигурността на системата и приоритетно изпълнение 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 на 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 извеждането 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.

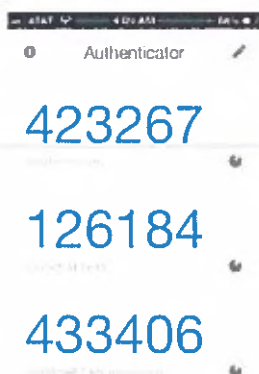
Тази мярка намалява риска от неправомерен достъп за сметка на подобряването на политиката и процедурите за информационна сигурност и налагане на правила на потребителите на системата, не позволяващи избор на „слаба“ парола, която би могла да бъде отгатната по метода на социалния инженеринг или чрез груба сила (налучкване), както и защита чрез двустепенна идентификация (2FA) в случаите, когато данните за идентификация на потребителя са станали известни на друг.

## 1.3. Защита от неправомерен достъп с двустепенна идентификация (2FA) с допълнителна еднократна парола

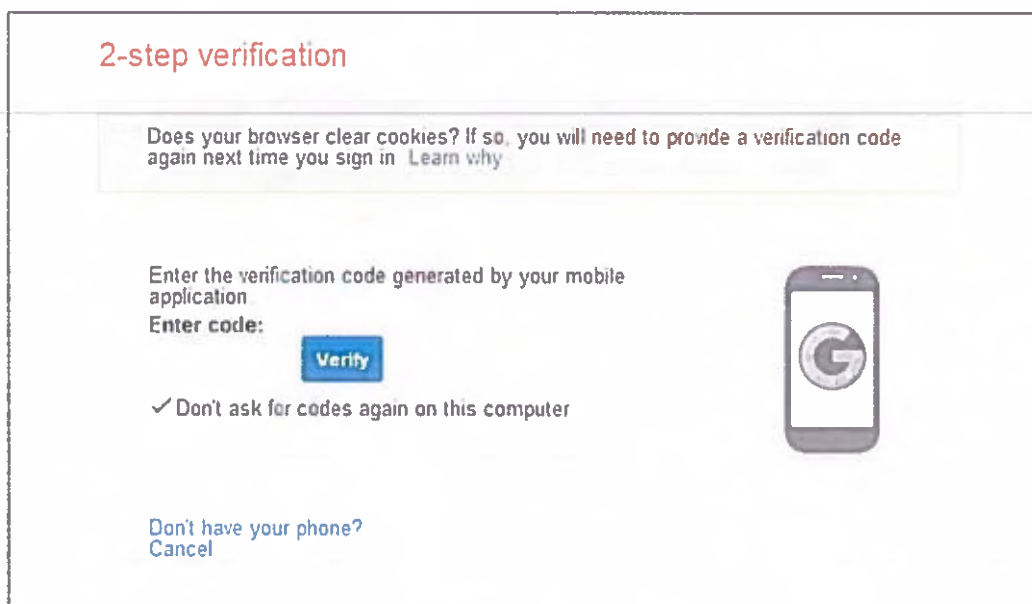
Въвеждане на възможност за двустепенна идентификация (2FA) с допълнителна еднократна парола (шест цифри), получавана на мобилен телефон за всички потребители на вътрешната част на системата, като се използва стандартни безплатни приложения за смарт телефони или SMS/email. Подходящи приложения за целта са Microsoft Authenticator, Google Authenticator, Lastpass Authenticator, които са безплатни и налични



за всички мобилни операционни системи.



За да не затормозява ежедневните потребители след еднократна двустепенна идентификация (2FA), съответния браузър ще може да се запише като безопасен, за да не се изисква допълнителната еднократна парола за определено време (примерно един месец, една седмица или един ден според профила на съответния потребител).



2-step verification

Does your browser clear cookies? If so, you will need to provide a verification code again next time you sign in. [Learn why](#)

Enter the verification code generated by your mobile application  
Enter code:

☒ Don't ask for codes again on this computer

[Don't have your phone?](#)  
[Cancel](#)

Ще бъде реализирана възможност за настройка на двустепенна идентификация (2FA) за всяка от ролите в системата, като за административните роли препоръчваме да е включена по подразбиране с изискване на еднократна парола ежедневно или ежеседмично.

Особено сериозни биха били последствията от неправомерен достъп до вътрешната част (непублична) част на системата, тъй като вътрешните потребители имат достъп до много по-голям обем информация, а също и по правило по-големи права. За тези потребители (от управляващи органи и ЦКЗ) препоръчваме двустепенна идентификация (2FA) да е включена по подразбиране с изискване за подновяване на еднократна парола ежеседмично или ежемесечно.

Този мярка намалява риска от неправомерен достъп за сметка на „слаба“ парола, която би могла да бъде отгатната по метода на социалния инженеринг, чрез груба сила (палучкване) или е станала известна по друг начин.

#### **1.4. Преглед на правата за всяка роля**

С цел минимизиране на влиянието на риска от неправомерен достъп до данни, до които съответния 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 наличното 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.

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

#### **1.5. 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.

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

#### **1.6. 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.

Този мярка намалява риска от неправомерен 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.

### 1.7. 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 с възможност за използване на двустепенна идентификация (2FA) с допълнителна еднократна парола, която ще се изисква ежедневно 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. Ще бъдат съхранявани само в криптиран вид в сигурно хранилище, защитено с двустепенна идентификация (2FA) и силна парола.
- 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 неерегламентиран достъп до системата ИСУН 2007-2013 и изграждащите я компоненти.

Този мярка намалява риска от неправомерен достъп до системата чрез използване на данните за достъп на експерти ангажирани с изпълнението на поръчката.

#### **1.8. 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 сбъдваемост 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.

#### **1.9. 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.

#### **1.10. Мерки за защита от неоторизиран достъп при реализация на промени в системата или от уязвимости в модулите на системата**

В рамките на подобрението на ИСУН 2007-2013 ще бъдат реализирани промени в системата свързани с:

- Отстраняване на открити грешки в приложението;
- Извършване на корективни дейности (в т.ч. и корекции в базата данни) и дейности при инциденти за изпълнението, на които ще се налага и създаването или промяна на програмни единици (модули, скриптове за изпълнение и др.);
- Разработка на изцяло нови функционалности.

При проектиране и реализация на софтуерните промени в системата, на фокус ще бъде минимизиране на риска от неоторизиран достъп до системата, както от наличните потребители, така и от външни страни. За минимизиране на този риск ще прилагаме инженерни принципи за разработка на сигурни приложения, намаляващи риска от неоторизиран достъп.

##### **1.10.1. Прилагане на „Инженерни принципи за разработка на сигурни приложения“**

Ще спазваме правилата заложили във вътрешния ни документ „Инженерни принципи за разработка на сигурни приложения“, в който ще заложим 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 ще доведе до еднотипен стил на разработка, базиран на правила, фокусирани върху всички аспекти на сигурността на системата и респективно до намаляване на вероятността въздействието при евентуална реализация на определени рискове, в т.ч. и риска неототоризиран достъп до системата.

В инженерните принципи ще бъдат включени и детайлизирани следните мерки за защита, водещи до намаляване на риска от „Неоторизиран достъп до системата“:

#### 1.10.2. Защита от SQL Injection

SQL Injection е една от най-опасните уеб уязвимости и е класирана на първо място в класацията на Open Web Application Security Project (OWASP) за десетте най-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 неототоризирано извличане на данни или осигуряване на идентифицираща информация и достъп до системата или нейни компоненти. 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.

Използването 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 да променят поведението на SQL заявките от клиентския слой на системата и така значително намалява риска от неправилен достъп до системата.

#### 1.10.3. 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 и придобиване на нерегламентиран достъп до системата.

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 неправилен достъп.

#### 1.10.4. Проверка и валидиране на входните данни

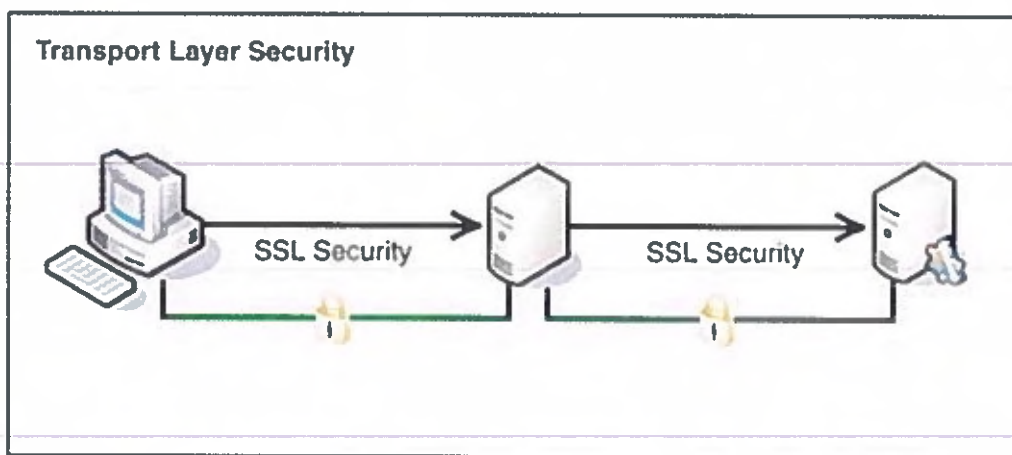
На всички места, където се въвеждат данни в системата ще се прави проверка и валидиране на входните данни по типове, маски, възможни диапазони във всички форми на системата (например: за въвеждане на дати – не трябва да се допуска въвеждане на дати извън възможният диапазон определен за съответните данни, за процент – не повече от 100). Всички данни, които са от тип символен низ ще преминават филтриране

(премахване) на специални символи, които са недопустими символи, филтриране на HTML кодове, URL адреси и използване на позитивен списък, където това е приложимо.

Валидирането на входните данни минимизира вероятността за внасяне на код за реализация на атаки с цел получаване на нерегламентиран достъп до системата (напр. XSS - Cross Site Scripting).

#### 1.10.5. Използване на защитени канали за комуникация

Използването на защитени канали за комуникация, между отделните слоеве на системата и при интеракция с потребители и външни системи, намалява риска от нерегламентиран достъп до данните в процеса на трансфер на тези данни.



Предлагаме използването на мрежата на държавната администрация, където това е възможно като среда за пренос на данни за вътрешните модули на информационната система и при обмен данни с други системи от администрация. Това допълнително ще намали риска от прихващане на данни за оторизация в системата за вътрешните потребители, чиито права като правило са по-големи. Тази мярка директно кореспондира с изискванията към системната архитектура, заложиени в т. 1.3 на предварителните условия за допустимост на проекти за е-управление.

#### 1.10.6. Разработка и спазване на правила за използване на криптографски средства за съхраняване, предаване и приемане информация в информационната система ИСУН 2007-2013

След анализ на използваните средства за защита, текущото състояние и чувствителните данни, ще създадем правила за използване на криптографски средства за защита на информацията в системата, регламентиращи видовете криптографски средства, които ще се използват, както и процесите и архитектурните слоеве на системата, в които ще се използват при изпълнение на нови функционалности и поддръжка на ИСУН 2007-2013.

С внедряването на точни и ясни правила за използване на криптографски средства в слоевете и процесите, в които това е възможно и оценено като необходимо ще се постигне ниска вероятност от придобиване на неотортизиран достъп до чувствителни данни в системата (напр. идентифициращата информация на потребителите) и до системата като цяло.

#### 1.11. 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 бюлетени 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.

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

#### **1.12. Провеждане на тестове за проникване в системата**

Според изследване на Verizon Data Breach Web за 2016 (<http://www.verizonenterprise.com>), уеб базираните системи имат дял от над 40% от всички нарушения на сигурността на информационни системи. В 93% от случаите, на атакуващите лица са им били необходими минути, за да компрометират дадена информационна система.

Базирайки се тези факти и за минимизиране на риска от пробиви в сигурността на системата, и намаляване на риска от нерегламентиран достъп ще проведем тестове за проникване (penetration test) на системата.

Провеждането на тестове за проникване (penetration test) на системата, има за цел да се провери устойчивостта ѝ към външни атаки, целящи придобиване на нерегламентиран достъп и да се предприемат мерки за своевременното им отстраняване. Тестовите за проникване ще бъдат провеждани преди инсталация в тестовата среда на Възложителя, което ще позволи откриването на уязвимости и отстраняването им преди инсталацията на уязвимите компоненти в средите на Възложителя.

Тестовите ще бъдат провеждани от експерт по информационна сигурност, с компетенции на водещ одитор по стандарт ISO 27001:2013, като се използва AppSpider - софтуер за динамично тестване на сигурността на приложенията (dynamic application security testing - DAST) за проверка на комплексни приложения, включващ следните възможности:

- Бързо тестване на приложения за над 80 вида уязвимости, в това число и най-



често използваните за атака уязвимости (OWASP Top 10);

- Автоматично откриване на уязвимости в приложенията;
- Интелигентно симулиране на реални атаки за оценка на вероятността за реализация на дадена заплаха през набор от уязвимости;
- Бързо повторно възпроизвеждане на атаки с цел оценка на предприетите действия по отстраняване на уязвимости;
- Тестване на приложения, използващи както стандартна идентификация (потребителско име и парола), така и разширени методи като - Single Sign-On (SSO), OAuth, Client SSL Certificate и др.
- Тестване на динамични клиенти с API и услуги с помощта на Universal Translator (Advanced JavaScript, AJAX, GWT, JSON, REST, AMF, SOAP)
- Резултатите от тестовете се предоставят в динамични отчети, посредством които могат да се направят както общи изводи за уязвимостта на системата, така и детайлни анализи за конкретна уязвимост или метод на атака.

Прилагането на мярката ще позволи превантивно откриване на уязвимости в системата, превантивното им отстраняване и осигуряване на високо качество на защита от познати технологични уязвимости и методи за атака и проникване в системата, което намалява риска от използване на уязвимости за придобиване на нерегламентиран достъп до нея.

### **1.13. Проверка (одит) на реалното прилагане на мерките, за предотвратяване на неправомерен достъп**

Ще бъде направен цялостен одит на реалното прилагане на мерките за предотвратяване на неправомерен достъп, предвидени в политиката, процедурите и правилата за информационна сигурност на ИСУН.

В резултат от одита, който предвиждаме да направим оценка на реалното прилагане на мерките, предвидени в политиката, процедурите и правилата за информационна сигурност на ИСУН ще идентифицираме подобни проблеми и те ще бъдат отстранени в процеса на поддържане на ИСУН 2007-2013“.

Тази мярка ще доведе до реалното прилагане на мерките за предотвратяване на неправомерен достъп, предвидени в политиката, процедурите и правилата за информационна сигурност на ИСУН и така ще се намали риска от неправомерен достъп.

## **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. За всяка предложена мярка за намаляване на риска сме дали обяснение, демонстриращо как предложената мярка ще повлияе на вероятността за събъждане или въздействието на събъждането на съответния риск. 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**

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. Ще провеждаме регулярен преглед на политиките на планирани интервали от 6 месеца или при възникване на необходимост и изготвяне на предложения за актуализацията им в съответствие с най-добрите практики и в отговор на нови появили се типове заплахи.

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). Това ще намали значително вероятността от проява на риска за уязвимост към зловреден код.

### **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.

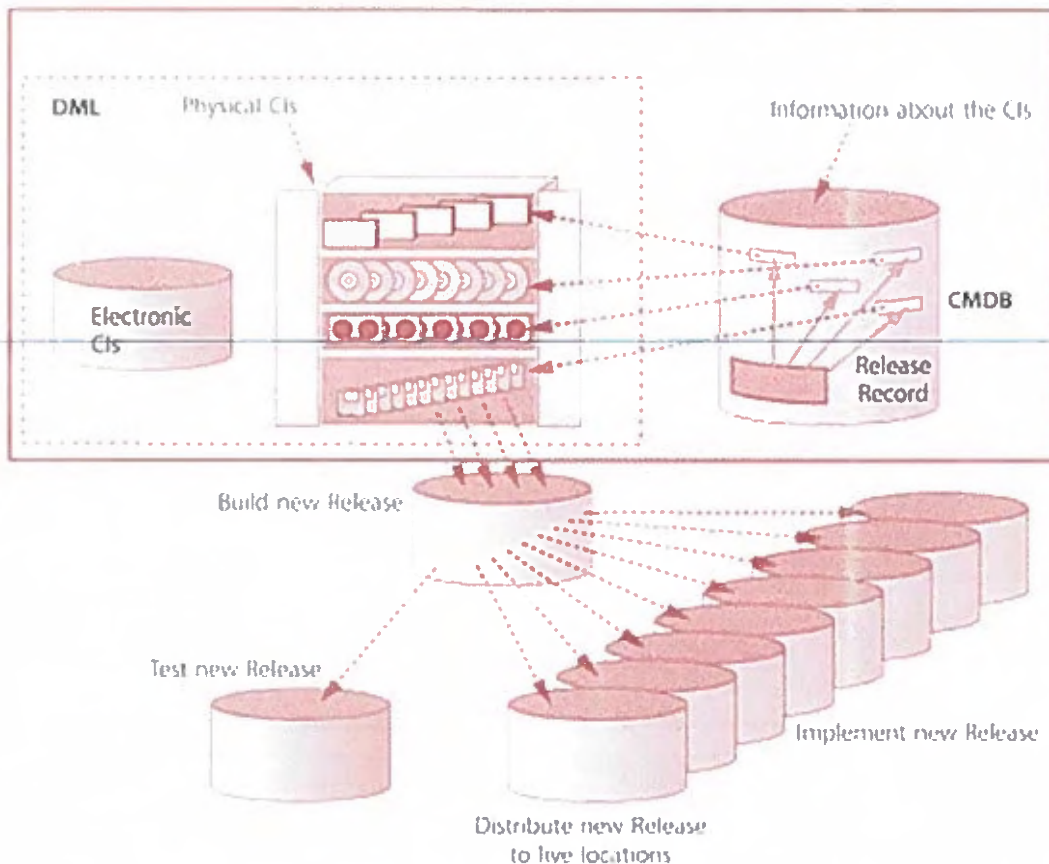
#### **2.4. Използване на Definitive Media Library (DML) за инсталация на софтуер**

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 одобренията 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 неодобрен 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. Провеждане на тестове за уязвимост на системата

За намаляване на уязвимостта от зловреден код ще проведем тестове за уязвимост (vulnerability test) на системата. Тестове за уязвимост ще бъдат провеждани и преди предоставяне на промени в системата за тестване от Възложителя.

Провеждането на тестове за уязвимост (vulnerability test) на системата, има за цел да се провери устойчивостта ѝ към външни атаки и да се предприемат мерки за своевременно им отстраняване. Тестовите за уязвимост, провеждани преди инсталация в тестовата среда на Възложителя, ще позволи откриването на уязвимости и отстраняването им преди инсталацията на уязвимите компоненти в средите на Възложителя.

Тестовите ще бъдат провеждани от експерт по информационна сигурност, с компетенции на водещ одитор по стандарт ISO 27001:2013, като се използват следните инструменти: AppSpider - софтуер за динамично тестване на сигурността на приложенията (dynamic application security testing - DAST) за проверка на комплексни приложения, включващ следните възможности:

- Бързо тестване на приложения за над 80 вида уязвимости, в това число и най-



често използваните за атака уязвимости (OWASP Top 10);

- Автоматично откриване на уязвимости в приложенията;
- Интелигентно симулиране на реални атаки за оценка на вероятността за реализация на дадена заплаха през набор от уязвимости;
- Бързо повторно възпроизвеждане на атаки с цел оценка на предприети действия по отстраняване на уязвимости;
- Тестване на приложения, използващи както стандартна идентификация (потребителско име и парола), така и разширени методи като - Single Sign-On (SSO), OAuth, Client SSL Certificate и др.
- Тестване на динамични клиенти с API и услуги с помощта на Universal Translator (Advanced JavaScript, AJAX, GWT, JSON, REST, AMF, SOAP)
- Динамични отчети за резултатите от тестовете, посредством които могат да се направят както общи изводи за уязвимостта на системата, така и детайлни анализи за конкретна уязвимост или метод на атака.

**Metasploit** - най-популярната и мощна платформа за извършване на тестове за уязвимост. Използва се за тестване на уеб базирани приложения, компютърни мрежи, сървъри, комуникационно оборудване и други за уязвимости чрез стартиране на сложни опити за атака.

Тестването посредством Metasploit има за цел да открие уязвимости на системата – т.е. технологичен пропуск, позволяващ да се направи опит и евентуално да се постигне успешно компрометиране на защитите на информационната система, чрез методи и средства използвани от причинители на зловредни атаки.

Към настоящият момент в базата на Metasploit има над 3000 експлойт модула – софтуерни компоненти, даващи възможности за възползване от уязвимости на системата и изграждащите я компоненти. След детайлно запознаване с архитектурата на системата ще бъде подбран набора от експлойти, които ще се ползват за тестване уязвимостите на системата, като задължително ще се включат експлойти за тестване на най-често използваните за атака уязвимости на уеб базирани системи: SQL injection, Cross-site Scripting и др.

Прилагането на мярката ще се позволи превантивно откриване на уязвимости във всички компоненти на системата, превантивното им отстраняване и осигуряване на високо качество на защита на информационната система срещу познати технологични уязвимости на изграждащите я компоненти и респективно намалява риска от използване на уязвимости за внедряване на зловреден код в системата.

## 2.6. 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, патоварването 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.
- 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.

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“.

## 2.7. Премахване на ненужни сървърни услуги и софтуер

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.

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.

## 2.8. Внедряване на средства за проактивен мониторинг и откриване на нетрадиционно поведение

Ще направим анализ на регистрационните файловете (log) на системата, събитията, които се регистрират в тях и данните за всеки вид събитие, които се поддържат в съответните лог файлове.

Анализ на възможностите на системата за настройка на тригери (нива на регистриране на определени видове събития), като:

- брой неуспешни опити за влизане в системата от конкретно IP/работна станция,
- опит за влизане с блокиран потребител,
- количество предизвикани грешки от определен потребител за период от време,
- определен брой изпълнения на дадени операции от даден потребител за даден период от време и др.
- определен брой заявки за сваляне или качване на файлове от един потребител за даден период (например: опит за качване или сваляне на файл 10 пъти в рамките на 1 минута).

Анализ на възможностите за автоматично уведомяване на определени длъжностни лица (администратори на потребителски профили, администратори на системи) и поведението на системата (например: заключване за потребителя за определено време или изискване на въвеждане на случайно генериран код /captcha/ за потвърждаване на операцията) при достигане на ниво на тригиране.

На база направеният анализ ще предложим мерки, включително и чрез разработка на функционалности за автоматично уведомяване, настройка на тригери, промени в структурата на лог файловете на системата. Прилагането на мярката ще фокусира вниманието на екипите по поддържане на системата към потенциално опасни действия от външни страни или съществуващи потребители и ще осигури възможност за взимане на бързи коригиращи действия и/или превенция срещу нетрадиционно поведение, което може да е заплаха за сигурността на системата.



С тази мярка ще се намали възможността за внедряване на зловреден код в системата, чрез автоматизирани атаки, ботове, търсене на уязвимости и експлойти, което ще намали риска от проникване на зловреден код в системата.

### 3. Загуба или манипулиране на данни;

Информационна система ИСУН 2007-2013 е предназначена за управление на всички аспекти от фондовете за европейско финансиране за програмният период 2014-2007-2013г. и загубата или манипулирането на каквато и да е част от данните на системата може да доведе до големи неблагоприятни последици както за бенефициентите, така и за репутацията и държавния бюджет на Р. България. 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.

На база наличните данни към момента за информационната система и обхвата на възможните дейности за изпълнение в рамките на този проект, сме 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

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 архиви 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 т.7.5.3 на 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.



Приемането на оценката на риска и плана за третиране на риска от Възложителя ще послужи за актуализиране на политиките и процедури по информационна сигурност за системата. Актуалната политика по сигурност ще намали значително вероятността от проява на риска и влиянието му при евентуално проявление.

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

В процеса на поддръжка и подобрения ще прилагаме „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 намалява 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 до 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 променени 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.

### **3.2.5. Използване на криптографски методи за защита на данни**

След анализ на използваните средства за защита, текущото състояние и чувствителните данни, ще създадем правила за използване на криптографски средства за защита на информацията в системата, които ще регламентират видовете криптографски средства които ще се използват, както и процесите и архитектурните слоеве на системата, в които ще се използват.

С внедряването на точни и ясни правила за използване на криптографски средства в слоевете и процесите, в които това е възможно и оценено като необходимо, ще се постигне много ниска вероятност на риска от манипулиране на данни в системата.

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 от загуба или манипулиране на данни.

### **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.

### **3.5. 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).

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

### **3.6. Разработка на приложен интерфейс за коригиране на данни в системата**

С цел да се подобри проследимостта предвиждаме да създадем потребителски интерфейс за извършване на корекции в базата данни, който да е достъпен в системата за потребители със съответната административна роля и права. Идеята е да се ограничат до минимум директните действия, извършвани на ниво база данни, като се постигне пълно

регистрация и проследимост на действията по корекция на данните.

Този мярка от една страна ще намали риска от загуба на данни в следствие на изпълнение на неправилна заявка на ниво база данни, а от друга ще намали риска от манипулиране на данни директно в базата данни, като добави още един слой за регистрация и проследимост на действията по корекция на данните.

### 3.7. Имплементиране на стратегия за автоматизирано оперативно резервиране на данните

В съответствие с процедурата за „Резервиране и архивиране на информацията“ ще бъде имплементирана, със средствата на системата за управление на база данни, цялостна стратегия за автоматизирано оперативно резервиране на данните. Тя е в съответствие с най-добрите практики и се базира на комбинация от три различни вида резервиране (backup) с различна честота с цел осигуряване на максимална сигурност, като архивирането на данните се извършва on-line, като това не се отразява на нормалното функциониране на системата:

- Пълно резервиране (Full backup)
- Диференциално резервиране (Differential backup)
- Резервиране на журнала за транзакции (Transaction log backup)



1. Пълно резервиране (Full backup) се изпълнява всяка седмица в неделя в 1:00 часа.

1.1. Преди стартиране на резервирането се изпълнява проверка на интегритета на данните (Check Database Integrity Task), за да сме сигурни, че архивираме данни, които не са повредени.

1.2. Изпълнява се резервирането на цялата база данни (Full Backup database task) задължително с включена опция Verify backup integrity, за да сме сигурни, че създаденото резервно копие не е повредено.

2. Диференциално резервиране (Differential backup) се изпълнява всеки ден в 22:00 часа.

2.1. Преди стартиране на резервирането се изпълнява проверка на интегритета на данните (Check Database Integrity Task), за да сме сигурни, че архивираме данни, които не са повредени.

2.2. Изпълнява се диференциално резервиране (само на промените от последния пълен архив) на базата данни (Backup database task) задължително с включена опция Verify backup integrity, за да сме сигурни, че създаденото резервно копие не е повредено.

3. Резервиране на журнала за транзакции Transaction log backup се изпълнява на всеки час от 07:30 до 20:30.

3.1. Изпълнява се резервиране само на транзакциите в базата данни от последния диференциално резервиране (Backup Transaction log task) задължително с



включена опция *Verify backup integrity*, за да сме сигурни, че създаденото резервно копие не е повредено.

4. *Maintenance cleanup* определя колко седмици назад колко архиви искаме да пазим – примерно 9 седмици, за да имаме оперативно архивирани данни за над 60 дни.
5. Изпълнение на рутинни операции по базата данни, като *History Cleanup Task* (включва „Backup and restore history“, „SQL Server Agent history“ и „Maintenance history“) – по подразбиране е 4 седмици, ще бъде настроен на 9;
6. Изпълнение на операции по цялостна оптимизация на базата данни *Rebuild Index + Update Statistics* - всяка седмица в неделя в 23:00ч., а при нарастване на базата данни и при нужда и в други дни.
7. Изпълнение на операции по оптимизация на базата данни *Reorganize Index* - всяка седмица в сряда в 23:00 а при нужда и в други дни.

Тази стратегия позволява възстановяване базата данни в рамките на 60 дни, като състоянието може да се възстановява с точност до конкретен час за всеки от тези дни.

Стратегията ще бъде имплементирана за изцяло автоматично изпълнение, чрез дефиниране на съответните планове за поддръжка (*Maintenance plans*) в *Microsoft SQL Server*, като ще се следи за правилно ѝ изпълнение.

Тази мярка директно намалява вероятността за реализация на риска от загуба на данни, като имплементира напълно автоматизирана и практически приложима стратегия за резервиране на данните в оперативен архив.

### 3.8. 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.

### 3.9. Защита от неправомерен достъп

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

### 3.10. Налагане на механизми за контрол на правата на потребителите

При разработването на системата ще бъде приложен принципа за проверка, че потребителя е идентифициран и валидиране, 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 спази 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. Защита от неправомерен достъп до вътрешната (непублична част) на системата**

Особено сериозен риск съществува при неправомерен достъп до вътрешната част (непублична) на системата, тъй като вътрешните потребители (служебни потребители и поддържащи екипи) имат достъп до много по-голям обем информация, а също и по-големи права.

Въвеждане на възможност за двустепенна идентификация (2FA) с допълнителна еднократна парола (шест цифри), получавана на мобилен телефон за всички потребители



на вътрешната част на системата, като се използват стандартни безплатни приложения за смарт телефони или SMS/email. Подходящи приложения за целта са Microsoft Authenticator, Google Authenticator, Lastpass Authenticator, които са безплатни и налични за всички мобилни операционни системи. За да не се затормозяват ежедневните потребители след еднократна двустепенна идентификация (2FA), съответния браузър ще може да се запише като безопасен, за да не се изисква допълнителната еднократна парола за определено време (примерно един месец). Ще бъде реализирана възможност за настройка на двустепенна идентификация (2FA) за всяка от ролите в системата, като за административните роли препоръчваме да е включена по подразбиране.

Тази мярка намалява риска от нарушаване на конфиденциалността на чувствителни данни за сметка на достъп с неправомерно получени валидни идентификационни данни на служебни потребители и поддържащи екипи.

#### **4.3. Анализ на съществуващите роли и права за достъп**

Ще направим 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.

#### **4.4. 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).

#### **4.5. 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.

Този 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.

#### **4.6. Криптиране на чувствителни данни, съхранявани в системата**

Ще направим оценка дали някои данни 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.

#### **4.7. 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.

#### **4.8. 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 съвършен 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.

#### 4.9. Използването на сертификати с разширено валидиране (EV SSL) за сървърите на системата

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.

Визуализация на EV SSL сертификати в основните браузъри:



Използването на EV SSL осигурява най-сигурното криптиране на данните, а също и ясна визуална индикация, че потребителите работят на истинския сайт на системата, а не на негово копие. Възможността потребителя да идентифицира визуално във всеки момент само с един поглед, че се намира в истинската система защитава срещу phishing атаки, при което хакери създават фалшиво копие на сайта на системата, в което подмамват потребителите да въведат името и паролата за достъп. Обикновено това става с изпращане на имейл, съдържащ препратка към фалшивото копие, маскирана като истинска. По този начин се сдобиват с потребителско име и парола, които в последствие могат да използват в истинската система и да достигнат неправомерно до цялата информация, до която дадения потребител има достъп.

Прилагането на тази мярка драстично намалява риска от нарушаване конфиденциалността на чувствителните данни, като защитава най-чувствителната информация – данните за идентификация на потребителя, както при обмен, така и от опити за разкриването им с измама (phishing атаки).

#### 4.10. Защитен обмен на данни с други системи

Обмена на данни с външни системи и приложения ще се изпълнява по защитени канали за комуникация, гарантиращи висока степен на защита от нарушаване конфиденциалността на чувствителните данни. 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.

Защитата на транспортната среда е един от основните фактори за осигуряване на защита от нарушаване конфиденциалността на чувствителните данни, като предложените правила, които ще се спазват при изпълнението на дейностите ще поддържа на ниско ниво вероятността от прихващане на данни в транспортните среди между компонентите на системата и потребителите и следователно ще намалява риска за нарушаване конфиденциалността на чувствителните данни до системата.

При проектирането на интерфейс 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, а само за чувствителни данни, тъй като намалява риска за нарушаване конфиденциалността им при обмен с други системи.

Прилагането на тази мярка намалява риска от нарушаване конфиденциалността на чувствителните данни, като ги криптира веднъж, за да гарантира автентичността им и втори път, като позволява декриптирането им само от получателя на данните.

#### 4.11. 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.

#### 4.12. 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 неговата 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.

Успешна защита в случая е заключването на потребителския профил в случай, че бъдат направени повече от 5 неуспешни опита за влизане в системата в рамките на 5 минути. В този случай, съответният профил се заключва, като на потребителя се изпраща уведомяващ имейл с хипервръзка (линк) за принудителна смяна на паролата. В „3.4-Изисквания към потребителските идентификатори“ от правилата и процедурите за контрол на достъпа до ИТ активите, в т.3.4.5(е) (стр.20) е дефинирана подобна мярка, но тя не е реализирана в системата (включително и в реалната среда). Този подход няма да създава допълнително натоварване и ангажимент на административните потребители от ЦКЗ.

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.

#### 4.13. 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 на приложните модули, в който

лишават задни вратички (back doors) и DML за всички компоненти на системата.

## **5. Възможни срывове на системата поради грешни действия на изпълнителя.**

Предвид обхвата на оказваните услуги в рамките на обществената поръчка, потенциална реализация на риска от срывове на информационна система ИСУН 2007-2013 поради грешни действия на Изпълнителя може да доведе до сериозни последствия.

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 последствия при реализация на риск „Възможни срывове на системата поради грешни действия на изпълнителя“, ще прилагаме следният комплекс от мерки:

### **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 срывове на системата, поради грешни действия на изпълнителя.

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 срывове в системата поради грешни действия на изпълнителя.

Целият екип, който предлагаме за изпълнение на поръчката вече е осъществявал поддръжка на ИСУН 2007-2013 и познава отлично системата. Специалистите от екипа са запознати и имат практически опит с всички модули, архитектурата и особеностите на системата.

Прилагането на мярката намалява както вероятността, така и последствията 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.

### **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 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 срывове 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 срывове 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 ролята 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 отговорности е предпоставка за своевременно откриване на потенциални проблеми и реализация на механизми за тяхното отстраняване, което намалява вероятността от реализация на риска от срывове 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 6 месеца.

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 на товарването 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 сривове 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) 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 неодобрен 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 сригове на системата вследствие на действие или бездействие на експерти на Изпълнителя.

### 5.8. Анализ на досегашни сригове 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 сригове на системата поради грешни действия на изпълнителя, ако има данни за такива, като изследваме причините довели до срив в системата и набележим конкретни мерки за предотвратяването сригове 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 аварияте 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.

### 5.9. Анализ на действията при изпълнение на договора

Предвиждаме създаването на експертна работна група от експерти, сертифицирани по ITIL и ISO27001, за анализ изпълнението на договора и спазване на изискванията за сигурност, достъпност и непрекъсваемост. Експертната работна група ще осъществява регулярен преглед веднъж на 6 месеца, а при значими инциденти и по-често, на всички действия по изпълнение на договора.

В обхвата на прегледа от експертната работна група ще бъде изготвен анализ на регистрираните действия и дейности в процеса на изпълнение на договора, реакции при докладвани събития/инциденти, изпълнени регулярни действия и резултатите от тях и др. Ще бъде направен преглед и анализ на:

- Плановите 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 плановите 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 от анализа при необходимост ще се планират и прилагат превантивни и коригиращи дейности за увеличаване достъпността и сигурността на информационната система.

Този мярка ще осигури непрекъснато намаляване на вероятността и въздействието на риска „Възможни сринове на системата поради грешни действия на изпълнителя“ в хода на изпълнение на поръчката.

Предложените мерки за намаляване на риска са изготвени на база опита в поддръжката а ИСУН 2007-2013 и ИСУН 2007-2013, както и най-добрите практики заложи в ITIL и стандартите за информационна сигурност ISO27002:2013 Code of practice и ISO20000-2:2012 и опита ни в разработката и поддръжката на уеб-базиран информационни системи.

### 3.2. Предложения за подобряване на Публичния модул и вътрешната среда на ИСУН 2007-2013:

#### 1. Корекция на данни във вътрешната среда

**Описание:** Предложената промяна включва въвеждане на ново право в ИСУН 2007-2013 за администратор на информацията и създаването на функционалност, позволяваща на потребител с новосъздадените административни права да нанася корекции в информацията, въведена в ИСУН 2007-2013.

**Обосновка:** Предложената мярка е целесъобразна с оглед необходимостта от дългосрочното отстраняване на въведени от потребителите технически грешки, водещи до извеждането на некоректни данни в системата и преустановяването на некоректната практика от нанасянето на корекции в базите данни с програмни средства.

**Срок за внедряване:** 8 месеца след подписване на договор за изпълнение на поръчката.

#### 2. Електронна комуникация в ИСУН 2007-2013

**Описание:** Предложената функционалност включва въвеждането на възможност за изпращане на съобщения от потребители от различни организации, което ще доведе до намаляване на хартиената комуникация между институциите и ще гарантира наличието на адекватна одитна следа в дългосрочен план.

**Обосновка:** В процеса на управление на програмите са установени случаи на допуснати технически грешки от страна на потребителите при въвеждането на информация в системата. В много от случаите за отстраняването на тези грешки се води официална кореспонденция на хартиен носител, която не е налична в системата. С оглед оптимизирането и дигитализирането на процеса е обосновано, въвеждането на форма за комуникация между организациите, използващи ИСУН 2007-2013 (управляващи органи, междинни звена, сертифициращ орган и други) и ЦКЗ.

**Срок за внедряване:** 6 месеца след подписване на договор за изпълнение на поръчката.

#### 3. Разширяване на номенклатурите, въведени от ЦКЗ

**Описание:** Предложената функционалност включва възможност за въвеждането на допълнителни номенклатури в системата, които не изискват програмна намеса и могат да бъдат извършени със средствата на потребителския интерфейс.

**Обосновка:** Предложената функционалност позволява на потребителя да въведе номенклатури, които към момента са заложили в програмния код на системата и за техните допълнения се изисква намеса на програмно ниво. Пример за това са допустимите години за въвеждане на информация в системата, като всяка година е необходима намеса от страна на оторизирани програмисти.

**Срок за внедряване:** 7 месеца след подписване на договор за изпълнение на поръчката.





IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world.  
IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.

# СЕРТИФИКАТ № CERTIFICATE No. ITSMS-28/13

УДОСТОВЕРЯВА, ЧЕ СИСТЕМАТА ЗА УПРАВЛЕНИЕ НА ИТ УСЛУГИТЕ НА  
IT IS HEREBY CERTIFIED THAT THE INFORMATION TECHNOLOGY SERVICE MANAGEMENT SYSTEM OPERATED BY

**ДАВИД ХОЛДИНГ АД**  
**DAVID HOLDING INC**

УЛ. СТАРА РЕКА 2, ДК АРСЕНАЛ, КАЗАНЛЪК 6100, БЪЛГАРИЯ  
2, STARA REKA STR., DK ARSENAL, 6100 KAZANLAK, BULGARIA

ЗА СЛЕДНИТЕ ОПЕРАТИВНИ СТРУКТУРИ / IN THE FOLLOWING OPERATIONAL UNITS

УЛ. СТАРА РЕКА 2, ДК АРСЕНАЛ, КАЗАНЛЪК 6100, БЪЛГАРИЯ  
2, STARA REKA STR., DK ARSENAL, 6100 KAZANLAK, BULGARIA

СЪОТВЕТСТВА НА СТАНДАРТ / IS IN COMPLIANCE WITH THE STANDARD

**ISO/IEC 20000-1:2011**

С ОБЛАСТ НА ПРИЛОЖЕНИЕ / FOR THE FOLLOWING FIELD(S) OF ACTIVITIES

СИСТЕМА ЗА УПРАВЛЕНИЕ НА ИТ УСЛУГИТЕ ОСИГУРЯВАЩА ПРЕДОСТАВЯНЕТО ИТ УСЛУГИ ЗА  
ИНФОРМАЦИОННИ СИСТЕМИ НА ВЪНШНИ КЛИЕНТИ СЪГЛАСНО КАТАЛОГА НА УСЛУГИТЕ.

IAF:33  
IAF:35

THE IT SERVICE MANAGEMENT SYSTEM SUPPORTING THE PROVISION OF IT SERVICES FOR INFORMATION  
SYSTEMS FOR EXTERNAL CLIENTS IN ACCORDANCE WITH THE SERVICE CATALOGUE.

Валидността на този сертификат зависи от резултатите от годишните одити и цялостния преглед на системата за управление на всеки три години.

The validity of this certificate is dependent on an annual audit and on a complete review, every three years, of the management system.

Използването и валидността на този сертификат зависят от спазването на правилата на РИНА за сертификация на системи за управление на ИТ услугите.

The use and validity of this certificate are subject to compliance with the RINA Rules for the certification of Information Technology Service Management Systems.

Първо издание First Issue	28.03.2013
Валидност до Expiry Date	21.01.2022
Последна промяна Revision date	19.01.2019
Подновен на Renewal decision date	19.01.2019

Kalin Panev  
Bulgaria Certification  
Head

RINA Services S.p.A.  
Via Corsica 12 - 16128 Genova Italy



ITX N° 002 L

Signatory of EA, IAF and ILAC  
Mutual Recognition Agreements



Върно сортирнал  
Базов джикер



www.cisq.com





СЕРТИФИКАТ №

49/11

CERTIFICATE No.

УДОСТОВЕРЯВА, ЧЕ СИСТЕМАТА ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА НА  
IT IS HEREBY CERTIFIED THAT THE INFORMATION SECURITY MANAGEMENT SYSTEM OPERATED BY

**ДАВИД ХОЛДИНГ АД**  
**DAVID HOLDING INC**

УЛ. СТАРА РЕКА 2, ДК АРСЕНАЛ, ЕТ. 4, ОФИС 417, КАЗАНЛЪК 6100, БЪЛГАРИЯ  
2, STARA REKA STR., DK ARSENAL, FL. 4, OFFICE 417, 6100 KAZANLAK, BULGARIA

ЗА СЛЕДНИТЕ ОПЕРАТИВНИ СТРУКТУРИ / IN THE FOLLOWING OPERATIONAL UNITS

УЛ. СТАРА РЕКА 2, ДК АРСЕНАЛ, ЕТ. 4, ОФИС 417, КАЗАНЛЪК 6100, БЪЛГАРИЯ  
2, STARA REKA STR., DK ARSENAL, FL. 4, OFFICE 417, 6100 KAZANLAK, BULGARIA

СЪОТВЕТСТВА НА СТАНДАРТ / IS IN COMPLIANCE WITH THE STANDARD

**ISO/IEC 27001:2013**

С ОБЛАСТ НА ПРИЛОЖЕНИЕ / FOR THE FOLLOWING FIELD(S) OF ACTIVITIES

ПРОЕКТИРАНЕ, РАЗРАБОТКА, ВНЕДРЯВАНЕ И ПОДДРЪЖКА НА СОФТУЕР, ИНФОРМАЦИОННИ СИСТЕМИ И ИТ  
РЕШЕНИЯ. ДОСТАВКА, ВНЕДРЯВАНЕ И ПОДДРЪЖКА НА ГЕОГРАФСКИ ИНФОРМАЦИОННИ СИСТЕМИ.  
СИСТЕМНА ИНТЕГРАЦИЯ. ИТ И КОНСУЛТАНТСКИ УСЛУГИ. УПРАВЛЕНИЕ НА ПРОЕКТИ.

За информация относно  
валидността на  
сертификата може да  
посетите [www.rina.org](http://www.rina.org)

For information concerning  
validity of the certificate, you  
can visit the site  
[www.rina.org](http://www.rina.org)

Валидността на този сертификат  
зависи от годишните /  
шестмесечните одити и от цялостния  
преглед на системата за управление  
на всеки три години.

The validity of this certificate is  
dependent on an annual / six monthly  
audit and on a complete review, every  
three years, of the management  
system

IAF:33  
IAF:35

ДЕКЛАРАЦИЯ ЗА ПРИЛОЖИМОСТ,  
ВЕРСИЯ 8 ОТ 02.11.2016.  
STATEMENT OF APPLICABILITY,  
VER. 8, DATED 02.11.2016.

DESIGN, DEVELOPMENT, IMPLEMENTATION AND SUPPORT OF SOFTWARE, INFORMATION SYSTEMS AND IT  
SOLUTIONS. SUPPLY, IMPLEMENTATION AND SUPPORT OF GEOGRAPHIC INFORMATION SYSTEMS. SYSTEM  
INTEGRATION. IT AND CONSULTING SERVICES. PROJECT MANAGEMENT.

Използването и валидността на сертификата зависят от спазването на правилата за сертификация на РИНА  
The use and validity of this certificate are subject to compliance with the relevant RINA rules

Първо издание First Issue	14.06.2011
Валидност до Expiry Date	21.01.2022
Последна промяна Revision date	19.01.2019
Подновен на Renewal decision date	19.01.2019

Kalin Panev

Bulgaria Certification  
Head

RINA Services S.p.A.  
Via Corsica 11, 10128 Genova Italy



SSI N° 001 G

Signatory of EA, IAF and ILAC  
Mutual Recognition Agreements



[www.cisq.com](http://www.cisq.com)

CISQ е Италианската Федерация на Органите по  
Сертификация на Системи за управление  
CISQ is the Italian Federation of  
management system Certification Bodies





IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world.  
IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.

СЕРТИФИКАТ №

23323/11/S

CERTIFICATE №.

УДОСТОВЕРЯВА, ЧЕ СИСТЕМАТА ЗА УПРАВЛЕНИЕ НА КАЧЕСТВОТО НА  
IT IS HEREBY CERTIFIED THAT THE QUALITY MANAGEMENT SYSTEM OF

**ДАВИД ХОЛДИНГ АД**  
**DAVID HOLDING INC**

За информация относно  
валидността на  
сертификата може да  
посетите [www.rina.org](http://www.rina.org)

For information concerning  
validity of the certificate, you  
can visit the site  
[www.rina.org](http://www.rina.org)

УЛ. СТАРА РЕКА 2, ДК АРСЕНАЛ, ЕТ. 4, ОФИС 417, КАЗАНЛЪК 6100, БЪЛГАРИЯ  
2, STARA REKA STR., DK ARSENAL, FL. 4, OFFICE 417, 6100 KAZANLAK, BULGARIA

ЗА СЛЕДНИТЕ ОПЕРАТИВНИ СТРУКТУРИ / IN THE FOLLOWING OPERATIONAL UNITS

УЛ. СТАРА РЕКА 2, ДК АРСЕНАЛ, ЕТ. 4, ОФИС 417, КАЗАНЛЪК 6100, БЪЛГАРИЯ  
2, STARA REKA STR., DK ARSENAL, FL. 4, OFFICE 417, 6100 KAZANLAK, BULGARIA

Неприложимите изисквания на  
стандарта могат да бъдат  
намерени в документираната  
информация на организацията.

Reference is to be made to the  
relevant documented information  
for the requirements of the  
standard that cannot be applied to  
the Organization's management  
system scope

СЪОТВЕТСТВА НА СТАНДАРТ / IS IN COMPLIANCE WITH THE STANDARD

**ISO 9001:2015**

С ОБЛАСТ НА ПРИЛОЖЕНИЕ / FOR THE FOLLOWING FIELD(S) OF ACTIVITIES

ПРОЕКТИРАНЕ, РАЗРАБОТКА, ВНЕДРЯВАНЕ И ПОДДРЪЖКА НА СОФТУЕР, ИНФОРМАЦИОННИ СИСТЕМИ И  
ИТ РЕШЕНИЯ. ДОСТАВКА, ВНЕДРЯВАНЕ И ПОДДРЪЖКА НА ГЕОГРАФСКИ ИНФОРМАЦИОННИ СИСТЕМИ.  
СИСТЕМНА ИНТЕГРАЦИЯ. ИТ И КОНСУЛТАНТСКИ УСЛУГИ. УПРАВЛЕНИЕ НА ПРОЕКТИ.

IAF:33  
IAF:35

DESIGN, DEVELOPMENT, IMPLEMENTATION AND SUPPORT OF SOFTWARE, INFORMATION SYSTEMS AND IT  
SOLUTIONS. SUPPLY, IMPLEMENTATION AND SUPPORT OF GEOGRAPHIC INFORMATION SYSTEMS. SYSTEM  
INTEGRATION. IT AND CONSULTING SERVICES. PROJECT MANAGEMENT.

Организацията е сертифицирана по  
гореуказвания стандарт от 28.01.2010.

This Organisation is certified for the  
above standard since 28.01.2010.

Валидността на този сертификат зависи от годишните / шестмесечните одити и от цялостния преглед на системата за управление на всеки три години.  
The validity of this certificate is dependent on an annual / six monthly audit and on a complete review, every three years, of the management system  
Използването и валидността на сертификата зависят от спазването на правилата на RINA за сертификация на системи за управление на качеството.  
The use and validity of this certificate are subject to compliance with the RINA document: Rules for the certification of Quality Management Systems

Първо издание  
First Issue

10.06.2011

Валидност до  
Expiry Date

21.01.2022

Последна промяна  
Revision date

19.01.2019

Подновен на  
Renewal decision date

19.01.2019

Kalin Panev

Bulgaria Certification  
Head

RINA Services S.p.A.  
Via Corsica 12 - 16128 Genova Italy



SGQ N° 002 A

Signatory of EA, IAF and ILAC  
Mutual Recognition Agreements



Върно с оригинала  
Балчо Динев



[www.cisq.com](http://www.cisq.com)

CISQ е Италианската Федерация на Органите по  
Сертификация на Системи за управление  
CISQ is the Italian Federation of  
management system Certification Bodies

Приложение № 6

**ДЕКЛАРАЦИЯ**  
**по чл. 47, ал. 3 от Закона за обществените поръчки**

Долуподписаният Бальо Атанасов Динев  
в качеството ми на Изпълнителен директор (посочва се длъжността и качеството, в  
което лицето има право да представлява и управлява - напр. изпълнителен  
директор, управител или др.) на „ДАВИД Холдинг“ АД (посочва се наименованието  
на участника), с ЕИК 833092882, със седалище и адрес на управление: гр. Казанлък,  
ул. „Стара река“ 2, офис 417 – участник в процедура за възлагане на обществена  
поръчка с предмет: „Осигуряване на поддръжка на ИСУН за програмния период  
2007-2013“.

**ДЕКЛАРИРАМ, че:**

При изготвяне на офертата са спазени задълженията, свързани с данъци и  
осигуровки, опазване на околната среда, закрила на заетостта и условията на труд, които  
са в сила в страната.

Известно ми е, че за неверни данни нося наказателна отговорност по чл. 313 от  
Наказателния кодекс.

И т . с . , . . . . .

Длъжност: Изпълнителен директор

Длъжност: Изпълнителен директор

Подпис и печат.



Приложение № 7

ДО  
МИНИСТЕРСКИ СЪВЕТ  
гр. София, бул. „Княз Ал. Дондуков“ № 1

**ЦЕНОВО ПРЕДЛОЖЕНИЕ**

в процедура за възлагане на обществена поръчка с предмет:

**„Осигуряване на поддръжка на ИСУН за програмния период 2007-2013“.**

от „ДАВИД Холдинг“ АД (наименование на участника), ЕИК/БУЛСТАТ: 833092882, представлявано от Бальо Атанасов Динев (*трите имена*) в качеството на длъжност, или друго качество), адрес гр. Казанлък, ул. „Стара река“ 2, офис 417, телефон 02 490 1600 факс 0431 62253, електронна поща [info@david.bg](mailto:info@david.bg)

**УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,**

С настоящото Ви представяме нашето ценово предложение за изпълнение на обявената от Вас обществена поръчка с предмет: „Осигуряване на поддръжка на ИСУН за програмния период 2007-2013“, както следва:

**1. Абонаментна цена за услугата за 1 месец: 9876.00 (девет хиляди осемстотин седемдесет и шест) лева без ДДС или 11851.20 (единадесет хиляди осемстотин петдесет и един лева и 20 стотинки) с включен ДДС.**

*Абонаментната цена за услугата за 1 месец не може да надхвърля стойността от 10 500,00 (десет хиляди и петстотин) лева без ДДС.*

*\*Забележка: В случай че договорът не влезе в сила на първо число, за първия непълен месец, цената се определя по следния начин: цената по т. 1, разделена на броя дни в конкретния месец и умножена по броя на дните от влизането в сила на договора до 1-во число на следващия месец.*

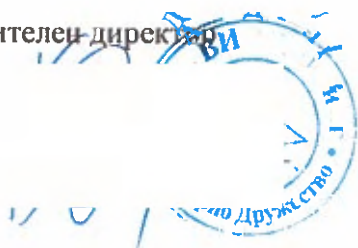
**2. В случай че е налице разминаване между цената, посочена без ДДС и тази, посочена с включен ДДС, за релевантна се приема цената без ДДС.**

**3. Посочената цена включва всички разходи по изпълнение на поръчката.**

Име и фамилия: Бальо Динев

Длъжност: Изпълнителен директор

Подпис и печат: \_\_\_\_\_



## СПИСЪК

на документите, доказващи опита на членовете на екипа на ДАВИД ХОЛДИНГ АД, за изпълнение на обществена поръчка по чл. 18, ал. 1, т. 1 от ЗОП с предмет: „Осигуряване на поддръжка на ИСУН за програмния период 2007-2013“

### I. Списък на Референции от клиенти

- Референция (1) – от Държавен фонд Земеделие (ДФЗ) по проект „Разширение, внедряване, обновяване и поддръжка на уеб-базирана информационна система за управление на документооборота“.
- Референция (2) – от Изпълнителна агенция по горите (ИАГ) по проект „Анализ, разработване и внедряване на електронни административни услуги от 3-то и 4-то ниво“.
- Референция (3) – по проект Виртуална система за електронно-комуникативна връзка, свързана с административното обслужване на граждани, фирми и организации – външни контрагенти на Изпълнителна агенция “Автомобилна администрация” (ИААА)
- Референция (4) – от ИААА за разработка, внедряване и поддръжка на софтуерна система за управление на документи и работни процеси Archimed eDMS
- Референция (5) – от Министерство на физическото възпитание и спорта (МФВС) по проект „Надграждане и интегриране на информационните системи на МФВС съобразно закона за електронно управление и модернизиране и развитие на електронния сайт на МФВС до информационен портал с оглед въвеждането на електронно обслужване във връзка с изпълнение на проект „Модерни практики и иновативно обслужване в сферата на младежкото развитие и спорта“.
- Референция (6) – от Агенцията за социално подпомагане (АСП) по проект „Внедряване, поддръжка, актуализация, развитие и комплексна системно-техническа помощ и обучение на служители в АСП, на интегрирана автоматизирана информационна система“.
- Референция (7) – от АСП по проект „Внедряване, поддръжка, актуализация, развитие и комплексна системно-техническа помощ и обучение на служители в АСП, на интегрирана автоматизирана информационна система“.

### II. Списък на Препоръки от Участника

- Препоръка (1) – от ДАВИД Холдинг АД за проект EUnet - Разработка, внедряване и поддръжка на информационна система за обработка на съобщения, получавани от Европейския съюз“.
- Препоръка (2) – от ДАВИД Холдинг АД за проект „Надграждане на Виртуална система за електронно-комуникативна връзка, свързана с административното обслужване на граждани, фирми и организации – външни контрагенти на Изпълнителна агенция “Автомобилна администрация”“
- Препоръка (3) – от ДАВИД Холдинг АД за проект в НЦЗПБ „Изграждане на интегрирана информационна система в НЦЗПБ“

Към списъка от сертификати на всеки експерт - в раздел III, е посочена референция или препоръка, за проект, в който той е участвал.

Сертификатите на език, различен от български са придружени от превод от авторизиран преводач.





### III. Списък на Сертификати на експертите от екипа на Участника

#### **1. (SN) Стойчо Недев Стойчев - Ръководител на екип**

Сертификат: PRINCE 2 Foundation , Издател: APMG International

Сертификат: Подготовка за изпит PMP, Издател: TenStep България

Сертификат: Управление на проекти, Издател: Projecta BG

Участвал е като експерт по Управление на проекти, посочени в следните референции:

Референция (1) – от Държавен фонд Земеделие

Референция (2) – от Изпълнителна агенция по горите

Препоръка (2) – от ДАВИД Холдинг АД за проект в ИААА

Референция (3) – от ИААА

Препоръка (1) – от ДАВИД Холдинг АД за проект EUNet

#### **2. (YS) Йовка Начева Стаменова - Бизнес аналитик**

Сертификат: Certified Business Analysis Professional™ (CBAP®), Издател: International Institute of Business Analysis

Участвал е като експерт Бизнес анализатор по проекти, посочени в следните референции:

Препоръка (3) – от ДАВИД Холдинг АД за проект в НЦЗПБ

Референция (2) – от Изпълнителна агенция по горите

Препоръка (2) – от ДАВИД Холдинг АД за проект в ИААА

Референция (3) – от ИААА

#### **3. (VD) Валери Петров Дачев - Експерт „Програмиране”**

Сертификат: Microsoft Certified Technology Specialist .Net Framework 2.0: Web Applications, Издател: Microsoft Certified Professional

Сертификат: TS: Microsoft® .NET Framework 2.0 - Web-based Client

Development, Издател: Microsoft Certified Professional

Сертификат: TS: Microsoft® .NET Framework 2.0 - Application Development

Foundation, Издател: Microsoft Certified Professional

Участвал е като експерт Програмист по проекти, посочени в следните референции:

Референция (1) – от Държавен фонд Земеделие

Референция (2) – от Изпълнителна агенция по горите

Препоръка (2) – от ДАВИД Холдинг АД за проект в ИААА

Референция (5) – от ММС

Референция (3) – от ИААА

#### **4. (ЕМ) Евгений Венциславов Младенов - Експерт „Програмиране”**

Сертификат: Microsoft Certified Solutions Associate: SQL Server 2012/2014, Издател: Microsoft

Участвал е като експерт Програмист по проекти, посочени в следните референции:

Референция (1) – от Държавен фонд Земеделие

Референция (2) – от Изпълнителна агенция по горите

Препоръка (2) – от ДАВИД Холдинг АД за проект в ИААА

Референция (5) – от ММС

Референция (3) – от ИААА

#### **5. (YF) Йордан Георгиев Фотев - Експерт „Системно администриране“**

Сертификат: Microsoft Certified Solutions Associate: SQL Server 2012/2014

Участвал е като експерт Системен администратор по проекти, посочени в следните референции:

Референция (1) – от Държавен фонд Земеделие

Референции (6 и 7) – от АСП

Референция (2) – от Изпълнителна агенция по горите

Препоръка (2) – от ДАВИД Холдинг АД за проект в ИААА



=====



## АВИЗО ПРЕВОДНО НАРЕЖДАНЕ



Номер на операцията / Operation number <b>963B1001916906ZN</b>		Дата и час на операцията / Operation date time <b>18.06.2019 09:11:47</b>																	
Платете на - име на получателя / Beneficiary Name <b>Администрация на министерски съвет</b>																			
IBAN на получателя / Beneficiary IBAN <b>BG38BNBG96613300157901</b>		BIC на банката на получателя / Beneficiary Bank <b>BIBG BGSD</b>																	
При банка - име на банката на получателя / Bank Name <b>БЪЛГАРСКА НАРОДНА БАНКА</b>		Вид плащане*** / Payment Type <b>000000</b>																	
<b>ПРЕВОДНО НАРЕЖДАНЕ за плащане от/към бюджета</b>		Валута / Currency <b>BGN</b>	Сума / Amount <b>14 814.00</b>																
<b>PAYMENT ORDER for Budget Payment</b>																			
Основание за плащане / Details of Payment <b>Гаранция за изпълнение</b>																			
Още пояснения / Additional Details <b>Заповед ФС-57/30.05.2019 г.</b>																			
Вид док.* / Type <b>9</b>	Номер на документа, по който се плаща/Number of Document		Дата на документа /Date																
Период, за който се плаща / Period of Payment От дата / From Date	До дата / To Date																		
Задължено лице - наименование на юридическото лице или трите имена на физическото лице/ Obligated Person - Legal Entity or Individual <b>ДАВИД ХОЛДИНГ АД</b>																			
БУЛСТАТ на задълженото лице / BULSTAT <b>833092882</b>	ЕГН на задълженото лице / Personal Number	ЛНЧ на задълженото лице / Personal ID																	
Наредител - наименование на юридическото лице или трите имена на физическото лице / Customer <b>ДАВИД ХОЛДИНГ АД</b>																			
IBAN на наредителя / Ordering Customer IBAN <b>BG14UNCR76301005019607</b>		BIC на банката на наредителя / Customer Bank BIC <b>UNCRBG SF</b>																	
При банка - име на банката на наредителя / Bank Name <b>УНИКРЕДИТ БУЛБАНК АД</b>																			
Платежна система / Payment System <b>BISERA</b>	Такси** / Taxes <b>2</b>	Вид плащане*** / Payment Type																	
Дата на регистрация / Payment system registration date <b>18.06.2019</b>		Номер на регистрация / Payment system registration number																	
<p>*Вид документ:</p> <table border="0"> <tr> <td>1 – декларация</td> <td>5 – парт. номер на имот</td> <td>**Такси:</td> <td>***Вид плащане - ползва се</td> </tr> <tr> <td>2 - ревизионен акт</td> <td>6 – постановление за принудително събиране</td> <td>1 - за сметка на наредителя</td> <td>за сметки на администратори</td> </tr> <tr> <td>3 – наказ. постановление</td> <td>9 - други</td> <td>2 - споделени (стандарт за местни преводи)</td> <td>на приходи и на Централния бюджет</td> </tr> <tr> <td>4 – авансова вноска</td> <td></td> <td>3 - за получателя</td> <td></td> </tr> </table>				1 – декларация	5 – парт. номер на имот	**Такси:	***Вид плащане - ползва се	2 - ревизионен акт	6 – постановление за принудително събиране	1 - за сметка на наредителя	за сметки на администратори	3 – наказ. постановление	9 - други	2 - споделени (стандарт за местни преводи)	на приходи и на Централния бюджет	4 – авансова вноска		3 - за получателя	
1 – декларация	5 – парт. номер на имот	**Такси:	***Вид плащане - ползва се																
2 - ревизионен акт	6 – постановление за принудително събиране	1 - за сметка на наредителя	за сметки на администратори																
3 – наказ. постановление	9 - други	2 - споделени (стандарт за местни преводи)	на приходи и на Централния бюджет																
4 – авансова вноска		3 - за получателя																	

**ВАРНО С  
ОРИГИНАЛА!**

