

## ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

### Предмет

Осигуряване на решение за „Изграждане на система за защита на информацията, автоматизирано архивиране и възстановяване на данните в ИСУН2020

### Цел

1. Да се изгради надеждно решение за защита на информацията и надеждно автоматизирано архивиране и възстановяване данните в ИСУН2020, което трябва да осигури необходимия капацитет и производителност на устройствата архивирани данните на информационната система, тяхната защита от технически повреди или злонамерени действия, както и да осигури нужния капацитет за тестово възстановяване и последващо верифициране на процеса по архивиране и възстановяване на ИСУН2020.

2. Осигуряване на допълнителни изчислителни ресурси за планираните нови свързани информационни системи, като: изграждане на предвидения ГИС компонент към ИСУН2020, изграждане на новата система за управление и наблюдение на националните инвестиции и т.н.

### Обхват

За постигане на заложените цели е необходимо да бъдат извършени следните основни дейности:

- Доставка на специализирано хардуерно оборудване и софтуер за изграждане на цялостно единно решение за автоматизирано архивиране и възстановяване на ИСУН2020 и осигуряване на допълнителни изчислителни ресурси;
- Инсталиране и конфигуриране на доставеното хардуерно оборудване, съобразно наличното оборудване и дизайна.
- Инсталиране и конфигуриране на доставените софтуерни продукти, съобразно дизайна на решението
- Изграждане на пълно функционално и надеждно решение за защита на информацията, автоматизирано архивиране и възстановяване на.
- Функционални тестове за работоспособност, включително проверка на процедурите по възстановяване на данните на ИСУН2020 в цялост.

### Място на изпълнение

Дейностите трябва да бъдат изпълнени в Контролно-техническия център на електронното правителство (КТЦЕП) включващ основния продуктивен център (ДХЧО) и резервния център на ИСУН2020.

### Технически изисквания

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, Държавната агенция електронно управление (ДАЕУ) е изградила и продължава надграждането на Държавен хибриден частен облак (ДХЧО), осигуряващ споделени информационни ресурси за електронните 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 ДХЧО, 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.

Следвайки политиката за електронно управление и принципите, залегнали в Програмата на правителството, Информационната система за управление и наблюдение на средствата от ЕС (ИСУН2020) беше мигрирана и понастоящем предоставя своите услуги от ДХЧО, като за тази цел е изградено реално сътрудничество със Държавната агенция електронно управление.

Понастоящем ИСУН2020 разполага с Център за възстановяване след бедствие (Disaster Recovery Center (DRC)), осигуряващ безпроблемната работа на ИСУН2020 в случай на бедствие или аварии на основния център за данни - ДХЧО.

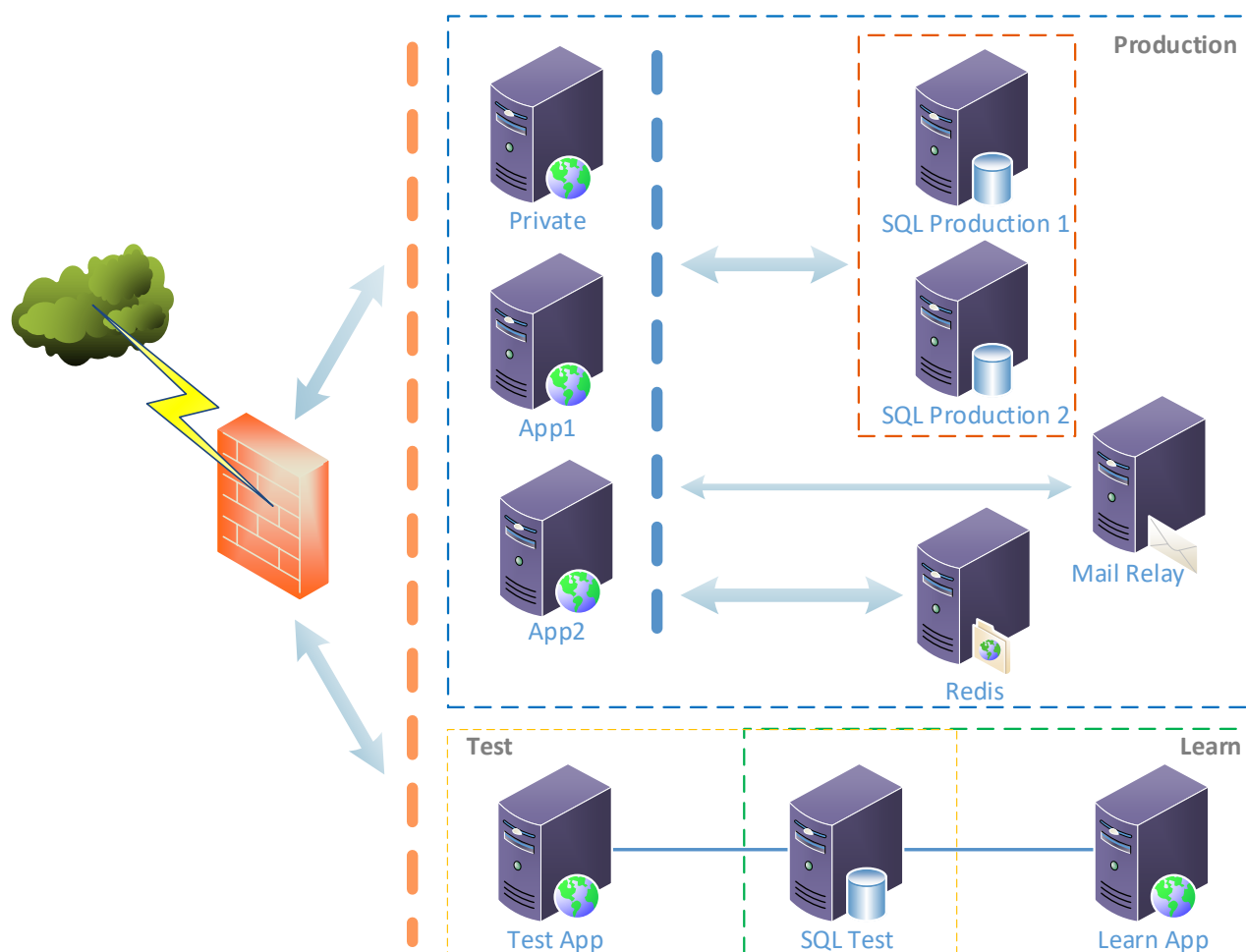
Системата ИСУН2020 използва следните хардуерни и софтуерни инфраструктурни ресурси:

- 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;
- система за киберзащита и балансиране на натоварването, базирана на продукти и технологии на F5;
- висококапацитетна сървърна инфраструктура изградена от висок клас сървърен хардуер Cisco UCS.
- среда за виртуализация, реализирана на базата на Microsoft Hyper-V.
- среда за съхранение на данни – дискови масиви HPE и EMC за осигуряване на нужния дисков капацитет. Съобразявайки се с регламентите на ЕК за програмен период 2014 - 2020, ИСУН2020 е реализирал функционалности, за които по предварителна оценка ще бъдат необходими 64 TiB данни.

На приложно ниво ИСУН2020 е WEB-базирана информационна система, съхраняваща данните в структуриран вид. Системата е изградена на база на технологиите Microsoft 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 информационната система 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

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

#### *Резервен център*

- **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 – работещи в конфигурация AlwaysOn с базите данни в продуктивната среда.

За осигуряване на висококачествената конфигурация има изградена Активна Директория със съответните Домейн Контролери (DCs) във всеки сайт.

С цел да се гарантира цялостна защита на данните от евентуални технически повреди или злонамерени действия е необходимо да се изгради нова единна система за автоматизирано архивиране и възстановяване (в случай на необходимост). Решението следва да е предвидено да работи в два географски отделени центъра с два отделни, но взаимно свързани компонента – софтуер и специализирани устройства за архивиране и възстановяване с дискови носители с оглед осигуряване на резервни копия на данните и гарантиране на наличност и пълна функционалност на системата във всеки един от центровете. То трябва да позволява двупосочна криптирана репликация на архивите между двете архивни устройства. С цел на запазване на пълната функционалност и бързодействие при настъпване на критично събитие независимо от локацията, двете устройства трябва да са конфигурирани с една и съща огледална конфигурация.

С цел постигане на проследимост и мониторинг на извършените действия по архивиране и възстановяване, решението трябва да предлага автоматично създаване и изпращане на отчети, автоматично изпращане на съобщения при настъпване на критични събития, „лог“ на действията от различните оторизирани потребители.

С цел минимизиране на времето за архивиране на голям обем от данни (TiB), решението трябва да притежава функционалности като: компресиране и дедупликация на данните, както при софтуерните клиенти, така и върху хардуерните устройствата за архивиране. Това позволява създаване на процес за архивиране съставен изцяло от множество пълни архиви (full backup), като по този начин многократно се намалява времето за възстановяване на данните и се осигурява необходимата производителност.

За осигуряване на работещо решение с необходимата гъвкавост в настоящата среда, както и при бъдещото ѝ развитие, предложеното решение трябва да поддържа Microsoft Hyper-V и VMware vSphere среди.

С цел задоволяване на специфичните нужди на всяко отделно приложение за продължителност на съхранение на архивите, решението трябва да предлага функционалност за определяне на различна продължителност на съхранение на всяка от архивните задачи и дефиниране на т. н. „**Златно копие**“, специален тип архив защитен от външни влияния и умишлени злонамерени въздействия. За повишаване на сигурността на направените архиви, решението да трябва да предлага възможност за заключване на част от архивните копия, които не могат да бъдат променяни/изтривани, дори и от потребители с делегирани пълни административни права, преди изтичане на определен период от време.

Решението следва да включва софтуер и специализирани устройства за архивиране и възстановяване с дискови носители - HDD (лентовите носители са остаряла технология и не трябва да се съдържат и/или използват в предложения дизайн), като по-този начин се гарантира висока наличност и надеждност с цел постигане на високо-надеждна, устойчива и скалируема конфигурация, както в посока увеличаване на бързодействие, така и в посока увеличаване на капацитета.

Минимални параметри и брой на техническите средства (включително софтуер):

**Специализирано устройство за архивиране и възстановяване на данни с дискови носители – 2 броя**

Всяко устройство следва да осигурява необходимия капацитет от мин. 180 TiB RAW. Архитектурата да гарантира защита и резервираност на управлението, храненето, охлаждането, пътищата за достъп. Дисковете да са hot plug и конфигурирани в RAID 6 или еквивалент. Да осигурява дедупликация при софтуерните клиенти и върху самото устройство, компресия на данните, криптиране на данните, двупосочна криптирана репликация, функционалност за задаване на продължителност на съхранение на всяка от архивните задачи и предпазване на данните от промяна. Да се интегрира за работа с Microsoft Hyper-V и VMware vSphere среди, бази данни на Microsoft, Oracle, IBM.

**Софтуерен пакет за архивиране и възстановяване на данни – 1 брой**

Да осигурява единна графична конзола за управление на процесите по архивиране и възстановяване на данни от физически сървъри (OS MS Windows, Linux) и виртуални среди (Microsoft Hyper-V и VMware vSphere), работещи в SAN среда (Fibre Channel свързаност). Да работи в два географски отделени центъра и да включва лицензи за общо 100 TiB входящ капацитет за неограничен брой клиенти, без значение от използваната функционалност или валидност на поддръжка / абонамент. Да осигурява като минимум създаване на резервни копия - Full, Incremental, Synthetic Full Backups за файлови системи и виртуални машини. Да осигурява архивиране и възстановяване на цели виртуални машини, възстановяване на отделни файлове от виртуална машина без да е необходимо възстановяване на цялата виртуална машина, стартиране на виртуални машини от архив без да е необходимо предварителното им възстановяване (instant recovery). Да осигурява дедупликация, компресия и криптиране на данните. Да се интегрира за работа с Microsoft Windows Volume ShadowCopy Service (VSS), да включва онлайн архивиране на бази данни на Microsoft, Oracle, IBM. Да позволява създаване на резервно копие от snapshot от наличните дискови масиви. Да разполага със средства за управление и наблюдение на процесите, да предлага автоматично създаване и изпращане на отчети, автоматично изпращане на съобщения при настъпване на критични събития, „лог“ на действията от различните оторизирани потребители.

**Шаси за сървъри за разширение на съществуваща сървърна система Cisco UCS – 1 брой**

Да е съвместимо за работа с наличната система Cisco UCS и да се управлява от наличните модули UCS 6296UP Fabric Interconnect Module. Да осигурява слотове за мин. 8 half-width блейд сървъра, 40Gb Ethernet комуникация за всеки сървър чрез шината за вътрешна комуникация, резервираност на храненията и свързаността.

**Сървъри от модулен тип (блейд сървъри) – 4 броя**

Сървърите да са съвместими за работа с наличната система Cisco UCS, да се управляват от наличните модули UCS 6296UP Fabric Interconnect Module, да се монтират в

шаси за сървъри за разширение на съществуваща сървърна система Cisco UCS. Всеки сървър да разполага с 2 броя процесори от тип Intel Xeon Gold или еквивалентни, 3,20 GHz работна честота, 8 ядра; 256 GB DDR4 памет, два броя дискове 300GB 10K SAS, конфигурирани в RAID 1, мин. 40 Gbps мрежови адаптер, позволяващ виртуализиране на мрежови карти от тип Ethernet NIC и/или Fibre Channel HBA.

#### **Допълнителен капацитет за дисков масив за съхранение на данни Dell EMC Unity 400 – 1 брой**

Да се достави и инсталира допълнителен дисков капацитет за разширение на съществуващ дисков масив EMC Unity 400 - 4 броя дискови кутии за Unity 400 за 25 броя 2.5“ дискове, мин. 19 броя 2.5“ високопроизводителни SSD/Flash дискове с обем 800 GiB, мин. 83 броя 2.5“ SAS бързи дискове (минимум 10K rpm) с обем 1.2 TiB.

#### **Софтуер за изграждане на среда за виртуализация, базирана на Hyper-V – 1 брой**

За изграждане на виртуална среда, технологично идентична с използваната, е необходимо да се доставят следните лицензи:

Windows Server Datacenter Edition – за мин. 64 ядра (съобразно архитектура на модулните сървъри)

System Center Datacenter Edition за мин. 64 ядра (съобразно архитектура на модулните сървъри)

#### **ИЗИСКВАНИЯ КЪМ ОБОРУДВАНЕТО:**

- Предлагащото оборудване следва да съблюдава точно характеристиките и параметрите на артикулите, посочени в технически спецификации.
- Предлагащото 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 сервисна поддръжка.
- Предлагащата техника трябва да бъде комплектувана с всички необходими силови, интерфейсни и други кабели, адаптери и аксесоари, необходими за нормалната ѝ работа. Захранването и кабелните крайници на силовите кабели да са предвидени за експлоатация в Република България;
- Предлагащата техника трябва да бъде напълно комплектувана така, че да бъде работоспособна и да изпълнява предвидените функции. 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, заложи в спецификацията или да бъде заменено с друго за сметка на изпълнителя.
- При изпълнение на доставката, в случай, че офериранияте 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.
- 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.

#### **ИЗИСКВАНИЯ КЪМ РЕАЛИЗАЦИЯТА**

- Изпълнителят трябва да предложи дизайн на предложеното решение.

Решението да включва:

- ✓ изграждане на система за архивиране и възстановяване на ИСУН2020 в два географски отделени центрове за данни,
  - ✓ репликация на данните между двата центъра,
  - ✓ процедури за регулярно архивиране на информацията,
  - ✓ процедури за възстановяване на информацията,
  - ✓ процедури за регулярно тестване на целостта на архивираните данни
- ИЗПЪЛНИТЕЛЯТ трябва да изготви функционални тестове, чрез които ще се верифицира правилното функциониране на изградената система за архивиране и възстановяване на данни.
  - 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.
  - Срок за изпълнение на дейностите – до 4 (четири) месеца от датата на подписване на договора.

### **ГАРАНЦИОННА ПОДДРЪЖКА**

- Дейностите по хардуерната поддръжка трябва да се извършват на място.
- 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.
- 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 подмененото оборудване.
- 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.
- 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).
- Всички подменени технически компоненти трябва да фигурират в актуалната сервизна или ценова листа на съответния производител.
- В рамките на осигурената от ИЗПЪЛНИТЕЛЯ поддръжка, трябва да се гарантират следните времена за реакция и отстраняване на възникнал проблем:
  - ✓ Ниво на покритие - 24 x 7;
  - ✓ Време за реакция (време за приемане на заявката за възникнал проблем) – до 4 часа;
  - ✓ Време за отстраняване на възникнал проблем: до 3 (три) работни дни.
- Дейностите по гаранционна поддръжка включват корективно поддържане на нормалната работоспособност на инсталирания системен софтуер при поискване.
- При необходимост ИЗПЪЛНИТЕЛЯТ извършва възстановяване на системата при пълна или частична неработоспособност в следствие на инцидент.
- При необходимост ИЗПЪЛНИТЕЛЯТ асистира и/или управлява промените на ниво хардуер и ниво системен софтуер.

- 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.
- 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.