РАЗДЕЛ IX. ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

1. ПРЕДНАЗНАЧЕНИЕ

Настоящият документ съдържа подробна техническата спецификация на хардуер. софтуер и дейностите, предвидени за реализиране на обществена поръчка по ЗОП за изграждане надеждна система за киберзащита за Информационната система за управление и наблюдение на средствата от ЕС за програмен период 2014 г. - 2020 г. (ИСУН2020).

2. ПРЕДМЕТ

Предметът на обществената поръчка по ЗОП е **„Осигуряване на система за киберзащита на ИСУН2020“** и има за цел да достави, инсталира и конфигурира хардуер с прилежащия му софтуер към наличните ресурси от информационно-комуникационната среда в центровете за данни за електронно управление.

3. ОБХВАТ

За постигне на заложените цели в настоящата обществена поръчка е необходимо да бъдат извършени следните основни дейности:

3.1. Доставка на хардуерно оборудване, съответния специализиран софтуер и софтуерни лицензи необходими за ползване на предвидените функционалности.

3.2. Инсталиране и конфигуриране на доставеното хардуерно оборудване, съобразно наличното оборудване и дизайна.

3.3. Изграждане на пълно функционално и надеждно решение за киберзащита за Информационната система за управление и наблюдение на средствата от ЕС (ИСУН2020).

4. МЯСТО

Изпълнението на дейностите по тази поръчка трябва да бъдат изпълнени в **Контролно-техническия център на електронното правителство (КТЦЕП)**.

5. ТЕКУЩО СЪСТОЯНИЕ

Информационната система за управление и наблюдение на средствата от ЕС (ИСУН2020) е основен инструмент за работа и ключов компонент в работните процеси на всички управляващи органи на оперативните програми и бенефициенти ползващи финансови средства от ЕСИФ. Поради тази причина ИСУН2020 се определя като критична от бизнес гледна точка за кандидатстване, отчитане и управление на европейските фондове в Р. България. Тя е основен инструмент, чрез който се осъществява обмен на информация и отчитане на финансовите средства със съответните електронни системи на Европейската комисия.

ИСУН2020 се използва от 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. Електронната система

предоставя възможност за свободен достъп на широката общественост, предоставяйки и обобщена информация за напредъка и усвояването на средствата от ЕС на публичния интернет адрес: http://2020.eufunds.bg/.

В съответствие с изпълняваната в момента държавна политика в Република България е изграден Държавен хибриден частен облак (ДХЧО), осигуряващ споделени информационни ресурси за електроните услуги на държавната администрация. Това е една от задачите в изпълнение на целите на Програмата на правителството за стабилно развитие на Република България за периода 2014 – 2020 г. Изграждането на Държавен хибриден частен облак, който предоставя „инфраструктура като услуга" (IaaS), осигурявайки изчислителен ресурс под формата на виртуални сървъри, системи за съхранение на данни и комуникационна среда, позволява значително да се оптимизира ИТ инфраструктурата, подобрява се нейната поддръжка и се улеснява значително нейното обновяване и мащабиране. По този начин се реализират икономии на финансови средства и се подобрява качеството на предоставяните услуги от страна на държавната администрация.

Следвайки политиката за електронно управление и принципите, залегнали в Програмата на правителството, Информационната система за управление и наблюдение на средствата от ЕС беше мигрирана и понастоящем предоставя своите услуги от ДХЧО, като за тази цел е изградено реално сътрудничество с отговорните държавни структури (Държавната агенция електронно управление - ДАЕУ).

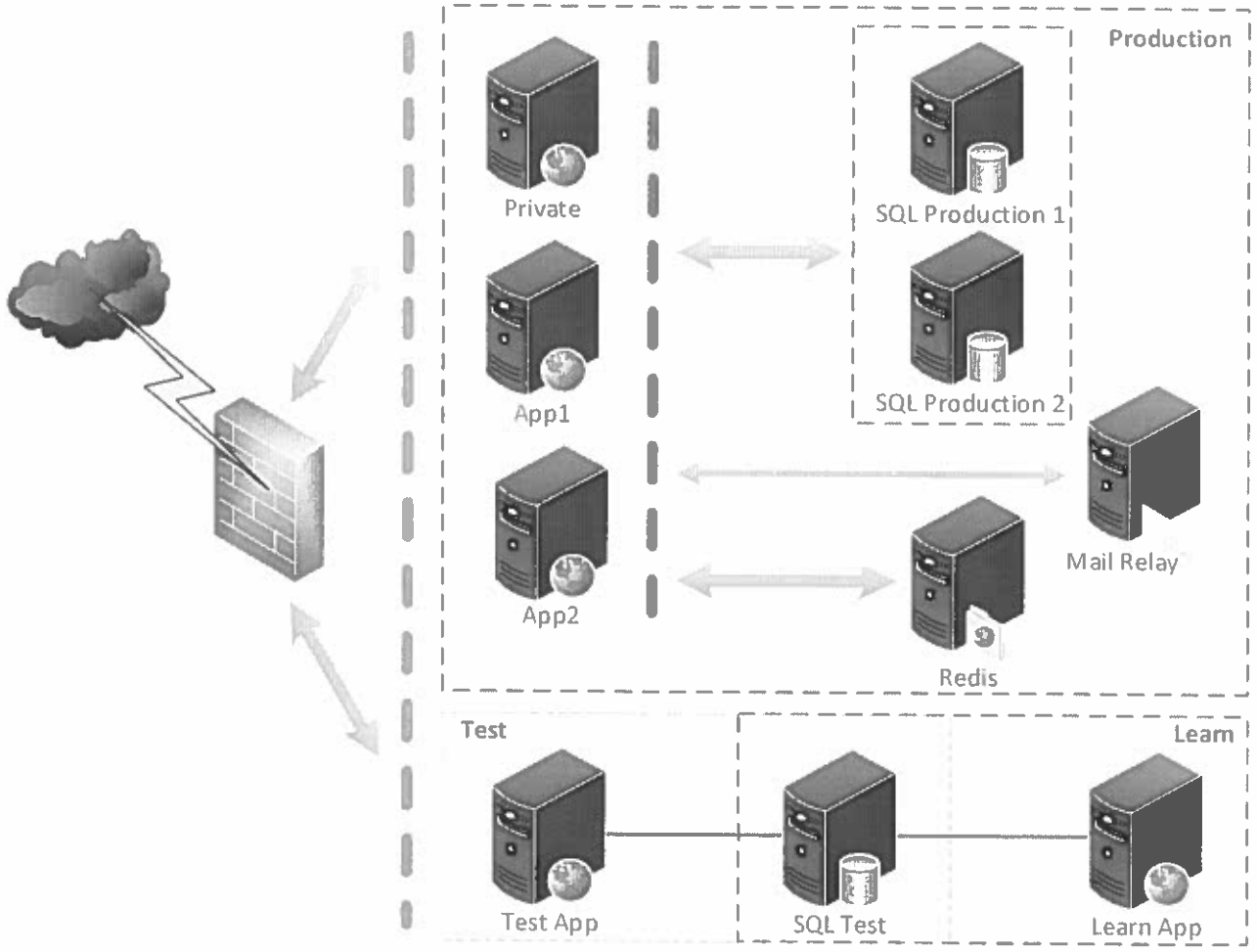
Текущото състояние на основния продуктивен сайт (ДХЧО), ИСУН2020 използва следните хардуерни и софтуерни инфраструктурни ресурси:

- мрежова инфраструктура, базирана на продукти и технологии на Сиско Системс - високо-скоростна среда на предаване на данни, включително 8Gb/s, 10Gb/s и 40Gb/s мрежова свързаност с най-съвременни мрежови протоколи, единна SDN (Software Defined Networking) архитектура.
- високоналична сървърна инфраструктура изградена от висок клас сървърен хардуер.
- среда за виртуализация, реализирана на базата на Microsoft Hyper-V.
- среда за съхранение на данни, която осигурява необходимия дисков капацитет. Съобразявайки се с регламентите на ЕК, ИСУН2020 е реализирал функционалности, за които ще бъдат необходими 64 TiB данни през новия програмен период 2014 – 2020 г.
- подсистеми за архивиране, осигуряващи бързодействието и капацитета за архивиране на горецитирания обем от данни и използващи софтуер HPE Data Protector.
- Софтуер за управление и наблюдение на компютърните мрежи, сървъри и софтуерни приложения (Service Manager).
- Системи за управление и наблюдение на информация свързана със сигурността и управление на събитията (Security information and event management - SIEM).

На приложно ниво ИСУН2020 е WEB-базирана информационна система, съхраняваща данните в структуриран вид. Системата е изградена на база на технологиите MS dotNET, MS SQL, MS IIS.

Текущият дизайн на ИСУН2020 (**Фигура 1**) е наложен от изискванията за високо налично решение и отчита добрите практики по отношение на разработване, внедряване и обслужване на ИСУН2020 като включва следните софтуерни среди:

- Продуктивна (работна) среда;
- Тестова среда и среда за обучение.



Фигура 1

ИСУН2020 е изградена изцяло върху виртуални машини с операционни системи Microsoft Windows Server, както следва:

Продуктивна Среда

- **Приложни сървъри** – 3 броя WEB сървъри: App1, App2 и Private, ОС Microsoft Windows 2012 R2 Server, MS Internet Information Server (IIS). Разположени са в логическа DMZ с възможност от публичен достъп.
- **Сървъри за бази данни** – 2 броя DB сървъри, ОС Microsoft Windows 2016 Server, MS SQL Server 2016 Enterprise Edition
- **Cache/Session** – 1 брой Redis, ОС Linux server

Тестова среда и среда за обучение

- **Приложен сървър** – WEB сървър за тестова среда, ОС Microsoft Windows 2012 R2 Server, базирани на MS Internet Information Server (IIS)

- **Приложен сървър** – WEB сървър за обучителна среда, ОС Microsoft Windows 2012 R2 Server, базирани на MS Internet Information Server (IIS)
- **Сървър за бази данни** – DB сървър за тестова и обучителна среда, ОС Microsoft Windows 2016 Server, MS SQL Server 2016 Enterprise Edition
- **Mail Relay** – сървър за изпращане на e-Mail съобщения до ползвателите на системата.

Системата разполага и със съответно Център за възстановяване след бедствие (Disaster Recovery Center - DRC).

6. ТЕХНИЧЕСКИ ИЗИСКВАНИЯ

С цел да се гарантира нормалното и непрекъсваемо функциониране на ИСУН2020 в съответствие с приетите правила за информационна сигурност и подсигуряване работата на бенефициентите и потребителите от всички административни структури, участващи в процеса на управление, наблюдение и контрол на средствата от ЕСИФ, е необходимо да се осигури модерна система за киберзащита предпазваща от многообразните съвременни online атаки. Едновременно с това, следвайки добрите практики, където една информационна система по дизайн е разгърната в основен (primary) и резервен (DRC) дейта центрове, е необходимо създаване на техническа възможност за балансиране на натоварването между центровете и автоматично превключване при отпадане на единия от тях. Системата за киберзащита и за балансиране на натоварването трябва да разполага с поне два клъстера от физически устройства за основен и резервен дейта център, като всеки клъстер трябва да се състои от поне две устройства.

Предложеното решение трябва да отговаря на политиката за мрежова и информационна сигурност с оглед защита на ИСУН2020 срещу неправомерен достъп, който може да наруши достъпността, автентичността, целостта и конфиденциалността на съхраняваните, обработваните или предаваните данни.

Техническото решение трябва да притежава като минимум Web Application Firewall и Layer 7 Attack Protections, да открива и предотвратява L7 DoS, DoS/DDoS, Brute force, OWASP top 10 attacks, да може да открива и защитава Heavy URLs, да има възможност да открива и ограничава достъпа до приложението на Ботове и инструменти за атака. Система за защита трябва надеждно да осигури защита на публичните WEB приложения от злонамерени атаки, които имат за цел да открият и да се възползват от уязвимости и пропуски в конфигурацията на отделните WEB приложения.

Освен това възможностите за балансиране на натоварването трябва да осигурят SSL хардуерно разтоварване, TCP оптимизация, DNS услуги свързани с глобалното балансиране между двата центъра (основен и резервен) за данни и stickiness. Компонентите от един и същ географски разпределен дейта център трябва да споделят общ (виртуален) мрежови адрес, отговарящ на съответната услуга в центъра за данни. Активните заявки (сесии) за всеки един от сървърните ресурси, обслужвани от системата за защита и балансиране, трябва да се наблюдава, а статистиките да се синхронизират между отделните компоненти, с цел централизирано наблюдение на натоварването и разпределение на новите заявки към компонентите с по-ниско натоварване.

Предложеното решение следва да се състои минимум от следните компоненти:

1.	**Надграждане на устройство за балансиране на натоварването – 2 бр.**
1.1.	Да се надградят функционално съществуващите две устройства (**модел: F5-BIG-LTM-I5600 BIG-IP i5600 Local Traffic Manager**) устройства в основния и резервен дейта център.

1.2.	Осигуряване на виртуализация на инсталираните и надградени модули и функционалности.
1.3.	Надграждането да включва лиценз за осигуряване на хардуерна компресия за минимум 18 Gbps
1.4.	Надграждане на Network Firewall със следните функции: ▪ ICSA Certified Network L3-L4 Firewall ▪ Support for ACL ▪ Over 100 DoS vectors & Hardware-based DoS protections ▪ Dynamic IP intelligence & Blacklisting ▪ Remote Trigger Black Hole Filtering ▪ SSH Proxy policy protectionPort misuse detection and mitigation
1.5.	Надграждане на DNS firewall със следните функции: ▪ DNS Protocol inspection and validation ▪ DNS record type ACL ▪ DNS load balancing ▪ Complete DNSSEC signing ▪ Centralized DNSSEC key management ▪ Top-level domain support for DNSSEC ▪ DNSSEC validation ▪ DNS DDoS Mitigation
1.6.	Надграждане на Web Application Firewall със следните функции: ▪ XML Firewall ▪ Application DDoS protection ▪ OWASP Top 10 prevention ▪ Web scraping prevention ▪ Automated attack defense and bot detection ▪ Geolocation blocking
1.7.	Стандартна гаранционна поддръжка за срок не по-малък от 36 месеца, която да позволява софтуерни обновления до по-нова версия, обслужване „на място“. Да се включат всички необходими лицензи и софтуерни обновявания на сигнатурите за всички функционалности за срок не по-малък от 36 месеца.
2.	**Устройство за балансиране на натоварването – 2 бр.**
2.1.	Устройството да може да се клъстеризира по двойки с наличните **(модел: F5-BIG-LTM-I5600 BIG-IP i5600 Local Traffic Manager)** в основния и/или резервен дейта център, за осигуряване на висока степен на балансиране и резервираност.
2.2.	Устройството следва да осигури балансиране на Клиенти, достъпващи услуги чрез Интернет
2.3.	Броят на Клиентите, достъпващи услуги чрез Интернет, да е неограничен.
2.4.	Устройството следва да осигури балансиране на служителите, достъпващи различни бизнес апликации чрез нейната локална мрежа.
2.5.	Устройството трябва да може да извлича информация за сървърите към услугата, която балансира (ping, достъп до порт, съдържание), за да разпределя само до наличните.
2.6.	Трябва да е възможно изваждането на сървъра от балансирането без прекъсване на услугата.
2.7.	Устройството да поддържа виртуализация на инсталираните модули.
2.8.	Да са налични различни начини на балансиране като: ▪ Round Robin ▪ Least Connections ▪ Weighted Least Connections ▪ Maximum Connections

	▪ Response Time ▪ Observed (Least Conn + Fastest Resp) ▪ Predictive (Observed over time) ▪ Dynamic Ratio (Based on server utilization)
2.9.	Да разполага с минимум 12 физически слота, 4 от които да поддържат скорост от 40 Gb. Да се доставят 2бр. 10GBASE-SR SFP+ модула.
2.10.	Горните физически интерфейси трябва да позволяват формиране на port channel.
2.11.	Устройството да може да работи в режим на работа Active/Active;
2.12.	Устройството трябва да има възможност за L3 и L2 балансиране на различните приложения.
2.13.	Трябва да могат да се балансират SSL/TLS конекции.
2.14.	Администрация и управление ▪ Интерфейсът на операционната система на устройството следва да бъде интуитивен. ▪ Администрацията на операционната система на устройството следва да допуска дефиниране на различни роли за различните типове потребители.
2.15.	Устройството следва да предоставя възможност за генериране на рапорти и мониторинг в следните направления: ▪ Да рапортува за наличност на услугите и участващите в тях сървъри/апликации. ▪ Да рапортува за натовареността на различните услугите и сървъри/апликации в тях. ▪ Да рапортува относно консумирания трафик. ▪ Устройството следва да предоставя опции за дефиниране на dashboard за администратор с цел бързо извеждане на актуалните рапорти и мониторинг.
2.16.	Минимални изисквания към устройство от система за балансиране: ▪ Производителност – минимум 35 Gbps L4/L7. ▪ L4 HTTP заявки за секунда - минимум 10M. ▪ L4 конкурентни връзки – минимум 40M. ▪ Хардуерен Offload SSL/TLS – минимум 18 Gbps. ▪ Памет – минимум 48 GB ▪ Хардуерна компресия – минимум 18 Gbps ▪ Резервирани захранвания 100-240 VAC – максимална консумирана мощност 680W за всяко от тях.
2.17.	Устройството да работи като Network Firewall със следните функции: ▪ ICSA Certified Network L3-L4 Firewall ▪ Support for ACL ▪ Over 100 DoS vectors & Hardware-based DoS protections ▪ Dynamic IP intelligence & Blacklisting ▪ Remote Trigger Black Hole Filtering ▪ SSH Proxy policy protectionPort misuse detection and mitigation
2.18.	Задължително да отговаря на следните стандарти ETSI EN 300 328, EN 55032, EN 61000, EN 55024
2.19.	Устройството да работи като Web Application Firewall със следните функции: ▪ XML Firewall ▪ Application DDoS protection ▪ OWASP Top 10 prevention ▪ Web scraping prevention ▪ Automated attack defense and bot detection ▪ Geolocation blocking
2.20.	Устройството да работи като DNS firewall със следните функции:

	▪ DNS Protocol inspection and validation ▪ DNS record type ACL ▪ DNS load balancing ▪ Complete DNSSEC signing ▪ Centralized DNSSEC key management ▪ Top-level domain support for DNSSEC ▪ DNSSEC validation ▪ DNS DDoS Mitigation
2.21.	Стандартна гаранционна поддръжка за срок не по-малък от 36 месеца, която да позволява софтуерни обновления до по-нова версия, обслужване „на място". Да се включат всички необходими лицензи и софтуерни обновявания на сигнатурите за всички функционалности за срок не по-малък от 36 месеца.

ВАЖНО: За всеки конкретно посочен в настоящите технически спецификации стандарт, спецификация, техническа оценка, техническо одобрение или технически еталон, възложителят приема и еквивалентно/и такива. За всеки конкретно посочен в настоящите технически спецификации модел, източник или специфичен процес, който характеризира продуктите, предлагани от конкретен потенциален изпълнител, търговска марка, патент, тип или конкретен произход или производство, възложителят приема и еквивалентни такива.

7. ИЗИСКВАНИЯ КЪМ ОБОРУДВАНЕТО:

7.1. Предлаганото оборудване следва да съблюдава точно характеристиките и параметрите на артикулите, посочени в технически спецификации.

7.2. Предлаганото оборудване трябва да е ново, оригинално, неупотребявано, в оригинална окомплектовка и опаковка, предвидена от производителя, придружени с инструкции за употреба и гаранционни карти и да е в срок на актуална гаранционна сервизна поддръжка.

7.3. Предлаганата техника трябва да бъде комплектувана с всички необходими силови, интерфейсни и други кабели, адаптери и аксесоари, необходими за нормалната й работа. Захранването и кабелните накрайници на силовите кабели да са предвидени за експлоатация в Република България;

7.4. Предлаганата техника трябва да бъде напълно комплектувана така, че да бъде работоспособна и да изпълнява предвидените функциите. Ако се окаже, че дадено устройство не може да изпълнява дадена функция, то устройството следва да се приведе в състояние, при което може да изпълнява функциите, заложени в спецификацията или да бъде заменено с друго за сметка на изпълнителя.

7.5. При изпълнение на доставката, в случай, че оферираните стоки вече не се произвеждат, следва да бъдат доставени стоки с еквивалентни или по-добри технически характеристики без промяна в единичната цена и след предварително одобрение от възложителя.

7.6. Софтуерът следва да бъде последна възможна версия (най-актуална към момента на подаване на тръжните предложения, която фигурира в актуалната продуктова листа на съответния производител) и съвместима с текущите конфигурации, работещи към момента.

8. ИЗИСКВАНИЯ КЪМ РЕАЛИЗАЦИЯТА

8.1. Изпълнителят трябва да предложи дизайн на предложеното решение.

8.2. Изпълнителят трябва да изготви функционални тестове, чрез които ще се верифицира правилното функциониране на изградената система за киберзащита и балансиране на натоварването.

8.3. Всички извършвани дейности трябва да са съобразени с изискванията поставени от стандарта за информационна сигурност ISO 27000 и политиката, и процедурите за информационна сигурност, използвани при работа с ИСУН 2020.

8.4. Срок за изпълнение на дейностите – до 2 (два) месеца от датата на подписване на договора.

9. ГАРАНЦИОННА ПОДДРЪЖКА

9.1. Дейностите по хардуерната поддръжка трябва да се извършват на място.

9.2. Подмяна на дефектиралите хардуерни компоненти, трябва да се извършва с оригинални (от производителя на хардуерното оборудване) и нови компоненти или еквивалентни на новите по отношение на производителността, но напълно съвместими с оборудването на системата ИСУН.

9.3. При необходимост за отстраняване на конкретен проблем се допуска инсталирането на ъпдейти на firmware или на специализирания системен софтуер, които според производителя на оборудването са необходими за връщането на системата към нормална работа или за да направят възможна поддръжката на подменото оборудване.

9.4. Изпълнителят, осигуряващ сервизиране на доставената техника, следва да извършва преконфигуриране и настройки на системно ниво при поискване. Под системно ниво се разбира настройки и/или преконфигуриране на firmware на отделни компоненти или настройки, и/или преконфигуриране на интегрираните операционни системи в мрежовите устройства.

9.5. Всички дейности по сервизиране и/или конфигуриране следва да се извършват след одобрението на Възложителя. Когато се налага частично или цялостно спиране на системата ИСУН, е необходимо дейностите да бъдат планирани така, че да бъде минимализирано или напълно избегнато планираното прекъсване на услугата (downtime).

9.6. Всички подменени технически компоненти трябва да фигурират в актуалната сервизна или ценова листа на съответния производител.

9.7. В рамките на осигурената от ИЗПЪЛНИТЕЛЯ поддръжка, трябва да се гарантират следните времена за реакция и отстраняване на възникнал проблем:

- 9.7.1. Ниво на покритие - 24 x 7;
- 9.7.2. Време за реакция (време за приемане на заявката за възникнал проблем) – до 4 часа;
- 9.7.3. Време за отстраняване на възникнал проблем: до 3 (три) работни дни.

9.8. Дейностите по гаранционна поддръжка включват коригиращо поддържане на нормалната работоспособност на инсталирания системен софтуер при поискване.

9.9. При необходимост ИЗПЪЛНИТЕЛЯТ извършва възстановяване на системата при пълна или частична неработоспособност в следствие на инцидент.

9.10. При необходимост ИЗПЪЛНИТЕЛЯТ асистира и/или управлява промените на ниво хардуер и ниво системен софтуер.

9.11. При необходимост ИЗПЪЛНИТЕЛЯТ асистира при внедряване на промени в приложния софтуер, когато тези промени изискват промяна или допълнителни настройки в системния софтуер или устройствата на мрежово ниво.

9.12. Дейностите по гаранционна поддръжка включват и анализ на подадените от ВЪЗЛОЖИТЕЛЯ данни от логове и инциденти свързани с функционирането на системите и производителността им при поискване.

9.13. Срок на гаранционната поддръжка – минимум 36 месеца.

РАЗДЕЛ X. КРИТЕРИЙ ЗА ВЪЗЛАГАНЕ „ИКОНОМИЧЕСКИ НАЙ-ИЗГОДНА ОФЕРТА“ „НАЙ-НИСКА ПРЕДЛАГАНА ЦЕНА”

Предложената от участника цена, трябва да включва всички разходи за изпълнение на настоящата поръчка, в т.ч. транспортни разходи до мястото посочено за доставка, инсталиране и конфигуриране на решението, гаранционна поддръжка и други.

ЕВРОПЕЙСКИ СЪЮЗ

ЕДНА ПОСОКА
МНОГО ВЪЗМОЖНОСТИ

Приложение № 2

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

ПРЕДЛОЖЕНИЕ ЗА ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА
в процедура за възлагане на обществена поръчка с предмет:
„Осигуряване на система за киберзащита на ИСУН2020“
по Проект BG05SFOP001-4.002-0003-C01 „Повишаване на ефективността и ефикасността на Централното координационно звено“, Дейност 1: „Осигуряване на функционирането на информационните системи“, финансиран по Оперативна програма „Добро управление“

от „Комсофт“ ООД, с ЕИК: 030435072 в съответната държава Република България, със седалище Република България, гр. София 1202, район „Възраждане“, бул. „Княгиня Мария Луиза“ № 47 и адрес на управление Република България, гр. София 1202, район „Възраждане“, бул. „Княгиня Мария Луиза“ № 47, адрес за кореспонденция: Република България, гр. София 1202, район „Възраждане“, бул. „Княгиня Мария Луиза“ № 47, телефон за контакт +359 2 981 4566, факс +359 2 987 1723, електронна поща sales@comsoft.bg, представлявано от Христо Анчев Великов в качеството на управител

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 система за киберзащита на ИСУН2020“ по Проект BG05SFOP001-4.002-0003-C01 „Повишаване на ефективността и ефикасността на Централното координационно звено“, Дейност 1: „Осигуряване на функционирането на информационните системи“, финансиран по Оперативна програма „Добро управление“. Заявяваме, че желаем да участваме в процедурата и предлагаме да осъществим предмета ѝ в пълно съответствие с Техническите спецификации и изискванията на Възложителя от документацията за обществената поръчка.

Предложеното решение се състои минимум от следните компоненти:

1.	Надграждане на устройство за балансиране на натоварването – 2 бр.	Параметри на предлаганата техника Надграждане на устройство за балансиране на натоварването – 2 бр.	Производител, модел или друг отличителен знак
1.1.	Да се надградят функционално съществуващите две устройства **(модел: F5-BIG-LTM-I5600 BIG-IP i5600 Local Traffic Manager)** в основния и резервен дейта център.	Ще се надградят функционално съществуващите две устройства **(модел: F5-BIG-LTM-I5600 BIG-IP i5600 Local Traffic Manager)** в основния и резервен дейта център.	Производител F5 Networks, Inc., модел BIG-IP i5600 to i5800 License Upgrade, BIG-IP Local Traffic Manager to Best Bundle Upgrade.
1.2.	Осигуряване на виртуализация на инсталираните и надградени модули и функционалности.	Осигуряване на виртуализация на инсталираните и надградени модули и функционалности.	https://www.f5.com/pdf/products/big-ip-platforms-datasheet.pdf
1.3.	Надграждането да включва лиценз за осигуряване на хардуерна компресия за минимум 18 Gbps	Надграждането включва лиценз за осигуряване на хардуерна компресия за 20 Gbps	https://www.f5.com/pdf/licensing/good-better-best-licensing-overview.pdf
1.4.	Надграждане на Network Firewall със следните функции: ▪ ICSA Certified Network L3-L4 Firewall ▪ Support for ACL ▪ Over 100 DoS vectors & Hardware-based DoS protections ▪ Dynamic IP intelligence & Blacklisting ▪ Remote Trigger Black Hole Filtering ▪ SSH Proxy policy protection Port misuse detection and mitigation	Надграждане на Network Firewall със следните функции: ▪ ICSA Certified Network L3-L4 Firewall ▪ Support for ACL ▪ Over 100 DoS vectors & Hardware-based DoS protections ▪ Dynamic IP intelligence & Blacklisting ▪ Remote Trigger Black Hole Filtering ▪ SSH Proxy policy protection ▪ Port misuse detection and mitigation	https://www.f5.com/pdf/products/big-ip-advanced-firewall-manager-datasheet.pdf https://www.f5.com/pdf/products/big-ip-dns-datasheet.pdf https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
1.5.	Надграждане на DNS firewall със следните функции: ▪ DNS Protocol inspection and validation ▪ DNS record type ACL ▪ DNS load balancing ▪ Complete DNSSEC signing ▪ Centralized DNSSEC key management	Надграждане на DNS firewall със следните функции: ▪ DNS Protocol inspection and validation ▪ DNS record type ACL ▪ DNS load balancing ▪ Complete DNSSEC signing ▪ Centralized DNSSEC key management	

1.	**Надграждане на устройство за балансиране на натоварването – 2 бр.**	**Параметри на предлаганата техника Надграждане на устройство за балансиране на натоварването – 2 бр.**	**Производител, модел или друг отличителен знак**
	▪ Top-level domain support for DNSSEC ▪ DNSSEC validation ▪ DNS DDoS Mitigation	▪ Top-level domain support for DNSSEC ▪ DNSSEC validation ▪ DNS DDoS Mitigation	
1.6.	Надграждане на Web Application Firewall със следните функции: ▪ XML Firewall ▪ Application DDoS protection ▪ OWASP Top 10 prevention ▪ Web scraping prevention ▪ Automated attack defense and bot detection ▪ Geolocation blocking	Надграждане на Web Application Firewall със следните функции: ▪ XML Firewall ▪ Application DDoS protection ▪ OWASP Top 10 prevention ▪ Web scraping prevention ▪ Automated attack defense and bot detection ▪ Geolocation blocking	
1.7.	Стандартна гаранционна поддръжка за срок не по-малък от 36 месеца, която да позволява софтуерни обновления до по-нова версия, обслужване „на място“. Да се включат всички необходими лицензи и софтуерни обновявания на сигнатурите за всички функционалности за срок не по-малък от 36 месеца.	Стандартна гаранционна поддръжка за срок от 36 месеца, която позволява софтуерни обновления до по-нова версия, обслужване „на място“. Включени са всички необходими лицензи и софтуерни обновявания на сигнатурите за всички функционалности за срок от 36 месеца.	
2.	**Устройство за балансиране на натоварването – 2 бр.**	**Устройство за балансиране на натоварването – 2 бр.**	
2.1.	Устройството да може да се клъстеризира по двойки с наличните **(модел: F5-BIG-LTM-I5600 BIG-IP i5600 Local Traffic Manager)** в основния и/или резервен дейта център, за осигуряване на висока степен на балансиране и резервираност.	Устройството може да се клъстеризира по двойки с наличните **(модел: F5-BIG-LTM-I5600 BIG-IP i5600 Local Traffic Manager)** в основния и/или резервен дейта център, за осигуряване на висока степен на балансиране и резервираност.	Производител F5 Networks, Inc., модел BIG-IP i5800 Best Bundle (48 GB Memory, SSD, Max SSL, Max Compression, vCMP) https://www.f5.com/pdf/products/big-ip-platforms-datasheet.pdf
2.2.	Устройството следва да осигури балансиране на Клиенти, достъпващи услуги чрез Интернет	Устройството осигурява балансиране на Клиенти, достъпващи услуги чрез Интернет	

1.	Надграждане на устройство за балансиране на натоварването – 2 бр.	Параметри на предлаганата техника Надграждане на устройство за балансиране на натоварването – 2 бр.	Производител, модел или друг отличителен знак
2.3.	Броят на Клиентите, достъпващи услуги чрез Интернет, да е неограничен.	Броят на Клиентите, достъпващи услуги чрез Интернет, е неограничен.	https://www.f5.com/pdf/licensing/good-better-best-licensing-overview.pdf https://www.f5.com/pdf/products/big-ip-local-traffic-manager-ds.pdf https://www.f5.com/pdf/products/big-ip-advanced-firewall-manager-datasheet.pdf https://www.f5.com/pdf/products/big-ip-dns-datasheet.pdf https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
2.4.	Устройството следва да осигури балансиране на служителите, достъпващи различни бизнес апликации чрез нейната локална мрежа.	Устройството осигурява балансиране на служителите, достъпващи различни бизнес апликации чрез нейната локална мрежа.	
2.5.	Устройството трябва да може да извлича информация за сървърите към услугата, която балансира (ping, достъп до порт, съдържание), за да разпределя само до наличните.	Устройството може да извлича информация за сървърите към услугата, която балансира (ping, достъп до порт, съдържание), за да разпределя само до наличните.	
2.6.	Трябва да е възможно изваждането на сървъра от балансирането без прекъсване на услугата.	Възможно е изваждането на сървъра от балансирането без прекъсване на услугата.	
2.7.	Устройството да поддържа виртуализация на инсталираните модули.	Устройството поддържа виртуализация на инсталираните модули.	
2.8.	Да са налични различни начини на балансиране като: ▪ Round Robin ▪ Least Connections ▪ Weighted Least Connections ▪ Maximum Connections ▪ Response Time ▪ Observed (Least Conn + Fastest Resp) ▪ Predictive (Observed over time) ▪ Dynamic Ratio (Based on server utilization)	Налични различни начини на балансиране като: ▪ Round Robin ▪ Least Connections ▪ Weighted Least Connections ▪ Maximum Connections ▪ Response Time ▪ Observed (Least Conn + Fastest Resp) ▪ Predictive (Observed over time) ▪ Dynamic Ratio (Based on server utilization)	
2.9.	Да разполага с минимум 12 физически слота, 4 от които да поддържат скорост от 40 Gb. Да се доставят 2бр. 10GBASE-SR SFP+ модула.	Разполага с 12 физически слота, 4 от които поддържат скорост от 40 Gb. Ще се доставят 2бр. 10GBASE-SR SFP+ модула.	
2.10.	Горните физически интерфейси трябва да позволяват формиране на port channel.	Горните физически интерфейси позволяват формиране на port channel.	

1.	Надграждане на устройство за балансиране на натоварването – 2 бр.	Параметри на предлаганата техника Надграждане на устройство за балансиране на натоварването – 2 бр.	Производител, модел или друг отличителен знак
2.11.	Устройството да може да работи в режим на работа Active/Active;	Устройството може да работи в режим на работа Active/Active;	
2.12.	Устройството трябва да има възможност за L3 и L2 балансиране на различните приложения.	Устройството има възможност за L3 и L2 балансиране на различните приложения.	
2.13.	Трябва да могат да се балансират SSL/TLS конекции.	Могат да се балансират SSL/TLS конекции.	
2.14.	Администрация и управление ▪ Интерфейсът на операционната система на устройството следва да бъде интуитивен. ▪ Администрацията на операционната система на устройството следва да допуска дефиниране на различни роли за различните типове потребители.	Администрация и управление ▪ Интерфейсът на операционната система на устройството е интуитивен. ▪ Администрацията на операционната система на устройството допуска дефиниране на различни роли за различните типове потребители.	
2.15.	Устройството следва да предоставя възможност за генериране на рапорти и мониторинг в следните направления: ▪ Да рапортува за наличност на услугите и участващите в тях сървъри/апликации. ▪ Да рапортува за натовареността на различните услугите и сървъри/апликации в тях. ▪ Да рапортува относно консумирания трафик. ▪ Устройството следва да предоставя опции за дефиниране на dashboard за администратор с цел бързо извеждане на актуалните рапорти и мониторинг.	Устройството предоставя възможност за генериране на рапорти и мониторинг в следните направления: ▪ Рапортува за наличност на услугите и участващите в тях сървъри/апликации. ▪ Рапортува за натовареността на различните услугите и сървъри/апликации в тях. ▪ Рапортува относно консумирания трафик. ▪ Устройството предоставя опции за дефиниране на dashboard за администратор с цел бързо извеждане на актуалните рапорти и мониторинг.	
2.16.	Минимални изисквания към устройство от система за балансиране: ▪ Производителност – минимум 35 Gbps L4/L7.	Параметри на устройство от система за балансиране: ▪ Производителност – 35 Gbps L4/L7.	

1.	**Надграждане на устройство за балансиране на натоварването – 2 бр.**	**Параметри на предлаганата техника Надграждане на устройство за балансиране на натоварването – 2 бр.**	**Производител, модел или друг отличителен знак**
	▪ L4 HTTP заявки за секунда - минимум 10M. ▪ L4 конкурентни връзки – минимум 40M. ▪ Хардуерен Offload SSL/TLS – минимум 18 Gbps. ▪ Памет – минимум 48 GB ▪ Хардуерна компресия – минимум 18 Gbps ▪ Резервирани захранвания 100-240 VAC – максимална консумирана мощност 680W за всяко от тях.	▪ L4 HTTP заявки за секунда - 12M. ▪ L4 конкурентни връзки – 40M. ▪ Хардуерен Offload SSL/TLS – 20 Gbps. ▪ Памет – 48 GB ▪ Хардуерна компресия – 20 Gbps ▪ Резервирани захранвания 100-240 VAC – максимална консумирана мощност 650W за всяко от тях.	
2.17.	Устройството да работи като Network Firewall със следните функции: ▪ ICSA Certified Network L3-L4 Firewall ▪ Support for ACL ▪ Over 100 DoS vectors & Hardware-based DoS protections ▪ Dynamic IP intelligence & Blacklisting ▪ Remote Trigger Black Hole Filtering ▪ SSH Proxy policy protection Port misuse detection and mitigation	Устройството ще работи като Network Firewall със следните функции: ▪ ICSA Certified Network L3-L4 Firewall ▪ Support for ACL ▪ Over 100 DoS vectors & Hardware-based DoS protections ▪ Dynamic IP intelligence & Blacklisting ▪ Remote Trigger Black Hole Filtering ▪ SSH Proxy policy protection Port misuse detection and mitigation	
2.18.	Задължително да отговаря на следните стандарти ETSI EN 300 328, EN 55032, EN 61000, EN 55024	Отговаря на следните стандарти ETSI EN 300 328, EN 55032, EN 61000, EN 55024	
2.19.	Устройството да работи като Web Application Firewall със следните функции: ▪ XML Firewall ▪ Application DDoS protection ▪ OWASP Top 10 prevention ▪ Web scraping prevention ▪ Automated attack defense and bot detection ▪ Geolocation blocking	Устройството работи като Web Application Firewall със следните функции: ▪ XML Firewall ▪ Application DDoS protection ▪ OWASP Top 10 prevention ▪ Web scraping prevention ▪ Automated attack defense and bot detection ▪ Geolocation blocking	

1.	**Надграждане на устройство за балансиране на натоварването – 2 бр.**	**Параметри на предлаганата техника Надграждане на устройство за балансиране на натоварването – 2 бр.**	**Производител, модел или друг отличителен знак**
2.20.	Устройството да работи като DNS firewall със следните функции: ▪ DNS Protocol inspection and validation ▪ DNS record type ACL ▪ DNS load balancing ▪ Complete DNSSEC signing ▪ Centralized DNSSEC key management ▪ Top-level domain support for DNSSEC ▪ DNSSEC validation ▪ DNS DDoS Mitigation	Устройството работи като DNS firewall със следните функции: ▪ DNS Protocol inspection and validation ▪ DNS record type ACL ▪ DNS load balancing ▪ Complete DNSSEC signing ▪ Centralized DNSSEC key management ▪ Top-level domain support for DNSSEC ▪ DNSSEC validation ▪ DNS DDoS Mitigation	
2.21.	Стандартна гаранционна поддръжка за срок не по-малък от 36 месеца, която да позволява софтуерни обновления до по-нова версия, обслужване „на място“. Да се включат всички необходими лицензи и софтуерни обновявания на сигнатурите за всички функционалности за срок не по-малък от 36 месеца.	Стандартна гаранционна поддръжка за срок от 36 месеца, която позволява софтуерни обновления до по-нова версия, обслужване „на място“. Включени са всички необходими лицензи и софтуерни обновявания на сигнатурите за всички функционалности за срок от 36 месеца.	

Предлагаме срок за изпълнение на поръчката (доставка и пускане в експлоатация на доставеното оборудване): до 2 (два) месеца, считано от датата на сключване на договора.

Декларираме, че

- Предлаганото оборудване ще бъде ново, оригинално, неупотребявано, в оригинална окомплектовка и опаковка, предвидена от производителя, придружено с инструкции за употреба и гаранционни карти и в срок на актуална гаранционна сервизна поддръжка;
- Предлаганото оборудване ще бъде комплектувано с всички необходими силови, интерфейсни и други кабели, адаптери и аксесоари, необходими за нормалната й работа. Захранването и кабелните накрайници на силовите кабели са предвидени за експлоатация в Република България;

- Предлаганото оборудване ще бъде напълно комплектувано така, че да бъде работоспособно и да изпълнява предвидените функциите. Ако се окаже, че дадено устройство не може да изпълнява дадена функция, то устройството ще се приведе в състояние, при което може да изпълнява функциите, заложени в спецификацията или ще бъде заменено с друго за сметка на изпълнителя.
- При изпълнение на доставката, в случай, че оферираните стоки вече не се произвеждат, ще бъдат доставени стоки с еквивалентни или по-добри технически характеристики без промяна в единичната цена и след предварително одобрение от възложителя.

Име и фамилия: Христо Великов
Длъжност: управител
Подпис и печат:

ЕВРОПЕЙСКИ СЪЮЗ

ЕДНА ПОСОКА
МНОГО ВЪЗМОЖНОСТИ

МИНИСТЕРСКИ СЪВЕТ

Приложение № 3

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

ЦЕНОВО ПРЕДЛОЖЕНИЕ

в процедура за възлагане на обществена поръчка с предмет:
„Осигуряване на система за киберзащита на ИСУН2020“
по Проект BG05SFOP001-4.002-0003-C01 „Повишаване на ефективността и ефикасността на Централното координационно звено“, Дейност 1: „Осигуряване на функционирането на информационните системи“, финансиран по Оперативна програма „Добро управление“

от „Комсофт“ ООД, ЕИК/БУЛСТАТ: 030435072, представлявано от Христо Анчев Великов в качеството на управител, адрес Република България, гр. София 1202, район „Възраждане“, бул. „Княгиня Мария Луиза“ № 47, телефон +359 2 981 4566, факс +359 2 987 1723, електронна поща sales@comsoft.bg,

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

С настоящото Ви представяме нашето ценово предложение за изпълнение на обявената от Вас обществена поръчка с предмет: „Осигуряване на система за киберзащита на ИСУН2020“ по Проект BG05SFOP001-4.002-0003-C01 „Повишаване на ефективността и ефикасността на Централното координационно звено“, Дейност 1: „Осигуряване на функционирането на информационните системи“, финансиран по Оперативна програма „Добро управление“, както следва:

Общата предлагана от нас цена за изпълнение на поръчката възлиза на: 728,624.00 лева (седемстотин двадесет и осем хиляди шестстотин двадесет и четири лева) без ДДС, респ. 874,348.80 лева (осемстотин седемдесет и четири хиляди триста четиридесет и осем лева и осемдесет стотинки.) с включен ДДС.

/Христо Великов/

COMSOFT . LTD. ComSoft SOFIA

Общата предлагана цена е формирана, както следва:

Наименование	Броя у-ва	Единична цена в лв. без вкл. ДДС	Обща цена в лв. без вкл. ДДС
Надграждане на устройство за балансиране на натоварването	2	138,172.00	276,344.00
Устройство за балансиране на натоварването	2	226,140.00	452,280.00
		Общо в лв. без вкл. ДДС	728,624.00

Предложената от нас цена включва всички разходи за цялостното, точно, качествено и срочно изпълнение на поръчката, съгласно нормите и нормативите, предвижданията и изискванията на Документацията за участие, предложените от нас условия за изпълнение на поръчката, проектодоговора, както и всички законови изисквания за осъществяване на всички дейности, включени в предмет на горепосочената обществена поръчка в съответния вид и обем.

Цената за изпълнение е крайна и представлява възнаграждението за извършване на всички дейности за изпълнение на предмета на поръчката.

Ценовото предложение е формирано на база единични цени, които са окончателни, като са взети предвид всички разходи, свързани с изпълнение на предмета на обществената поръчка.

Име и фамилия: Христо Великов
Длъжност: управител
Подпис и печат:_____

ComSoft Ltd. SOFIA

Всяка страница от ценовото предложение трябва да е подписана и подпечатана от участника, като се посочи име и фамилия на лицето поставило подписа.

ЗАБЕЛЕЖКА: *Този документ задължително се поставя от участника в отделен запечатан непрозрачен плик – ПЛИК с надпис „Предлагани ценови параметри от ……..(име на участника)“*