ДОПЪЛНИТЕЛНО СПОРАЗУМЕНИЕ
№ 01

към Договор за обществена поръчка с предмет „Разработване, внедряване и поддръжка на единна национална електронна уеб-базирана платформа: Централизирана автоматизирана информационна система „Електронни обществени поръчки“ (ЦАИС ЕОП)“ от 14.12.2017 г.

Днес, 30/10/2019 г. в гр. София, между страните по Договор за обществена поръчка с предмет „Разработване, внедряване и поддръжка на единна национална електронна уеб-базирана платформа: Централизирана автоматизирана информационна система „Електронни обществени поръчки“ (ЦАИС ЕОП)“, сключен на 14.12.2017 г., наричан по-нататък за краткост „Договора“:

1. АГЕНЦИЯ ПО ОБЩЕСТВЕНИ ПОРЪЧКИ (АОП), със седалище и адрес на управление: гр. София, п.к. 1000, ул. “Леге” № 4, ЕИК 131236380, представлявана от **Михаил Михайлов** – главен секретар, възложител съгласно заповед № РД-48/24.06.2019 г., и **Дениза Станкова -** главен счетоводител,

наричана за краткост **ВЪЗЛОЖИТЕЛ**,

и

2. КОНСОРЦИУМ „ЕОП България“, със седалище: гр. София и адрес за кореспонденция: гр. София, ул. Панайот Волов № 2, ЕИК 177156956, представляван от **Ивайло Филипов**, изпълнителен директор на „Информационно обслужване“ АД,

наричан за краткост **ИЗПЪЛНИТЕЛ**,

на основание чл. 116, ал. 1, т. 2 от ЗОП, във връзка с възникнала поради непредвидени обстоятелства необходимост от извършване на допълнителни услуги, които не са включени в предмета на Договора, и с оглед на това, че извършването им от изпълнител, различен от този по Договора би предизвикало значителни затруднения, свързани с поддръжката, експлоатацията и обслужването на ЦАИС ЕОП,

се сключи настоящото допълнително споразумение за следното:

I. ПРЕДМЕТ

Чл. 1. (1) ВЪЗЛОЖИТЕЛЯТ възлага, а **ИЗПЪЛНИТЕЛЯТ** приема да изпълни срещу възнаграждение дейности по системно администриране на ЦАИС ЕОП през периода на изпълнение на Договора, които не са включени в неговия обхват, но са наложителни за осигуряване на наличността, работоспособността и достъпността на Централизираната автоматизирана информационна система „Електронни обществени поръчки“.

Видовете дейности, включени в предмета на настоящото споразумение, както и условията за тяхното изпълнение са посочени в Техническата спецификация - Приложение 1, неразделна част от настоящото допълнително споразумение.

(2) ИЗПЪЛНИТЕЛЯТ се задължава да изпълни дейностите по чл. 1, ал. 1 от настоящото споразумение в пълно съответствие и при спазване на условията в Техническата спецификация – Приложение 1 към споразумението.

II. СРОК НА ДЕЙСТВИЕ

Чл. 2. Изпълнението на дейностите по чл. 1 от настоящото допълнително споразумение започва считано от 01.11.2019 г. и приключва с изтичане срока на Договора, включително предвидената гаранционна поддръжка, съгласно чл. 2, ал. 1 и ал. 2 и чл. 9, ал. 4 от Договора от 14.12.2017 г. между АОП и Консорциум „ЕОП България".

III. ПРЕДАВАНЕ И ПРИЕМАНЕ НА ИЗПЪЛНЕНИЕТО, СРОКОВЕ И НАЧИН НА ОТЧИТАНЕ

Чл. 3. (1) В срок до 10-то число на месеца, следващ отчетния календарен месец **ИЗПЪЛНИТЕЛЯТ** предоставя писмен доклад за отчитане на извършените през предходния месец дейности по чл.1, ал.1, който съдържа минимум:

a. Пълно описание на извършените дейности, вкл.:
   - Дата/период на извършване на дейността;
   - Засегната среда;
   - Засегнато устройство/функционален модул;
   - Тип събитие;
   - Причина за извършване на действията;
   - Описание на действията;
   - Помощен файл, съдържащ важна относима информация за действията (напр. история на използвани команди, архив на състояние на конфигурационен файл, архив на изходни кодове и др.);
   - Резултат от действията;
   - Лице/а, извършило/и действията.
b. Предложение за конкретни действия и мерки за постигане и поддържане на ниски нива на информационните рискове и срокове за тяхното изпълнение.

(2) В срок до 5 (пет) работни дни от представянето му, **ВЪЗЛОЖИТЕЛЯТ** преглежда доклада по ал.1 и при необходимост писмено изисква от **ИЗПЪЛНИТЕЛЯ** да го коригира и/или допълни в срок до 5 (пет) работни дни. Приемането на доклада по ал. 1 се удостоверява с подписването от страните на двустранен приемо-предавателен протокол.

(3) В срок до 5 (пет) работни дни от подписване на настоящото допълнително споразумение **ИЗПЪЛНИТЕЛЯТ** се задължава:

1. да смени паролите на всички администраторски акаунти, необходими за администриране на ЦАИС ЕОП и нейните хардуерни, комуникационни и софтуерни компоненти;

2. да създаде персонализирани акаунти за своите експерти, извършващи дейности по системно администриране на ЦАИС ЕОП;

3. да създаде персонализирани акаунти на служители на АОП, посочени от Възложителя, даващи възможност за четене на всички лог-файлове, както и на пълната информация, предоставяна от системата за наблюдение.

(4) Акаунтите на служителите на АОП по ал. 3, т. 3 трябва да бъдат настроени за задължително обновяване на паролата от самия потребител при първо влизане.

(5) ИЗПЪЛНИТЕЛЯТ се задължава да не допуска извършване на дейностите по чл. 1, ал. 1 от своите служители с акаунти, различни от създадените по ал. 3, т. 2.

(6) До 5 (пет) работни дни от направено писмено искане от страна на **ВЪЗЛОЖИТЕЛЯ**, **ИЗПЪЛНИТЕЛЯТ** е длъжен да предостави на **ВЪЗЛОЖИТЕЛЯ** пълен актуален списък на потребителите с администраторски права.

(7) Не по-рано от 10 (десет) и не по-късно от 5 (пет) работни дни преди прекратяване действието на Договора, **ИЗПЪЛНИТЕЛЯТ** е длъжен да предостави на **ВЪЗЛОЖИТЕЛЯ** пълен актуален списък на потребителите с администраторски права.

(8) Списъците по ал. 6 и 7 трябва да включват акаунти за операционните системи, за всякакъв специализиран и управляващ софтуер, за виртуализационни среди и виртуални устройства, за достъп до физически устройства, канали за връзка и др., т. е. всички акаунти, необходими за администрирането на ЦАИС ЕОП, страницата на АОП, комуникационните канали, системата за наблюдение на ЦАИС ЕОП, Call Center. За вградените администраторски акаунти се посочват техните пароли. Списъкът се предава в криптиран вид на лице/лица, определени от **ВЪЗЛОЖИТЕЛЯ**. Приемането се удостоверява с двустранен приемо-предавателен протокол.

IV. ЦЕНА И НАЧИН НА ПЛАЩАНЕ

Чл. 4. (1) Цената за изпълнение на дейностите по чл. 1 от настоящото споразумение е в размер на **59 000 (петдесет и девет хиляди) лв. без ДДС за месец**, и включва всички необходими разходи на **ИЗПЪЛНИТЕЛЯ** за дейностите от предмета на споразумението, съгласно Техническата спецификация – Приложение 1 към настоящото допълнително споразумение.

(2) Плащането на цената се извършва в срок до 30 (тридесет) календарни дни след подписване на приемо-предавателен протокол за доклада за отчитане на извършените дейности, съгласно чл. 3, ал. 1, и представяне на фактура.

(3) Общата стойност за изпълнение на дейностите по чл.1, ал.1 от настоящото споразумение е 1 534 000 (един милион петстотин тридесет и четири хиляди) лв. без ДДС и се определя на база уговорената цена за месец, посочена в ал.1, за период от 26 календарни месеца.

V. ГАРАНЦИЯ ЗА ИЗПЪЛНЕНИЕ

Чл. 5. (1) При подписване на настоящото допълнително споразумение **ИЗПЪЛНИТЕЛЯТ** представя гаранция за изпълнение в размер на 5 % (пет на сто) от общата стойност.

(2) Гаранцията по ал. 1 се освобождава в срок до 30 (тридесет) календарни дни след изтичане на срока по чл. 2, при условие, че изпълнението на дейностите по чл. 1 отговарят на всички изисквания съгласно Техническата спецификация – Приложение 1, неразделна част от настоящото допълнително споразумение.

(3) По отношение на условията за задържане или усвояване на гаранцията или част от нея се прилагат съответните клаузи от Договора от 14.12.2017 г. между АОП и Консорциум „ЕОП България".

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 6. (1) ВЪЗЛОЖИТЕЛЯТ може да прекрати едностранно действието на настоящото споразумение с едномесечно писмено предизвестие при достигане на стойностите, посочени в чл. 116, ал. 2 от ЗОП, включително и във връзка с други изменения на Договора от 14.12.2017 г. между АОП и Консорциум „ЕОП България".

(2) С подписването на настоящото допълнително споразумение същото става неразделна част от Договора между АОП и Консорциум „ЕОП България" от 14.12.2017 г. Всички останали клаузи от този договор остават непроменени и запазват действието си съответно и към допълнителното споразумение, ако са приложими.

(3) Възникнали спорове по приложението на допълнителното споразумение се уреждат между страните, а при непостигане на съгласие – съгласно уговореното в чл. 19 и чл. 20 от Договора между АОП и Консорциум „ЕОП България" от 14.12.2017 г.

(4) Страните се задължават да спазват относимите разпоредби на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (в приложимите случаи), като предприемат

всички необходими действия и мерки за защита на личните данни, до които имат достъп при изпълнение на настоящия Договор.

Настоящото допълнително споразумение към Договора между АОП и Консорциум „ЕОП България“ от 14.12.2017 г. съдържа 4 (четири) страници и се състави и подписа в три еднообразни екземпляра – два за **ВЪЗЛОЖИТЕЛЯ** и един за **ИЗПЪЛНИТЕЛЯ.**

Неразделна част от споразумението е Техническа спецификация - Приложение 1.

ЗА ВЪЗЛОЖИТЕЛЯ:

**Информацията е заличена на основание чл. 4, т. 1 от Регламент ЕС 2016/679*

МИХАИЛ МИХАИЛОВ
Главен секретар,
Възложител по чл. 7, ал. 1 от ЗОП
съгласно заповед № РД-48/24.06.2019 г.

**Информацията е заличена на основание чл. 4, т. 1 от Регламент ЕС 2016/679*

ДЕНИЗА СТАНКОВА
Главен счетоводител

ЗА ИЗПЪЛНИТЕЛЯ:

**Информацията е заличена на основание чл. 4, т. 1 от Регламент ЕС 2016/679*

ИВАЙЛО ФИЛИПОВ
Изпълнителен директор на
„Информационно обслужване“ АД
и представляващ
Консорциум „ЕОП България“

ПРИЛОЖЕНИЕ 1

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

Дейности по системно администриране на Централизирана автоматизирана информационна система „Електронни обществени поръчки“ (продукционна, резервна, тестова подсистеми и Call Center), непопадащи в обхвата на договора между Агенцията по обществени поръчки (АОП) и Консорциум „ЕОП България“ от 14.12.2017 г.

1 Въведение

Въвеждането в експлоатация на Централизираната автоматизирана информационна система „Електронни обществени поръчки“ (ЦАИС ЕОП) изисква полагане на грижи и усилия за осигуряване на непрекъснатост и висока наличност на ИКТ услугите, които осигуряват бизнес процесите, реализирани в ЦАИС ЕОП, както и постоянно проактивно наблюдение и администриране на инфраструктурата и комуникационната среда на ЦАИС ЕОП, за краткост наричани по-долу УСЛУГИТЕ. Високото качество на УСЛУГИТЕ може да бъде гарантирано, само ако за изпълнение на УСЛУГИТЕ се избере опитен и утвърден доставчик на ИКТ услуги, който притежава необходимите компетенции, знания, умения и капацитет, кореспондиращи с обхвата на УСЛУГИТЕ в ЦАИС ЕОП. В тази връзка в настоящото изложение е представено описание на УСЛУГИТЕ и системата, които е необходимо да бъдат предоставяни и администрирани.

В настоящата техническа спецификация са включени дейности от препоръчителния списък, посочен в официално становище на външна фирма, наета от АОП да дефинира техническите дейности, необходими за осигуряване на наличността, работоспособността и достъпността на ЦАИС ЕОП, които обаче не попадат в обхвата на договора между АОП и Консорциум „ЕОП България“ за разработването, внедряването и поддръжката на ЦАИС ЕОП.

За техническите дейности, описани по-долу, са използвани политики, процедури и указания на The European Union Agency for Cybersecurity (ENISA), The National Institute of Standards and Technology (NIST),SANS Institute и други източници.

2 Описание на ЦАИС ЕОП

ЦАИС ЕОП е подсигурена с основен и резервен център за данни. В резервния център за данни са реализирани резервна и тестова среди.

В режим 24x7 се администрират:

- Продукционна (експлоатационна) среда;
- Резервна среда;
- Тестова система, която регулярно се обновява с нови версии, предвид продължаващата разработка и усъвършенстване на системата;
- Call center (Център за обслужване на клиенти).

Съгласно Закона за защита на класифицираната информация, всеки член на екипа, предоставящ УСЛУГИТЕ, е задължително да разполага с разрешение за достъп до класифицирана информация ниво „СЕКРЕТНО“.

Компонентите, изграждащи ЦАИС ЕОП, включват:

№	Компонент	Брой	Тип/OS
1.	Сървър	9	HYPER-V
2.	Виртуални машини	49	MS Windows Server 2016 + Ubuntu 18.04 server + CentOS
3.	Виртуален Рутер	1	VyOS
4.	Сървър	1	VMware ESXi 6.5
5.	Виртуални машини	5	Ubuntu 18.04, MS Windows Server 2016, MikroTik RouterOS
6.	Масив за съхранение на данни	2	Lenovo
7.	Защитни стени	2	SonicWall
8.	Устройство за разпределение на натоварването (Load Balancer)	2	F5
9.	Комутатор	3	
10.	SAN комутатор	2	
11.	UPS	4	Lenovo
12.	Център за данни	2	
13.	Подсистема (среда)	3	

3 Дейности в обхвата на УСЛУГИТЕ

3.1 Администриране на сървърните системи

3.1.1 Непрекъснат (24x7) проактивен мониторинг от страна на Изпълнителя на наличността, работоспособността и достъпността на сървърните системи (включително виртуалните устройства) на ЦАИС ЕОП чрез система за наблюдение, осигурена и поддържана от Изпълнителя, външна за средите на ЦАИС ЕОП;

3.1.2 Системно администриране на сървърните системи в продукционната, резервната и тестовата подсистеми.

Системно администриране на Windows базирани системи и на Windows операционни системи, включващо:

a) Конфигуриране на основни и базови услуги;
b) Конфигуриране на планирани задачи (Scheduled tasks);
c) При необходимост, оказване на съдействие при инсталиране и конфигуриране на 3rd party софтуер;
d) Анализ и оценка за необходимостта от осъвременяване на версиите на софтуера.

Системно администриране на Linux операционни системи, включващо:

a) Конфигуриране на основни и базови услуги;
b) Конфигуриране на планирани задачи (Crontab jobs);
c) При необходимост, оказване на съдействие при инсталиране и конфигуриране на 3rd party софтуер;
d) Анализ и оценка за необходимостта от осъвременяване на версиите на софтуера.

Системно администриране на Hyper-V и VMware софтуер за виртуализация, включващо:
a) Обновяване на софтуера до актуална версия;
b) Анализ на необходимостта от прилагането на обновления и поправки, издадени от производителя на софтуера;
c) Проактивен мониторинг на разпределението на ресурсите на виртуализационните платформи;
d) Имплементиране на промени във виртуалните среди с цел използване на допълнителни инфраструктурни ресурси - дискови масиви, мрежова свързаност и други;
e) Администриране и конфигуриране на достъпа до виртуалните инфраструктури;
f) Конфигуриране на права за достъп до виртуалните машини.

Системно администриране на активна директория (MS Active Directory), включващо:
a) Управление на Active Directory услугата;
b) Управление на AD Site Topology;
c) Управление на домейни;
d) Управление на Operations Masters;
e) Управление на схемата Active Directory;
f) Управление на репликацията между Domain Controllers (DC).

Системно администриране на DNS услуга, включващо:
a) Управление на DNS сървъри;
b) Управление на DNS зони;
c) Управление на състоянието на DNS услугата;
d) Управление на репликацията между DNS сървърите.

Системно администриране на Windows Server Update Services (WSUS), включващо:
a) Управление на WSUS Servers;
b) Управление на състоянието на кръпки (patches) по сигурността чрез WSUS сървъри.

Системно администриране на архивите, включващо:
a) Управление на резервирането на данни по предварително изготвена архивна схема спрямо нуждите на сървърните приложения;
b) Управление на архивните задачи;
c) Създаване на нови архивни задачи чрез специализиран софтуер и/или средствата за архивиране, вградени в операционните системи;
d) Наблюдение на процесите на архивиране;
e) Наблюдение на състоянието на архивите на операционните системи;

f) Наблюдение на състоянието на архивите на основните приложения в ИКТ инфраструктурата;
g) Наблюдение на състоянието на архивите на 3rd party приложения в ИКТ инфраструктурата;
h) Управление на процеса по архивиране на информацията - следене за успешното протичане на архивирането на ЦАИС ЕОП;
i) Реализация на механизъм за архивиране в общото хранилище на държавната администрация и следене за правилното му функциониране;
j) Ежемесечно извършване на тестови възстановявания от архиви на оперционни системи с цел проверка на тяхното качество, консистентност и цялост;
k) Системно администриране на системите за съхранение на данни, включващо и локалните RAID масиви.

Системно администриране на SAN инфраструктурата, включващо:
a) Системно администриране на дисковите масиви за съхранение на данни;
b) Системно администриране на виртуализираното дисково пространство.

Системно администриране на кръпки (patches) в сигурността, включващо:
a) Тестване на кръпки по сигурността за различните видове приложения и операционни системи;
b) Инсталиране на одобрените кръпки за различните видове приложения и операционни системи;
c) Инсталиране на одобрените кръпки на версии на 3rd party приложения.

3.1.3 Допълнителни технически дейности по сървърните системи:
a) Гарантиране на еталонните параметри в продукционната, резервната и тестовата подсистеми;
b) При необходимост - мигриране на внедрените приложения и програмни продукти;
c) Системно администриране на сървърните системи, обслужващи Call Center;
d) Координиране на действията, необходими за разрешаване на проблеми, свързани със сървърните системи на ЦАИС ЕОП, с АОП и външни доставчици на услуги;
e) Анализ на рисковете и преценка за необходимостта от инсталиране на нови компоненти на базовия системен софтуер (patches, updates, Services Packs, нови версии на софтуер/firmware, изтичане на поддръжка и други);
f) Уведомяване на АОП чрез Issue Tracking System (ITS) или IT Service Management (ITSM) при нарушаване на наличността, работоспособността и достъпността на сървърните системи. В случай на събитие, за което експерт на Изпълнителя, обслужващ ITS или ITSM система, прецени, че е инцидент, моментът на уведомяване чрез системата се счита за начало на срока за реакция и отстраняване на проблема. Ако информация за събитието е постъпила и по реда на т. 3.4.13 от Техническата спецификация, приложение към основния договор, за начало на срока за реакция и отстраняване на проблема се счита най-ранното уведомяване.

3.2 Администриране на системите за управление на бази данни (СУБД)

3.2.1 Непрекъснат проактивен мониторинг на работоспособността на СУБД в продукционната, резервната и тестовата подсистеми чрез система за наблюдение, осигурена и поддържана от Изпълнителя, външна за средите на ЦАИС ЕОП;

3.2.2 Системно администриране на сървърите, обслужващи СУБД, на специализиран приложен софтуер на сървърите и на информационните масиви за съхранение на бази данни, включващо:

a) Ежедневен контрол на еталонните параметри и работоспособността на СУБД;
b) Системно администриране на роли в приложните сървъри, свързани с информационните масиви за съхранение на данни/бази данни;
c) Системно администриране на сървърни приложения, в частта им, взаимодействаща с информационните масиви за съхранение на данни/бази данни;
d) Наблюдение и осигуряване на нормалното функциониране на специализираните приложни системи;
e) Отчитане, коригиране и докладване за често повтарящи се грешки;
f) Проучване на възможните грешки и последствия за информационните масиви за съхранение на данни/базите данни при обновяване на версията и възможностите за оптимизация при преминаване към по-нова версия;
g) Проверки и профилактики на продукционната, резервната и тестовата системи: всекидневни, седмични и месечни, в съответствие с изработен график, съгласуван с АОП;
h) Архивиране и предоставяне на статистическите файлове;
i) Промени на системни настройки;
j) Управление и справки от информационните масиви за съхранение на данни/базите данни за потребителите;
k) Обновяване на информационните масиви за съхранение на данни/базите данни, като всички обновления се прилагат и тестват на предварително изградена тестова среда;
l) Ежемесечно извършване на тестови възстановявания от архиви на базите данни с цел проверка на тяхното качество, консистентност и цялост в присъствието на експерт/и от АОП;
m) Наблюдение на поведението на СУБД чрез логовете.

3.2.3 Допълнителни технически дейности по СУБД:
Уведомяване на АОП чрез Issue Tracking System (ITS) или IT Service Management (ITSM) система при нарушаване на наличността, работоспособността или достъпността на сървърите, обслужващи СУБД, на специализиран приложен софтуер на сървърите и на информационните масиви за съхранение на бази данни. В случай на събитие, за което експерт на Изпълнителя, обслужващ ITS или ITSM система, прецени, че е инцидент, моментът на уведомяване чрез системата се счита за начало на срока за реакция и отстраняване на проблема. Ако информация за събитието е постъпила и по реда на т. 3.4.13 от Техническата спецификация, приложение към основния договор, за начало на срока за реакция и отстраняване на проблема се счита най-ранното уведомяване.

3.3 Администриране на комуникационните системи (КС)

3.3.1 Непрекъснат проактивен мониторинг на работоспособността на комуникационните системи (включително виртуални) и комуникационните канали и връзки в продукционната, резервната и тестовите подсистеми чрез система, осигурена и поддържана от Изпълнителя, външна за средите на ЦАИС ЕОП;

3.3.2 Системно администриране на комуникационните системи и преносната среда (LAN, MAN и WAN, специализирани устройства за разпределяне на мрежовия трафик, Firewalls, интернет свързаност, комуникационни канали от и към Единната електронна съобщителна мрежа (ЕЕСМ) на държавната администрация), включващо:

a) Промени в конфигурацията и настройките на комуникационните канали/връзки и КС, когато се налага, и поддържане на актуален списък с история на конфигурациите;
b) Архивиране на конфигурациите на активното мрежово оборудване;
c) Поддържане на база от данни за текущите и миналите конфигурации на активното оборудване;
d) Измерване и анализ на параметрите на трафика и изготвяне на предложения за оптимизации;
e) Управление на връзките за интернет свързаност на ЦАИС ЕОП;
f) Управление на връзките между центровете за обработка на данни на ЦАИС ЕОП;
g) Управление на LAN на ЦАИС ЕОП;
h) Следене на логовете (logs) на комуникационните системи и канали;
i) Актуализиране на КС в продукционната, резервната и тестовите подсистеми.

3.3.3 Допълнителни технически дейности по КС:

a) Координиране на действията, необходими за разрешаване на проблеми и инциденти, с АОП и външни доставчици на услуги;
b) Уведомяване на АОП чрез Issue Tracking System (ITS) или IT Service Management (ITSM) система при нарушаване на наличността, работоспособността или достъпността на КС и комуникационните канали и връзки. В случай на събитие, за което експерт на Изпълнителя, обслужващ ITS или ITSM система, прецени, че е инцидент, моментът на уведомяване чрез системата се счита за начало на срока за реакция и отстраняване на проблема. Ако информация за събитието е постъпила и по реда на т. 3.4.13 от Техническата спецификация, приложение към основния договор, за начало на срока за реакция и отстраняване на проблема се счита най-ранното уведомяване.

3.4 Управление на логовете (Logs)

3.4.1 Управление на системни логове - оценка след съгласуване с АОП кои имат стойност в дългосрочен план и според законови изисквания не трябва да бъдат изтривани;

3.4.2 Периодично архивиране/изтриване на неполезни логове след съгласуване с АОП;

3.4.3 Анализ, включително корелативен, на одитните събития, записани в логовете, с цел идентифициране на проблеми и зависимости и установяване на тенденции;

3.4.4 Наблюдение за грешки и предупреждения в Event Logs на Windows базирани сървъри;

3.4.5 Наблюдение за предупреждения и грешки в системни логове (syslog, messages, deamon и други) за Linux базирани сървъри;

3.4.6 Наблюдение на състоянието на Scheduled tasks;

3.4.7 Наблюдение на състоянието на Crontab jobs;

3.4.8 Наблюдение на логовете на комуникационната среда.

3.5 Наблюдение на състоянието на предоставения хардуер

3.5.1 Наблюдение на състоянието на предоставения по договор с Консорциум „ЕОП България“ хардуер чрез специализиран централизиран софтуер;

3.5.2 Наблюдение на състоянието на хардуера чрез специализиран софтуер, предоставен от производителя на хардуера;

3.5.3 При откриване на дефект Изпълнителят да уведоми АОП и Консорциум „ЕОП България“, който по договор с АОП носи отговорност за гаранционната поддръжка на ЦАИС ЕОП.

3.6 Информационна сигурност

3.6.1 Общо изискване: Всички дейности по системното администриране на ЦАИС ЕОП и другите допълнителни технически дейности трябва да поддържат ниски нива на информационни рискове и да се гарантира конфиденциалността, интергритета и достъпността на трансферираната, обработваната и съхраняваната информация в ЦАИС ЕОП, включително Call Center.

3.6.2 Сканирания за техническите уязвимости и прилагане на мерки за отстраняване на откритите слабости:

Изпълнителят е длъжен да сканира ежемесечно за технически уязвимости всички работещи в ЦАИС ЕОП информационни системи - мрежови, сървърни и интернет сайтовете. Тестовете за технически уязвимости трябва да бъдат извършвани чрез автоматизирани инструменти (ползващи база данни от Network Vulnerability Tests (NVTs)) и чрез прилагане на експертни неавтоматизирани методи - ръчни проверки. Процесът на тестване трябва да обхваща публично достъпните и локалните информационни ресурси на ЦАИС ЕОП и проверка за наличие на Common Vulnerabilities and Exposures (CVE), регистрирани в глобалните бази данни. Необходимо е всяко открито несъответствие да се анализира и оценява чрез Common Vulnerability Scoring System (CVSS), която дава информация за характеристиките на уязвимостите и формира оценки на критичността им.

3.6.3 Изпълнителят трябва да анализира всички системи за зловреден софтуер и да преконфигурира, надстройва, преинсталира или деинсталира приложения и/или операционни системи. Ежемесечно трябва да се извършват следните дейности:

a) Сканиране за технически уязвимости и прилагане на мерки за отстраняване на откритите несъответствия за всички публично достъпни ИКТ услуги на ЦАИС ЕОП, включително интернет сайтовете;
b) Сканиране за технически уязвимости и прилагане на мерки за отстраняване на откритите несъответствия за всички ИКТ ресурси в локалните мрежи на ЦАИС ЕОП;
c) Преглед на сървърните системи за наличие на зловреден софтуер;
d) Анализиране за компютърни вируси;
e) Анализиране за известни RootKits – механизми и техники, чрез които зловредни програми, включително компютърни вируси, шпионски програми и троянски коне, се опитват да се скрият от антивирусни програми и други приложения за сигурност;
f) Анализиране за участие на сървърните системи в botnets;
g) Анализиране за инсталиран софтуер без знанието на системните администратори, който събира лична информация (spyware), в това число софтуер за събиране на пароли (keylogger);
h) Анализиране за софтуер, който управлява рекламни съобщения (adware);
i) Анализиране на интернет сайтовете на АОП за риск от успешни DDoS атаки.

3.6.4 Изпълнителят трябва да предоставя на АОП ежемесечно Risk Assessment Report (RAR) за откритите уязвимости при извършените от него сканирания според Common Vulnerability Scoring System (CVSS) и отчет за отстраняването им.

3.7 Други технически дейности в обхвата на УСЛУГИТЕ

3.7.1 Уведомяване чрез Issue Tracking System (ITS) или IT Service Management (ITSM) система на всички заинтересовани страни при нарушаване на наличността, работоспособността или достъпността на ЦАИС ЕОП. В случай на събитие в ЦАИС ЕОП, за което експерт на Изпълнителя, обслужващ ITS или ITSM система, прецени, че е инцидент, моментът на уведомяване чрез системата се счита за начало на срока за реакция и отстраняване на проблема. Ако информация за събитието е постъпила и по реда на т. 3.4.13 от Техническата спецификация, приложение към основния договор, за начало на срока за реакция и отстраняване на проблема се счита най-ранното уведомяване. Осигуряването на ITS или ITSM система, външна за средите на ЦАИС ЕОП, е ангажимент на Изпълнителя на системното администриране;

3.7.2 Управление на потребителите – управление на вградените акаунти, управление на акаунтите за служители, имащи отношение към системното администриране - създаване на нови, промяна/изтриване на съществуващи, обновяване на пароли (в съответствие с политиката за сигурност, при необходимост, при искане от страна на Възложителя), инвентаризация на акаунтите;

3.7.3 Съдействие при одити и проверки, извършвани от външни организации;

3.7.4 Мигриране на подсистеми на ЦАИС ЕОП в нови локации при необходимост;

3.7.5 Дейности по включване на ЦАИС ЕОП в Държавния хибриден частен облак (ДХЧО) при необходимост;

3.7.6 Преди извършване на инсталация да се правят резервни копия на софтуера, файловете и базите данни и да се разработи roll back план в случай на неуспешна инсталация;

3.7.7 Предприемане на мерки за отстраняване на открити несъответствия и уязвимости за всички публично достъпни услуги и за всички ИКТ ресурси в локалните мрежи на ЦАИС ЕОП в резултат на одити, проверки и тестове, извършени от трета страна (независима от АОП и Изпълнителя);

3.7.8 Системно администриране, включващо минимум обновяване на версиите на софтуера WordPress, използван за изграждане страницата на АОП, и администриране на web сървър MS IIS и страницата/подстраниците на АОП.

3.8 Политики и процедури, необходими за осигуряване на наличността, достъпността, работоспособността и сигурността на ЦАИС ЕОП

Изпълнителят трябва да прилага минимум следните политики и процедури:

a) Information Security Policy;
b) Change Management Policy, включваща създаване и поддържане на актуална техническа документация, която да бъде предоставена на АОП при поискване;
c) Incident Response Policy;
d) Матрица на отговорностите.

4 Начин на отчитане на изпълнението на УСЛУГИТЕ

4.1 Отчитането на изпълнението се извършва с писмен доклад за извършените дейности.

4.2 По изключение (напр. при срив, непланирани спирания на ЦАИС ЕОП или други извънредни ситуации) и след писмено искане, вкл. чрез електронна поща, от страна на Възложителя, Изпълнителят следва в срок до 2 (два) работни дни след искането да предостави извънреден писмен доклад за състоянието на ЦАИС ЕОП, включващ изрично поискана информация.

4.3 Докладите се предоставят в електронен вид, позволяващ пълнотекстово търсене и копиране на части от съдържанието му, като съставящите ги файлове трябва да бъдат цифрово подписани от съответни упълномощени лица.

4.4 В срок от 30 (тридесет) календарни дни от подписване на споразумението за системно администриране Изпълнителят трябва да предостави на АОП минимум политиките и процедурите по т. 3.8, които прилага. Матрицата на отговорностите следва да бъде предоставяна на Възложителя и при промени при служителите на Изпълнителя, заети със системното администриране на ЦАИС ЕОП.

5 Заключителни разпоредби

5.1 Настоящата Техническа Спесификация съдържа 10 (десет) страници и се явява неразделна част от Допълнително Споразумение № 01 към Договор за обществена поръчка с предмет „Разработване, внедряване и поддръжка на единна национална електронна уеб-базирана платформа: Централизирана автоматизирана информационна система „Електронни обществени поръчки“ (ЦАИС ЕОП)“ от 14.12.2017 г.