***ПРИЛОЖЕНИЕ № 1***

# ТЕХНИЧЕСКО ЗАДАНИЕ И ТЕХНИЧЕСКИ ИЗИСКВАНИЯ

## I. Обща информация за поръчката

Българското електронно управление (БеУ) се явява неотделим структуроопределящ компонент от високо ниво на свързаните и взаимодействащи помежду си административни информационни системи (АИС) в Република България, имащи отношение към предоставянето на публични услуги.

Постоянна задача е експлоатационната поддръжка, управление на конфигурацията, гарантиране на информационната сигурност и усъвършенстването на действащата инфраструктурна среда в съответствие с най-актуалните ИТ тенденции, осигурявайки функционирането на обособените системни решения (Електронен портал за достъп до електронни административни услуги - ЕПДЕАУ, Регистри за оперативна съвместимост - РОС, Единна среда за обмен на електронни документи - ЕСОЕД-ESB), интегрирани в БеУ, както и осигуряване на условия за развитието им и добавяне на нови компоненти и системни решения, без да се нарушава работата на съществуващите.

Националната инфраструктурна среда на БеУ се базира на два взаимосвързани обекта.

- Контролно-технически център на БеУ - Бояна (КТЦБеУ), град София;
- Териториалния Център на БеУ (ТЦБеУ) в град Варна.

**Основни системни компоненти на инфраструктурната среда**

**Единна среда за обмен на електронни документи**

**ЕСОЕД-ESB - Единна среда за обмен на електронни документи (ЕСОЕД-ESB)** – управляема среда, която се използва като единна входна точка за предоставяне на услуги от администрациите (МИСУД) както и за версиониране на услугите.

ЕСОЕД-ESB (Enterprise Service Bus) е основен компонент за ефективна реализация на архитектура ориентирана към услуги (SOA). ЕСОЕД-ESB осигурява сигурна среда за услуги за оперативна съвместимост и транспорт на съобщения между различни системи, използвайки разнообразие от уеб услуги, XML, адаптери за интеграция, рутиране основано на правила, и свързани технологии.

ЕСОЕД-ESB (Enterprise Service Bus) в качеството си на набор от интеграционни технологии позволява динамичната свързаност и обмен на данни и съобщения между автономни системи.

**Единният портал за достъп до електронните административни услуги (ЕПДЕАУ)**

Единният портал за достъп до електронните административни услуги е неделима част от модела на електронно управление, чиито основни цели са:

- Осигуряване на сигурен и удобен канал за комуникация с потребителите на електронни административни услуги: администрация – граждани (G2C) и администрация – бизнес (G2B);
- Изграждане на единна входна точка за предоставяне на услуги по достъпен начин и в удобен за потребителите диалогов режим;
- Осигуряване на работа с електронно подписани документи;
- Реализиране на портална архитектура, базирана на най-модерните тенденции за разпределяне на натоварването (load-balancing) и възстановяване при аварии (disaster recovery).

Същевременно Единният портал за достъп до електронни административни услуги съдържа и информация, имаща за цел да подпомогне потребителя в процеса на заявяване на електронни административни услуги:

**Регистри за оперативна съвместимост**

Информационната система на Регистъра на електронни услуги (РЕУ) и Регистъра на информационни обекти (РИО) е реализирана в съответствие с изискванията, заложени в подзаконовите нормативни актове, предвидени в Закона за електронното управление. Осигурено е резервиране (чрез репликация) на двата регистъра в териториалния център на БеУ в гр. Варна.

Регистърът на регистрите и данните – РРД е обособен като самостоятелен информационен обект с цел събиране и поддържане на база данни за всички регистри и/или раздели от регистри и данни.

Регистрите са реализирани като централизирани бази данни и функционират в режими Intranet – за вътрешно ползване в рамките на ведомството (администриране и поддръжка, въвеждане и контрол на информация, справки, търсене, ведомствени информационни услуги и т.н.) и Internet – търсене и информационни услуги за публично ползване. Същите са интегрирани като неотменна част от ИСЕП.

**Други компоненти на инфраструктурната среда:**

- **Система за оторизация и автентикация на потребителите - MS Active Directory** – Директорийната услуга Active Directory е разпределена директорийна услуга, която е включена в операционните системи Microsoft Windows Server 2008, Microsoft Windows Server 2003 и Microsoft Windows 2000 Server. Внедряването на Active Directory позволява централизираната поддръжка и сигурно управление на мрежовите ресурси в цялата организация. Active Directory предоставя централизирана конзола за администриране на мрежата, делегиране на административни права, достъп до обекти представляващи всички мрежови потребители, устройства и ресурси, възможност за групиране на обекти за лесно управление и прилагане на политики.
- **Система за управление на достъпа до Интернет -** Системата за управление на достъпа до Интернет и сигурен достъп до системата за електронна поща е изградена на базата на Microsoft Internet Security and Acceleration (ISA) Server 2006 Standard Edition. ISA Server 2006 предлага съвременна защита, бърз и сигурен достъп за всички видове

мрежи. ISA Server съдържа съвременна защитна стена, работеща на ниво приложение и предоставя защита за всички видове заплахи – външни и вътрешни за организацията.

- **Система за електронна поща и съвместна работа -** Системата за електронна поща е изградена на базата на Microsoft Exchange Server 2003**.**

  Системата за електронна поща, освен че се използва по предназначение (т.е. пощенски кутии на служители от областни и общински администрации), също така обслужва и всички приложения в КТЦЕП, които имат функция за автоматично известяване по e-mail за настъпило събитие.

- **Система за оперативни актуализации на системните и приложните софтуерни пакети -** Изградена е на базата на HP Open View Configuration Management. Целта на системата е ефективно инсталиране и управление на софтуерни продукти и съдържание през хетерогенни компютърни платформи от интернет базирана конзола. Тя се използва за управление на системния софтуер на сървъри и операторски системи.

  Принципът на работа на системата се състои в отдалечена инсталация на клиентската част, която от своя страна събира нужната информация и сървърната я съхранява и визуализира.

  **Система за архивиране на критични данни HP OpenView Data Protector -** Чрез тази система се управляват данни, като се автоматизира архивирането и възстановяването им от диск или лента. Това осигурява 24x7 бизнес операции и оптимизира IT ресурсите. HP OpenView Data Protector е архивиращ софтуер, който предоставя възможността за обширен мениджмънт на данни с изцяло автоматизирано архивиране и възстановяване.

- **Система за централизирано управление и наблюдение на ИТ ресурсите на интеграционната система на БеУ и свързаните с него обекти -** системата е базирана на модулите**:**
  - ✓ HP OpenView Operations Manager for Unix
  - ✓ HP OpenView Network Node Manager Advanced Edition
  - ✓ HP OpenView Performance Manager
  - ✓ HP OpenView Performance Insight
  - ✓ HP Service Manager
  - ✓ HP Discovery and Dependency Mapping Inventory,,
  - ✓ HP Site Scope
- **Централизирана система за управление на комуникационната и хардуерната инфраструктура чрез консолидация**

  **Системата е съставена от:**
  - ✓ Платформа за виртуализация тип 1 – VMWare vSphere 5.0
  - ✓ Платформа за виртуализация тип 2 – Citrix Xen Desctop 5.6
  - ✓ Платформа за виртуализация тип 3 – Microsoft Hyper-V
  - ✓ Платформа за виртуализация тип 4 – HP Integrity Virtual Machines

- **Система за удостоверителни услуги (PKI основен и резервен)**

**<u>Софтуерни компоненти:</u>**

- ✓ InfoNotary софтуерен модул за реализиране издаването и управлението на удостоверения за електронен подпис и поддържане на регистър за тях InfoNotary софтуерен модул за осигуряване на LDAP и OCSP достъп до регистъра на удостоверенията;
- ✓ InfoNotary софтуерен модул за Time Stamps услуги по удостоверяване на време;
- ✓ InfoNotary софтуерен модул за проверка и валидиране на удостоверения за електронен подпис и на електронно подписани документи;

**Хардуерни компоненти:**

- ✓ nCipher netHSM F3,
- ✓ bundle 2000 IPS
- ✓ nShieldF3PCI500TPS

- **Система за отчитане на единно време**

**Софтуерни компоненти:**

- ✓ InfoNotary софтуерен модул за услуги по заверки на удостоверено единно време
- ✓ InfoNotary софтуерен модул за синхронизация на единно време
- ✓ Audit Server for Domain Time II софтуерен модул за одит и мониторинг на синхронизациите

**Хардуерни компоненти:**

- ✓ SyncServer S250 Специализирано хардуерно оборудване за синхронизация на времето София и Варна.

**Регистриране на всички потребителски действия -** Системите регистрират всички потребителски действия, свързани с влизане в системата, въвеждане, коригиране и изтриване на данни.

Регистрите за одит съдържат като минимум следните данни: дата и час на влизане в системата и излизане от системата, време на работа, данни за потребителя, IP адрес на машината, вид на действията и препратки към извършените промени.

- **Регистри за оперативна съвместимост (РОС)**

Осигуряват формализирани технологични описания на обектите, системите и услугите с цел оперативна съвместимост на информационните системи:

- ✓ Регистър на регистрите
- ✓ Регистър на информационните обекти - база от данни, управлявана от информационна система и съдържаща формализирани технологични описания на информационните обекти
- ✓ Регистър на електронните услуги - база от данни, управлявана от информационна система и съдържаща формализирани технологични описания на електронните услуги, предоставяни от администрациите

Изпълнителят е длъжен да осигури защитен локален и отдалечен достъп за администриране на съдържанието на регистрите за оперативна съвместимост от оторизирани представители на възложителя.

## 1. Компоненти на информационната система на Регистрите за оперативна съвместимост

Информацията за регистрите се съхранява в единна база данни, която се управлява от Oracle Database Server СУБД.

Подсистемата предоставя няколко различни входни точки за достъп до данните в зависимост от характеристиките на нуждите от информация и от разрешените операции върху данните.

- **Системи извън състава на БеУ, базирани върху инфраструктурна среда:**
- **Система за управление на човешките ресурси**

Изпълнителят е длъжен да изгражда и поддържа защитени канали за отдалечен достъп на оторизирани лица от държавната администрация за управление на съдържанието на системата, чрез писмено възлагане от възложителя.

Изпълнителят е длъжен да изгражда и поддържа защитени канали за отдалечен достъп на оторизирани лица от държавната администрация за управление на съдържанието на системата, чрез писмено възлагане от възложителя.

- **Административен регистър**

Изпълнителят е длъжен да изгражда и поддържа защитени канали за отдалечен достъп на оторизирани лица от държавната администрация за управление на съдържанието на регистъра, чрез писмено възлагане от възложителя.

- **Регистър на европейското право**

Изпълнителят е длъжен да изгражда и поддържа защитени канали за отдалечен достъп на оторизирани лица от държавната администрация за управление на съдържанието на регистъра, чрез писмено възлагане от възложителя.

- **Портална инфраструктура за стандартизиране на уеб сайтовете на българската държавната администрация**

Изпълнителят е длъжен да изгражда и поддържа защитени канали за отдалечен достъп на оторизирани лица от държавната администрация за управление на съдържанието на порталната инфраструктура чрез писмено възлагане от възложителя.

- **Подсистема за удостоверителни услуги на Комисия за регулиране на съобщенията (сгс PKI), към PKI системата на инфраструктурната среда на проект БЕУ**

  **<u>Софтуерни компоненти</u>**

  - ✓ nCipher софтуерен лиценз за връзка на сървър с netHSM F3 TPS 2000 bundle

  **<u>Хардуерни компоненти</u>**

  - ✓ nCipher криптографски модул nToken за връзка с netHSM F3 TPS 2000 bundle

- **Среда, осигуряваща електронни разплащания в процеса на предоставяне на административни услуги по електронен път, чиято цел е:**
  - ✓ Да осигури техническа възможност на отделните администрации да предоставят на гражданите и фирмите информация за дължимите от тях данъци, такси и др., чрез Интернет.

- ✓ Да осигури техническа връзка между администрацията и банките в страната (а също и системите за електронни плащания с карти VISA и MasterCard). Посредством тази връзка, всички участници в СРЕДАТА (администрациите и банките) могат да обменят в реално време информация, свързана с плащането на административни услуги
- ✓ Да осигури на администрацията автоматично потвърждение, по електронен път за извършените от гражданите и фирмите плащания.

Изпълнителят е длъжен да изгражда и поддържа защитени канали за отдалечен достъп на оторизирани лица от държавната администрация за управление на следните модули и интерфейси на системата:

- ✓ Управление на модул за автоматизиран обмен на данни с доставчици на административни услуги
- ✓ Управление на модул за автоматизиран обмен на данни с платежни оператори - доставчици на платежни услуги
- ✓ Управление на интерфейс за крайни потребители - ползватели на административни услуги
- ✓ Управление на справочен интерфейс
- ✓ Управление на административен интерфейс

- **Система за самооценка на административното обслужване**

Изпълнителят е длъжен да изгражда и поддържа защитен отдалечен достъп до системата за управление на съдържанието от оторизирани представители на държавната администрация чрез писмено възлагане от възложителя.

- **Национален портал за транспортна информация и електронни услуги**

Порталът предоставя пътна и трафик информация в реално време.

Изпълнителят е длъжен да изгражда и поддържа защитен отдалечен достъп до системата за управление на съдържанието от оторизирани представители на държавната администрация чрез писмено възлагане от възложителя.

- **Помощни системи към инфраструктурната среда:**

Помощните системи включват климатизиращи, токозахранващи, електрорезервиращи, пожароизвестителни и пожарогасителни системи и системи за достъп, които са налични в двата центъра.

**Възложителят носи отговорност за:**

- Общ контрол на действието на системите.
- Дейности по координация при присъединяване на поддържаните системи от инфраструктирната среда към системата за електрозахранване;
- Дейности по осигуряване на нормална климатична среда за сървърните зони в двата центъра, според предписанията на производителите на оборудването.
- Дейности по осигуряване на нормална ежедневна чистота и запрашеност на въздуха на територията на двата центъра в съответствие с изискванията на производителите на оборудването и екологичните норми

**Изпълнителят носи отговорност за:**

Поддръжката, ремонта и профилактика на помощните системи в двата центъра.

Спецификацията на наличното хардуерно и комуникационно оборудване е посочена в Приложение № 1 от настоящата документация.

**II. Дейности, включени в обхвата на поръчката**

**Общи дейности**

- Цялостен технически одит на одит на системите на БеУ в КТЦЕП „Бояна“ и ТЦЕП „Евксиноград“ - Варна
- Анализ на състоянието на системата за експлоатационно осигуряване и поддръжка.
- Ежедневно оперативно наблюдение и поддържане функционирането на системата.
- Експлоатационна поддръжка на софтуерни компоненти на системата.
- Осигуряване на надеждна и непрекъсната работа на потребителите, дефинирани като активни в системата.
- Информационно осигуряване - управление и съхранение на данните на информационната система.
- Гарантиране на информационна сигурност на системата.
- **Помощни системи към инфраструктурната среда:**

Помощните системи включват климатизиращи, токозахранващи, електрорезервиращи, пожароизвестителни и пожарогасителни системи и системи за достъп, които са налични в двата центъра.

**Възложителят носи отговорност за:**

- Общ контрол на действието на системите.
- Дейности по координация при присъединяване на поддържаните системи от инфраструктирната среда към системата за електрозахранване;
- Дейности по осигуряване на нормална климатична среда за сървърните зони в двата центъра, според предписанията на производителите на оборудването.
- Дейности по осигуряване на нормална ежедневна чистота и запрашеност на въздуха на територията на двата центъра в съответствие с изискванията на производителите на оборудването и екологичните норми

**Изпълнителят носи отговорност за:**

Поддръжката, ремонта и профилактика на помощните системи в двата центъра.

Изпълнителят следва да изготви вътрешни правила за оценка и управление на риска за мрежова и информационна сигурност в обхвата на поддържаната от него система и компоненти за центровете в София и Варна.

Препоръчителните действия по оценка и управление на риска трябва да съответстват на Приложение № 3 към чл. 31, ал. 2 от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност (обн., ДВ, бр. 101 от 2008 г., изм., бр. 58 от 2010 г., изм. и доп., бр. 102 от 2010 г. и бр. 48 от 2013 г.)

Потенциалните рискови фактори за мрежовата и информационната сигурност, формулирани и класифицирани в международния стандарт ISO/IEC TR 13335:2000, са посочени в Приложение № 4 към чл. 31, ал. 3 от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.

Управлението на сигурността да се осъществява на база на доставени и внедрени решения в инфраструктурата на БеУ.

За целите на настоящата поръчка взаимодействията с екипите на трети страни - външни доставчици на компоненти и услуги, по силата на вече съществуващи договори, се координират и контролират от възложителя.

**Дейност 1: Цялостен технически одит и анализ на системите на БеУ в КТЦЕП „Бояна“ и ТЦЕП „Евксиноград“ - Варна**

Изпълнителят ще трябва да извърши:

- Анализ на съществуващата информационна система на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС (експлоатационна и тестова среда) и текущия статус на всичките й компоненти;
- Анализ на интегрираността с останалите системи и комуникационна инфраструктура на БеУ (PKI, сървър за синхронизация и др.);
- Изготвяне на детайлен доклад за състоянието на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС след направения анализ, обосновани предложения за оптимизация и развитие.
- Изготвяне на схема за работните процеси и отговорностите по поддръжката на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС;
- Изготвяне на детайлен план за реализиране на дейността по експлоатационното поддържане на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС;
- Одит на степента на сигурност от гледна точка на неоторизиран достъп, въздействие и влияние върху информацията и данните;
- Оценка на риска от неправилно изграждане и управление на системите;
- Оценка на ефективността на използваните информационни технологии и анализ на възможността за оптимизирането им;
- Оценка на оперативната съвместимост и информационната сигурност при обмена на електронни документи в инфраструктурата на БеУ;
- Издаване на препоръки за повишаване сигурността на системите и инфраструктурата.

Специфичните дейности, свързани с тази дейност, да са както следва:

- Софтуерно обследване на техническото състояние на наличното хардуерно, комуникационно и софтуерно оборудване (сървъри, системи за съхранение на данни, операционни системи, системен софтуер за мониторинг, архивиране , анти-вирусна защита, и др.);
- Обследване на комуникационната архитектура, включваща мрежово и комуникационно оборудване, връзки към Интернет, връзки между отделните вътрешни и външни организации, защитни стени, техните параметри и конфигурации, и др.;
- Обследване и коментари по приложната архитектура, включващ стандартен приложен софтуер и специализирани приложения;
- Обследване и документиране на конфигурациите в ИТ инфраструктурата по звена.

Специфичните дейности, свързани с тази дейност, са както следва:

- Обследване на информационната сигурност на системите, комуникациите и базите данни, осигуряващи работата на различните информационни системи;
- Обследване и оценка на състоянието на наличния системен софтуер, включващ версии, приложени актуализации и други;
- Обследване и оценка на работоспособността на звената, осигуряващи работата на различните информационни системи;
- Обследване и оценка, свързани с наличието на задължителни правила и процедури, отнасящи се до ИТ инфраструктурните звена, съгласно най-добрите практики в областта;
- Обследване и оценка на методите за системна администрация и управление, включващ системи за мониторинг и администриране на сървъри, процедури за актуализация на инсталирания системен и приложен софтуер, методи за контрол на системните промени, процедури за архивиране и възстановяване след бедствия и аварии, планове за непрекъсваемост на услугите и други (disaster recovery and contingency planning).

**Дейност 2: Ежедневно (day-to-day) оперативно наблюдение и поддържане функционирането на инфраструктурната среда на поддържаните системи**

Изпълнителят отговаря за интегритета, непрекъсваемостта, сигурността и достъпността на инфраструктурата. Той трябва да обхване всички дейности, включващи оперативно ежедневно (day-to-day) наблюдение на функционирането на ИТ инфраструктурата.

За осъществяване на своите задължения изпълнителят следва да поддържа непосредствен контакт с възложителя, да участва в координацията на експертно ниво на дейности, свързани с доставчиците на съществуващите системи и приложения, интегрирани в инфраструктурната среда, и комуникационна свързаност.

Изпълнителят предлага процедура за генериране на отчети и разпространение на информацията.

Изпълнителят е длъжен своевременно да уведоми Възложителя за възникнали неизправности чрез отварянето на сервизна заявка, включваща подробно описание на възникналия проблем, приоритета и влиянието, което той оказва върху комплекса от инфраструктурна среда и системи, както и оценка на необходимостта от ескалация към производителя/доставчика на съответния дефектирал компонент. Изпълнителят получава инструкции от възложителя за по-нататъшни действия и оказва съдействие на изпълнителските екипи на трети страни - доставчици на продукти и услуги, свързани с поддържаната ИТ инфраструктура.

За целите на настоящата поръчка взаимодействията с екипите на трети страни - външни доставчици на компоненти и услуги, по силата на вече съществуващи договори, се координират и контролират от възложителя.

**Дейност 3: Ежедневно оперативно наблюдение и поддържане функционирането на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС.**

- Създаване и поддържане на база данни за всички възникнали проблеми в работата на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС с оглед постоянно проследяване качеството на изпълняваната работа и последващо оценяване. Регистрира всички заявки в собствена

система за управление на инциденти и заявки, разполагаща с модул за измерване на ниво на обслужване;

- Предоставяне на интерфейс към система на изпълнителя, чрез която МТИТС наблюдава и следи статуса на обработваните от изпълнителя заявки;
- Уведомяване за възникнали неизправности чрез отварянето на заявка, включваща подробно описание на възникналия проблем, приоритета и влиянието, което той оказва върху работоспособността на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС, както и оценка на необходимостта от ескалация към производителя/доставчика на съответния дефектирал компонент, част от хардуерната инфраструктура, върху която е изградена ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС.
- Извършване на необходимите действия за възстановяване работата на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС при отпадане на приложенията в основния сайт.
- Извършване на необходимите действия за възстановяване работата на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС при отпадане на основния сайт.

**Дейност 4: Техническа поддръжка на наличното хардуерно оборудване**

- Поддръжка на наличното хардуерно оборудване съгласно приложена спецификация.
- Инсталиране, конфигуриране и тестване на нови и ремонтирани компоненти и продукти. Дейността се извършва самостоятелно или при необходимост - съвместно с трети страни, като съвместните действия с трети страни се координират от възложителя. Инсталирането на нови компоненти се извършва след предоставено от изпълнителя и утвърдено от възложителя становище за съвместимостта на хардуера с останалите компоненти на средата, както и за всички допълнителни компоненти (предоставяни от възложителя) на конфигурацията за осигуряване нормалното присъединяване към съществуващата инфраструктурна среда.
- Извършване на преконфигурации при инциденти, както и с оглед подобряване на достъпността, надеждността и производителността, адаптиране към промени в средата или добавяне на нови компоненти. Дейността се извършва самостоятелно или при необходимост - съвместно с трети страни, като съвместните действия с трети страни се координират от възложителя;
- Непрекъснат мониторинг на функционирането, достъпността и производителността на всички компоненти на техническата инфраструктура. Извършване на диагностика.

**Дейност 5: Експлоатационна поддръжка на софтуерни компоненти на инфраструктурната среда - базов софтуер, ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС**

- Експлоатационна поддръжка на съществуващия системен софтуер в състава на инфраструктурната среда
- Инсталиране, настройки и конфигуриране и тестване на нови или усъвършенствани продукти (базов софтуер) или такива след инцидент при предоставени от възложителя софтуерни лицензи и/или актуализирани версии на продуктите. Инсталирането на нови компоненти се извършва след предоставено от изпълнителя и утвърдено от възложителя становище за съвместимостта на софтуера с останалите компоненти на

средата, както и за всички допълнителни компоненти на конфигурацията за осигуряване нормалното присъединяване към съществуващата инфраструктура;

- Извършване на настройки, преинсталиране и промяна на софтуерни конфигурации при инциденти или с оглед подобряване на производителността, адаптиране към промени в средата или добавяне на нови компоненти;
- Непрекъснат контрол на функционирането и производителността;
- Зареждане на промени в софтуера с цел коригиране на грешки и/или дефекти в софтуера (бъгове), за подобряване на производителността му или други негови параметри и за адаптиране към промени в обкръжението му**;**
- Надграждане и администриране на секцията в ЕПДЕАУ за изтегляне на съдържание (download section).

**Дейност 6: Осигуряване на надеждна и непрекъсната работа на потребителите, дефинирани като активни в инфраструктурната среда**

- Поддържане на профилите за достъп на потребителите до ИТ инфраструктурата на системно ниво.
- Създаване на нови потребителски профили за достъп до ИТ инфраструктурата на системно ниво съгласно утвърдена процедура съгласувана с възложителя.

**Дейност 7: Осигуряване на надеждна и непрекъсната работа на потребителите (администрациите), дефинирани като активни в ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС.**

- Поддържане на профилите за достъп на потребителите до ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС;
- Създаване на нови потребителски профили за достъп до ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС съгласно утвърдена процедура, съгласувана с МТИТС;
- Осигуряване на консултативно съдействие на трети лица при реализиране на техническата готовност на техните АИС за свързване с ЕСОЕД-ESB и ИС по утвърдена процедура, съгласувана с възложителя, съгласно следната документация и приложения:
    - Наредба за изискванията към Единната среда за обмен на електронни документи(обн. ДВ, бр. 62 от 2008 г., изм., бр. 58 от 2010 г.);
    - Ръководство за инсталация и използване на комуникационния клиент;
    - Инсталационен пакет на комуникационния клиент;
    - Спецификация на интерфейс между информационните системи на участниците в обмена и комуникационния клиент.
- Идентифициране и отстраняване на възникнали проблеми при работата на ЕСОЕД-ESB в предварително дефинирани срокове и времена за реакция, докладвани от потребителите на ЕСОЕД-ESB.
- Идентифициране и отстраняване на възникнали проблеми при работата на ЕПДЕАУ в предварително дефинирани срокове и времена за реакция, докладвани от потребителите на ЕПДЕАУ.
- Идентифициране и отстраняване на възникнали проблеми при работата на ИС на РОС в предварително дефинирани срокове и времена за реакция, докладвани от потребителите на ИС на РОС.

**Дейност 8. Техническа поддръжка за разработчици и администратори на АИС и ЕАУ:**

Изпълнителят следва да организира и реализира второ ниво на техническа поддръжка за разработчици на електронни административни услуги (ЕАУ) и АИС по въпроси, свързани с взаимодействието на техните системи и предоставяните услуги с ЕПДЕАУ.

*Поддейности:*

- Техническа поддръжка по телефона по схема 8x5 за разработчици на АИС и електронни административни услуги (ЕАУ);
- Публикуване на ЕАУ, в съответствие с изискванията за Разработване и публикуване на ЕАУ в ЕПДЕАУ. Всички изисквания в тази насока могат да бъдат намерени напълно безплатно на страницата на Министерството на транспорта, информационните технологии и съобщенията, раздел „Електронно управление“, профил „Документи и процедури”;
- Публикуване на статично съдържание: новини, връзки, често задавани въпроси
- Публикуване на информационно съдържание: описания на административни услуги.

**Дейност 9. Техническа поддръжка за крайни потребители (граждани и бизнес):**

- Техническа поддръжка по телефона (help desk) по схема минимум 24x7 (24часа, 7 дни в седмицата) за крайни потребители на ЕПДЕАУ – граждани и бизнес организации;
- Регистриране на клиентските обаждания и възникналите неизправности чрез отварянето на сервизна заявка, включваща подробно описание на възникналия проблем, приоритета и влиянието му, както и оценка на необходимостта от ескалация към трети страни.
- Класификация на регистрираните неизправности и пренасочване за изпълнение на сервизната заявка към трети страни, доставчици на услуги и компоненти, част от интеграционната платформа на БеУ (ЕСОЕД-ESB, РОС, хардуерните компоненти и системите в КТЦЕП)
- Създаване и поддържане на база данни за всички възникнали проблеми при работата на крайни потребители с ЕПДЕАУ, с оглед постоянно проследяване качеството на изпълняваната работа и последващо оценяване.

**Дейност 10: Информационно осигуряване: управление и съхранение на данните**

- Периодично репликиране и архивиране (backup) на данните от системите за съхранение на информация, конфигурационни данни на ИТ инфраструктурата на БЕУ, във всеки един от центровете.
- Периодично репликиране и архивиране (backup) (ежедневно, седмично, месечно, тримесечно и годишно) на данните от системите за съхранение на информация, конфигурационни данни на ЕПДЕАУ, във всеки един от центровете на БеУ;
- Периодично репликиране и архивиране (backup) (ежедневно, седмично, месечно, тримесечно и годишно) на данните от системите за съхранение на информация, конфигурационни данни на ЕСОЕД-ESB, във всеки един от центровете на БеУ;

- Периодично репликиране и архивиране (backup) (ежедневно, седмично, месечно, тримесечно и годишно) на данните от системите за съхранение на информация, конфигурационни данни на ИС на РОС, във всеки един от центровете на БеУ;
- Възстановяване на информация и конфигурационни данни след срив (Recovery);
- Поддържане, анализ и архивиране на статистически файлове (напр. System и Security Logs) на системния софтуер.
- Наблюдение на запълването и консистентност на данните в системите за съхранение на информация и предприемане на необходимите действия, вкл. уведомяване на екипа на възложителя при необходимост;
- Администриране на дисковото пространство на системите за съхранение на информация с цел оптималното му използване.

**Дейност 11: Осигуряване на инфраструктурна поддръжка на наличните локални компютърни мрежи и връзки (LAN), включително всички пасивни и активни компоненти на мрежите:**

- Администриране и поддръжка;
- Действия при аварийни ситуации съгласно дефинираните параметри за ниво на обслужване;
- Текущ мониторинг на функционирането, наблюдение на натоварването, предложения за оптимизация. Извършване на диагностика;
- Извършване на преконфигурации при инциденти или с оглед подобряване на производителността, адаптиране към промени в средата или добавяне на нови компоненти.

**Дейност 12: Гарантиране на информационна сигурност на инфраструктурната среда:**

С Постановление № 181 на Министерския съвет от 20 юли 2009 г. (обн. ДВ. бр.59 от 28 Юли 2009 г.) са определени стратегическите обекти и дейности, които са от значение за националната сигурност на Република България и които са част от критичната инфраструктура. Съгласно Приложение – Списък на стратегическите обекти и дейности от значение за националната сигурност, раздел VII - Сектор „Телекомуникации и информация", т. 2.6., контроленият техническият център на БеУ в комплекс „Бояна", дом 3 е определен като стратегически обект от значение за националната сигурност.

Изпълнителят следва да изготви вътрешни правила за оценка и управление на риска за мрежова и информационна сигурност на системите в обхвата на двата центъра.

Препоръчителните действия по оценка и управление на риска трябва да съответстват на Приложение № 3 към чл. 31, ал. 2 от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност Потенциалните рискови фактори за мрежовата и информационната сигурност, формулирани и класифицирани в международния стандарт ISO/IEC TR 13335:2000, са посочени в Приложение № 4 към чл. 31, ал. 3 от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.

Управлението на сигурността да се осъществява на база на съществуващите решения: Защитна стена (Firewall), IDS/IPS, IPSec VPN и реорганизиране на системата за защита на

електронна поща и системата за защита на информацията от злонамерени атаки, с цел осигуряване на функционалности съгласно следните изисквания:

**Реорганизация на системата за защита на информацията от злонамерени атаки:**
**След приключване на реорганизацията следва да бъдат покрити следните изисквания:**

- Системата да осигурява защита чрез:
  - ✓ антивирус;
  - ✓ защита от шпионски и рекламен софтуер;
  - ✓ защитна стена и защита от атаки (host IPS);
  - ✓ контрол на устройствата;
  - ✓ URL филтриране и отчети;
  - ✓ NAC (контрол на мрежовия достъп);
  - ✓ контрол на извършваните системни конфигурации;
  - ✓ сканиране на мрежата за външни, неоторизирани устройства (rogue detection).
- Дистрибуцията на различните функции да се осъществява централизирано през конзола за управление през единствен клиентски агент;
- Да поддържа инсталация във фонов режим (silent mode installation);
- Системата трябва да извлича информация от глобална база данни с дефиниции, с оглед предпазването на клиентските компютри и сървъри от нови и видоизменящи се заплахи;
- Да има функционалност за централизирано, автоматично обновяване на антивирусните и host IPS дефинициите, както и на сканиращото ядро на продукта. Компонентите за обновяване трябва да могат да се дистрибутират от централизиран сървър към работни станции, които не са свързани с Интернет.
- Да има възможност за инкрементални обновявания, които са по-малки от 500 KB;
- Да сканира във фонов режим;
- Да може да сканира при достъп или поискване (on access и on demand сканиране)
- Да се интегрира с Active Directory спрямо потребителско име или група по отношение налагането на политики. Потребителските имена трябва да се виждат в отчетите на системата;
- Да е съвместима с операционни системи Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows Server 2000/2003/2008;
- Да предлага централизирано управление и наблюдение на всички звена от защитата;
- Централизираната конзола за управление да поддържа методи за автентификация – локална, сертификати, MS Active Directory;
- Централизираната конзола за управление да поддържа конфигуриране на административни роли с различни нива на достъп;
- Централизираната конзола за управление да се свързва със системата за защита на електронна поща, да може да я управлява и да дава отчети за нея;
- Централизираната конзола за управление трябва да може да управлява и наблюдава в реално време работата на системата за сигурност за работни станции независимо от местоположението им.

**Задължителни функции: Антивирус, AntiSpyware, URL филтрация, NAC:**

- Проактивна защита от нови заплахи с помощта на евристичен модул за засичане;
- Защита от нови заплахи с помощта на облачна система за репутация в рамките на по-малко от 24 часа от регистриране на заплахата (zero day protection);
- Облачната система за репутация трябва да поддържа тази функционалност за IP, website, file;
- Възможност за контролиране за постигане на оптимално ниво на погрешно засечени файлове като заплахи (false positives);
- Да може да блокира опити за инсталиране на приложения, да наблюдава записването и стартирането на програми в директории Windows, Program Files, Temp.
- Да може да сканира вложени архивни файлове;
- Използване на multi-thread технология и оптимизация за многоядрени системи;
- Системата трябва да може да определя нивото на риск на всеки сканиран файл, чрез изследване на следните файлови характеристики и съдържание:
  - ✓ Източник на файла
  - ✓ Колко нов е файла
  - ✓ Колко често се наблюдавава файла в Интернет
- Да може да се извършва URL филтриране чрез бели\черни списъци и категории сайтове. Да поддържа над 95 категории. Да поддържа Internet Explorer, Mozilla Firefox, Chrome;
- Да предлага възможност за отчети за посетени сайтове на база потребители от MS Active Directory, часове, категории;
- Да може да ограничава достъпа на работна станция в зависимост от потребителско име, инсталиран софтуер, версия и софтуерни обновления.
- В ежедневната си работа Антивирус функционалността да не използва повече от 100 MB RAM при сканиране;
- Антивирус системата да е одобрена от Microsoft за работа с MS операционни системи;

**Задължителни функции: Host IPS:**

- Проактивна защита от атаки (host IPS);
- Защита на операционната система от уязвимости преди инсталиране на update (host IPS);
- Защита от нови заплахи с помощта на облачна система за репутация в рамките на по-малко от 24 часа от регистриране на заплахата (zero day protection);
- Да разполага с интегриран персонален statefull Firewall;

**Задължителни функции за контрол на устройствата:**

- Да може да контролира периферни устройства в това число флаш памети, външни дискове и други носители на данни, COM/Serial порт, Bluetooth, Firewire, CD/DVD като ги забранява, ограничава работата им или само наблюдава използването в зависимост от потребителско име ли група в MS Active Directory или в зависимост от ID и производител. Не трябва да се засяга работата с налични USB клавиатури, мишки и периферия.

**Задължителни функции наблюдение и отчети:**

- Възможност за създаване на отчети, подробни и сумарни, за събитията в мрежата (брой сканирани файлове, брой вируси, брой защитени/незащитени станции, станции с най-много вируси и т.н.)
- Изпращане на известия (email, SNMP trap) или предприемане на действия при възникване на предварително дефинирани събития (откриване на вируси, обновяване на дефиниции и др.);
- Отчетите трябва да са налични като минимум в следните формати: XML, HTML, CSV и PDF.
- Да разполага с поддръжка на планово генериране на отчети;

**Системата за защита на електронна поща трябва да отговаря на следните изисквания:**

- Защита на минимум 2500 електронни пощенски кутии;
- Да поддържа минимум 50 домейна;
- Предложената система за защита на електронна поща трябва да поддържа работа във виртуална среда като ESX virtual appliance;
- Да поддържа MS Exchange 2003, 2007 и 2010;
- Да има обща централизирана конзола за управление и наблюдение заедно със системата за защита на информацията от злонамерени атаки;
- Да защитава от DoS/DDos (Denial of service/Distributed Denial of service) атаки пощенските сървъри с функции на ядрото на операционната система (Kernel Block);
- Да защитава от harvest, DoS атаки;
- Да защитава от спам, фишинг, spyware, malware, вируси и червеи;
- Да може да сканира архиви;
- Да използва технологии за предпазване от SPAM: облачна система за репутация, grey listing, RBL, SPF, BATV, DKIM, разпознаване на изображения;
- При избор за инсталация на повече от едно устройства за защита на електронна поща да има централизирана и обща карантина;
- Централизираната карантина да не изисква закупуване на нова операционна система, база данни или хардуер;
- Централизираната карантина трябва да предлага на всеки индивидуален потребител: портал за освобождаване на погрешно заподозрян спам, портал за въвеждане на бели и черни списъци;
- Централизираната карантина трябва да може да се локализира и изпращаните към потребителите съобщенията да са на български език;
- Преконфигурирането на системата за защита на електронна поща за филтриране на SMTP мейл трафик от вируси и спам не трябва да включва доставка на нов хардуер.
- Преконфигурираната система проверява e-mail трафика в изходяща посока (от вътрешни потребители към Интернет)
- Да предлага виртуализация. Например – за нов домейн или група да може да се използва отделен административен интерфейс, с нов IP за приемане и изпращане на поща с цел сегментиране на email трафика и с цел различни отдели да могат да управляват само собствения си email трафик;

- Да има функции DLP – да може да се обучава за конфиденциално съдържание (да прави сигнатури за конфиденциални файлове и да използва регулярни изрази), да открива конфиденциални документи в email трафика и да блокира изпращането им;
- Да има функции Compliance – да може да проверява email трафика за изпълнение на международни стандарти и правила;
- Да използва LDAP за проверка на потребители и рутиране на email съобщения;
- Да притежава средства за подробен отчет и справки за случилото се (резултати от уловения спам в проценти, по дни и т.н.);
- Да притежава средства за отчетност, които да позволяват анализ на получените съобщения – час, дата, изпращач, получател, IP на сървър, използвани филтри за обработка на съобщението и т.н.;
- Да поддържа TLS, PGP, S/MIME;
- Да разполага с Web портал за криптирано доставяне на съобщения;
- Да може да работи в режим на резервираност (Clustering);
- Да поддържа централизирано управление на резервирания Cluster без нужда от допълнителен хардуер;

Изпълнителят следва да:

• Осъществява наблюдение и системен анализ на работата с цел предприемане на проактивни мерки за повишаване на защитата чрез системата за управление и наблюдение и актуализираните технологични решения за информационна сигурност;

• Контролира поддържаните системи с цел недопускане на неправомерен достъп до тях;

• Извършва наблюдение и оценка на мрежовата среда, с цел предприемане на проактивни мерки за повишаване на защитата и бързодействието й;

• Наблюдава непрекъснато състоянието на дисковите подсистеми.

• Осъществява непрекъснат контрол, предприема адекватни действия и своевременно писмено известява Възложителя при:

a. Неоторизирано прочитане или копиране или изнасяне на информация в електронен вид, вкл. неоторизиран достъп до информационни потоци, кражба на потребителски имена, пароли и друга поверителна информация;

b. Неоторизирано записване на данни и информация или унищожаване на такава в подсистема към системата, включително проникване на вируси;

c. Отказ или блокиране на устройства и ресурси (Интернет, мрежови ресурси, дисково пространство, памет и др.) поради пробив в системата, претоварване на връзките и т. н.

• Инсталира, конфигурира и тества ремонтираните компоненти и продукти в контекста на изискванията за гарантиране на информационната сигурност.

На изпълнителя ще бъде предоставена експлоатационната документация на всички системи за организиране на информационната сигурност на инфраструктурната среда.

**Дейност 13: Гарантиране на информационна сигурност на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС.**

- Изготвяне на вътрешни правила за оценка и управление на риска за мрежова и информационна сигурност на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС в обхвата на центровете на е-правителството;

- Управлението на сигурността на база на доставени и внедрени решения в центровете на е-правителството;
- Наблюдение и системен анализ на работата с цел предприемане на проактивни мерки за повишаване на защитата чрез системата за управление и наблюдение и съществуващите технологични решения за информационна сигурност;
- Контролиране на поддържаните модули на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС с цел недопускане на неправомерен достъп до тях;
- Извършване на наблюдение и системен анализ на работата на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС с цел предприемане на проактивни мерки за повишаване на защитата и бързодействието й;
- Съхраняване на архивните копия в съответствие със съществуващите разпоредби за съхранение на архивите, като се имат предвид и специфичните изисквания към конкретните носители на информацията;
- Осъществяване на непрекъснат контрол, предприемане на адекватни действия и своевременно писмено известяване на МТИТС при:
    - ✓ Неоторизирано прочитане или копиране или изнасяне на информация в електронен вид, вкл. неоторизиран достъп до информационни потоци, кражба на потребителски имена, пароли и друга поверителна информация;
    - ✓ Неоторизирано записване на данни и информация или унищожаване на такава в ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС, включително проникване на вируси;
    - ✓ Отказ или блокиране на приложния софтуер поради пробив в системата, претоварване на връзките и т. н.
- Инсталиране, конфигуриране и тестване на нови версии на приложния софтуер в контекста на изискванията за гарантиране на информационната сигурност;
- Изготвяне на процедури за работа при аварии, произшествия и бедствия. В тези процедури се описва редът за възстановяване на данните и работоспособността на поддържаните система.

**Дейност 14: Администриране и поддръжка на информационно съдържание. Администриране на процеса на управление на промените.**

- **Оптимизиране на технологичната среда с оглед оптимално използване на съществуващите хардуерни ресурси;**
- **Оказване на системна помощ на потребителите на специализираните приложни системи.**
- **Администриране на Процес по управление на промените (Change Management)**

Основната цел на управлението на промените е предотвратяване или оценяване, надлежно отразяване и получаване на необходимите одобрения за изпълнението на промените в рамките на организацията. Процесът по управление на промените описва следните дейности:

- ✓ Регистрация и оценка на искането за промяна;
- ✓ Класификация на промяната
- ✓ Оценка на влиянието и ресурси (приоритети и степен на въздействие)
- ✓ Съгласуване и одобряване на промяната
- ✓ Планиране на промяната

- ✓ Създаване, тестване и внедряване
- ✓ Оценка на промяната (потвърждаване на резултата)

- **Дейности по експлоатация и оперативна поддръжка на „Система за удостоверителни услуги (PKI)**

- ✓ Ресурсно обезпечение на Услуги по експлоатация и оперативна поддръжка:
- ✓ Конфигуриране на политиките на издаване на удостоверения, (Удостоверяващия орган, удостоверенията на междинните и оперативни органи от PKI инфраструктурата)
- ✓ Техническо съпровождане на управлението на политиките на видовете удостоверения за крайни потребители, които се издават от удостоверяващия орган;
- ✓ Техническо съпровождане на управлението на политика на дистрибутиране на списъците със спрени и прекратени удостоверения (публично или вътрешно дистрибутиране)
- ✓ Технически съпровод на дейностите по генериране и управление на криптографските ключове и на удостоверенията на удостоверяващия орган;
- ✓ Технически съпровод на дейностите по издаване/управление на удостоверения за крайни потребители и информационни системи
- ✓ Система за единно време
- ✓ Резервен PKI
- ✓ PKI crc

**Дейност 15: Наблюдение и оценка на достъпността на ИТ услугите в състава на БЕУ, в съответствие с изискванията на най-добрите ИТ практики: Information Technology Infrastructure Library (ITIL) по отношение процесите за управление на капацитета и достъпността на услугите (Capacity and Availability management)**

С цел да се осигури автоматизирано, централизирано, проактивно наблюдение и управление на достъпността на ИТ ресурсите в мрежата за предаване на данни на МТИТС, да се минимизира времето за реакция и отстраняване на проблеми, както и да се подпомогне достигането на висока степен на сигурност, надеждност, достъпност и работоспособност на всички автоматизирани информационни системи и приложения, съществуващата Система за централизирано управление и наблюдение на ИТ ресурсите на интеграционната система на БеУ и свързаните с него обекти следва да бъде преконфигурирана, в съответствие със следните изисквания:

- Преконфигурацията да бъде извършена в пълно съответствие с изискванията на Information Technology Infrastructure Library (ITIL), като се включат и възможности за поетапно бъдещо развитие;
- Наблюдението на достъпността на ИТ ресурсите и текущите услуги да се извършва без използването на софтуерни агенти, инсталирани върху наблюдаваните хостове (agentless monitoring)
- Системата да бъде оразмерена за наблюдение на най-малко 100 точки без използването на агенти.
- Да предоставя уеб интерфейс за наблюдение и администрация.
- Да поддържа следните протоколи за отдалечен достъп до наблюдаваните хостове:

TELNET, rlogin, HTTP, SSH, NetBIOS и WMI

- Да предоставя възможност за наблюдение на DNS услугата чрез симулиране на DNS заявки;
- Да предоставя възможност за наблюдение на DHCP услугата чрез симулиране на DHCP заявки;
- Да проверява за наличието на достъп до web приложения, чрез HTTP заявки ;
- При регистриране на инцидент да може да изпраща нотификация чрез email, SNMP Trap и HTTP post
- Да поддържа интеграция с Active Directory
- Да предоставя SOAP базиран програмен интерфейс за разширения
- Да позволява изпълняването на предварително записани стъпки симулиращи потребителско поведение спрямо различни DHTML, JavaScript, XML, SSL и др. приложения
- Да съдържа компонент за управление и наблюдение на хетерогенни ИТ системи: сървъри и приложения, и съхраняване и обработване на информацията събирана от тях.
- Да съдържа компонент за управление и наблюдение на мрежови устройства, и съхраняване и обработване на информацията събирана от тях.
- Да съдържа предефинирани средства за наблюдение и управление на инсталираните и функциониращи в МТИТС сървъри и работещите на тях операционни системи, системи за управление на бази данни и различните приложения;
- Да поддържа на SNMP v3 протокол;
- Да поддържа SNMP traps;
- Да разполага с поддръжка на security eventlog в MS Windows операционна система;
- Системата трябва да разполага с поддръжка за наблюдение на състоянието на хардуера на сървърите през операционната система или вградена мениджмънт карта;
- Системата трябва да предоставя средство за наблюдение на статуса на услугите (services) в MS Windows операционна система.
- Да предоставя средство за статистики на мрежовата подсистема (пакети, трафик, грешки)
- Да предоставя средство за наблюдение на NT броячите за производителност (performance counter);
- Да предоставя средство за наблюдение на натоварването и използването на паметта;
- Да предоставя средство за наблюдението на натоварването на процесорите;
- Да предоставя средство за наблюдение на натоварването на дисковете;
- Да предоставя средства за наблюдение на виртуализационни среда.

При преконфигурирането на системата следва да се имат предвид и да се запазят характеристиките на съществуващите съставни модули, като осигурените, съгласно горепосочените изисквания функционалности за наблюдение на достъпността на ИТ ресурсите и услугите, следва да се интегрират с наличните към момента.

Изпълнителят следва да реализира еднократната услуга по преконфигуриране на съществуващата Система за централизирано управление и наблюдение на ИТ ресурсите на

интеграционната система на БеУ и свързаните с него обекти, с цел осигуряване наблюдение и оценка на достъпността на услугите.

**Дейност 16: Оценка на капацитета на сървърната инфраструктура, и достъпността на услугите**

След приключването на Дейностите 14 и 15, Изпълнителят следва да извърши анализ и оценка на капацитета на наличните ИТ ресурси и достъпността на текущите услуги, като използва средствата на:

- Наличната в състава на инфраструктурната среда Система за централизирано управление и наблюдение на ИТ ресурсите на интеграционната система на БеУ и свързаните с него обекти, и, по-конкретно, нейните модули, даващи информация за наличните информационни активи и текущото състояние на хардуерното и комуникационно оборудване: HP OpenView Operations, HP OpenView Network Node Manager Advanced Edition, HP OpenView Performance Manager, HP Open View Performance Insight, HP Discovery and Dependency Mapping Inventory, HP Site Scope;
- Решенията за наблюдение на достъпността на наличните услуги, съответстващи на изискванията на възложителя (описани в Дейност 15)
- Експертната оценка на ключовите специалисти в екипа на изпълнителя, притежаващи необходимата квалификация и познания в областта на съществуващите решения в обхвата на инфраструктурата на системите на БеУ, съгласно изискванията на възложителя, посочени в условията за участие.

Участникът следва да представи алгоритъм/процеси за оценка и управление на капацитета и достъпността на услугите (Capacity&Availability Management), разработени в съответствие с най-добрите ИТ практики и да покаже тяхната интеграция с Процес за управление на инцидентите (Incident Management) и Процес за управление на промените и конфигурациите (Change Management/Configuration Management), заложени в стандартите за най-добри ИТ практики - Information Technology Infrastructure Library (ITIL).

Изпълнителят трябва да представи доклад от анализа и оценка на капацитета на наличните ИТ ресурси и достъпността на текущите услуги.

## III.Технически изисквания към изпълнителя. Ресурсна обезпеченост

### 1. Параметри на комплексната поддръжка и основни изисквания

- Всички дейности по хардуерната поддръжка се извършват изцяло от изпълнителя, като стойността на всички резервни части, труд и транспорт е за сметка на изпълнителя.
- Участникът трябва да представи схема за сервизните процеси и отговорностите по поддръжката на оборудването.
- Отчитането на сервизната дейност следва да се осъществява чрез изготвяне на протоколи за извършената работа, които се подписват от упълномощени от възложителя в отделните центрове лица и от съответните сервизни инженери. Тези протоколи се включват в писмените месечни отчети, които се подписват от оторизираните от МТИТС лица и от ръководителя на сервизната организация.
- Изпълнителят следва да създаде и поддържа база данни за всички технически устройства, постъпили за ремонт при него, с оглед постоянно проследяване качеството на

ремонтираните устройства и оценяване на работата му. Изпълнителят трябва да регистрира всички заявки в собствена система за управление на инциденти и заявки, разполагаща с модул за измерване на ниво на обслужване (SLA - Service Level Agreement).

Изпълнителят трябва да предостави интерфейс към своята система, чрез който възложителя наблюдава и следи статуса на обработваните от изпълнителя заявки.

- Участникът следва да предложи детайлен план за реализиране на дейността си по експлоатационното поддържане на инфраструктурната среда, както и детайлно описание на методика за оценка на състоянието на системите в обхвата на двата центъра и отстраняването на повреди.
- Изпълнителят следва да предостави описание на методиката за диагностициране на възникнали проблеми, профилактика, превантивни действия и други свързани с дейността спомагателни процеси.
- Параметрите на качеството на обслужване по поддръжка на хардуерните системи, които следва да се осигурят от изпълнителя, и не трябва да са по-ниски от дадените в Таблица № 1:

Таблица № 1.

| **Параметър** | **Обект на БЕУ / Местоположение** | **Параметри на обслужването** |
|---|---|---|
| **Режим на поддържане** | КТЦЕП „Бояна” | Непрекъснат режим (24x7) 365 дни в годината |
| | ТЦЕП „Евксиноград” – Варна | Непрекъснат режим (24x7) 365 дни в годината |
| **Време за реакция (ч) (макс)** | КТЦЕП „Бояна” | 30 минути от подаване на заявката |
| | ТЦЕП „Евксиноград” – Варна | 30 минути от подаване на заявката |
| **Време за отстраняване на повредата (ч) (макс)** | КТЦЕП „Бояна” | 8 часа от подаване на заявката |
| | ТЦЕП „Евксиноград” – Варна | 16 часа от подаване на заявката |

***Забележки:***

- ✓ Работно време е периодът от 00.00 ч. до 24.00 ч. - всеки ден от седмицата, 365 дни в годината.
- ✓ Времето за реакция се отчита от момента на съобщаване до момента на потвърждаване регистрирането на повредата от Изпълнителя през определена в договора точка за контакт.
- ✓ Времето за отстраняване на повредата се отчита от момента на потвърждаването на приемането й до момента на възстановяване на нормалната работоспособност на системите на БеУ чрез ремонт на повреденото устройство или осигуряване и

включване на оборотно устройство със същите или по-високи технически характеристики.

- ✓ Поддръжката на устройствата и специфичните конфигурации се извършва „на място” (on site).

- Всички дейности по софтуерната поддръжка на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС се извършват изцяло от изпълнителя.
- Участникът трябва да представи схема за работните процеси и отговорностите по поддръжката на приложния софтуер.
- Отчитането на дейността по поддръжката на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС следва да се осъществява чрез изготвяне на протоколи за извършената работа, които се подписват от упълномощени от възложителя в отделните контролни центрове лица и от съответните отговорни лица от страна на изпълнителя. На база на тези протоколи се изготвят приемо-предавателни протоколи за приемане на работата на изпълнителя за съответния период, които се подписват от оторизираните от МТИТС лица и от ръководителя от страна на изпълнителя.
- Изпълнителят следва да създаде и поддържа база данни за всички възникнали проблеми в работата на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС, с оглед постоянно проследяване качеството на изпълнената работа и оценяване. Изпълнителят трябва да регистрира всички заявки в собствена система за управление на инциденти и заявки, разполагаща с модул за измерване на ниво на обслужване. Изпълнителят трябва да предостави интерфейс към своята система, чрез който възложителя наблюдава и следи статуса на обработваните от изпълнителя заявки.
- Участникът следва да предложи детайлен план за реализиране на дейността си по експлоатационното поддържане на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС, както и детайлно описание на методика за оценка на състоянието на средата в обхвата на двата центъра и отстраняването на възникнали проблеми.
- Параметрите на качеството на обслужване на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС, които следва да се осигурят от изпълнителя, не трябва да са по-ниски от дадените в Таблица № 2:

Таблица № 2

| **Параметър** | **Обект / Местоположение** | **Параметри на обслужването** |
|---|---|---|
| **Режим на Поддържане** | ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС в КТЦЕП „Бояна” | Непрекъснат режим (24x7) 365 дни в годината |
| | ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС в ТЦЕП „Евксиноград” - Варна | Непрекъснат режим (24x7) 365 дни в годината |
| **Максимално време за реакция (ч) в зависимост от приоритизацията на проблема** | ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС в КТЦЕП „Бояна” | Приоритет 1 – до 30 мин от подаване на заявката<br>Приоритет 2 – до 2 часа<br>Приоритет 3 – до 8 часа |
| | ЕПДЕАУ, ЕСОЕД-ESB и ИС на | Приоритет 1 – до 30 мин от |

| | | |
|---|---|---|
| | РОС в ТЦЕП „Евксиноград” - Варна | подаване на заявката<br>Приоритет 2 – до 2 часа<br>Приоритет 3 – до 8 часа |
| **Максимално време за отстраняване на проблема (ч) в зависимост от приоритизацията на проблема** | ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС в КТЦЕП „Бояна” | Приоритет 1 – до 4 часа от идентифициране на проблема<br>Приоритет 2 – до 12 часа от идентифициране на проблема<br>Приоритет 3 – до 24 часа от идентифициране на проблема |
| | ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС в ТЦЕП „Евксиноград” - Варна | Приоритет 1 – до 4 часа от идентифициране на проблема<br>Приоритет 2 – до 12 часа от идентифициране на проблема<br>Приоритет 3 – до 72 часа от идентифициране на проблема |

Приоритизацията на възникналите проблеми с приложния софтуер на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС се дефинират както следва:

- Проблеми с **приоритет 1** – Проблемът нарушава работоспособността на цялата ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС или изключително важна функция от нея.
- Проблеми с **приоритет 2** – Проблемът засяга отделна част или функция на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС и той може да бъде временно заобиколен.
- Проблеми с **приоритет 3** – Проблемът е несъществен и не нарушава нормалната работа на ЕПДЕАУ, ЕСОЕД-ESB и ИС на РОС, но за да не се задълбочи или да не затруднява излишно потребителите, е необходима корекция.

**2. Техническото поддържане от страна на изпълнителя трябва да покрие като минимум следните дейности, включени в процеса за управление на инцидентите (Incident Management):**

- ✓ Приемане и регистриране на съобщение за повреда;
- ✓ Определяне на приоритет за съответното повикване, в случай че са постъпили едновременно няколко заявки за ремонт;
- ✓ Консултации по телефона;
- ✓ Посещение на място;
- ✓ Попълване на сервизна карта;
- ✓ Транспорт от и до съответния КТЦЕП или ТЦЕП;
- ✓ Диагностика на повреденото устройство;
- ✓ Ремонт/възстановяване работоспособността на устройството;
- ✓ Тестване на технически устройства за работоспособност;
- ✓ Осигуряване на оборотна техника;
- ✓ Поддържане на картотека от сервизни карти;
- ✓ Изпращане при необходимост на дефектирали модули и устройства за ремонт в предварително уточнени специализирани сервизни бази в страната,
- ✓ Изпълнителят осигурява доставката на всички необходими части за подмяна

- ✓ Наблюдение на състоянието;
- ✓ Оценка на състоянието;
- ✓ Генериране на отчети;
- ✓ Разпространение на информация;

Експлоатационното осигуряване включва и поддръжка на електронния каталог на услугите в работоспособно състояние и всички дейности свързани с това като:

- Актуализация на съществуващия каталог на електронните услуги с писмено възлагане от възложителя.
- Всички дейности по експлоатационното осигуряване на инфраструктурната среда и интегрираните системи.
- Изпълнителят да следи и измерва постоянно (24 часа х 7 дни) наличността на услугите и състоянието на подсистемите, за което да предоставя ежемесечно отчети на възложителя.

Изпълнителят да използва наличните средства, предоставени от възложителя, за наблюдение на процесите и работата на услугите в инфраструктурната среда и интегрираните системи като регистрира и документира всяко събитие, което може да доведе до неработоспособност на електронните услуги. На базата на тези събития и данни се представят писмените отчети за извършени дейности.

**IV. Дейности по експлоатационно осигуряване и поддръжка на всеки от действащите КТЦЕП и ТЦЕП**

Във връзка с технологичното и експлоатационно обезпечаване на безпроблемната работа на всички системни компоненти в обхвата на двата центъра за високо качество на предоставяните услуги и предоставяне поддръжка в дълговременен аспект от високо квалифициран персонал с разпределени отговорности и с възможност за взаимно припокриване е необходимо:

- Да се изготви предложение включващо дефиниране, изграждане и/или надстройване на зони за сигурност и подсистема към система за контрол на достъпа до тях във всеки от действащите териториални центрове.
- Изпълнителят следва да разкрие и поддържа точки за контакт, снабдени със съответни съобщителни средства - телефон, e-mail и непрекъснат (365дни*24часа) режим на работа във всеки от действащите териториални центрове.

**1. Ресурсна обезпеченост на дейности по експлоатационно осигуряване и поддръжка 24х7 на КТЦЕП – Бояна**

Изпълнителят следва да изпълнява операторските си функции, така че да отговарят на дефинираните в Таблица 1 нива на обслужване:

- Изграждане на най-малко 4 (четири) работни места с длъжност „Оператор”, на сменен режим с действие 24х7 от специалисти за администриране и поддръжка на БЕУ в работоспособно състояние при зададеното ниво на обслужване (SLA). Работните места да са структурирани по начин, който гарантира бързо и точно получаване на необходимата информация за състоянието на поддържаните системи, интегрирани в инфраструктурната среда; откриване на потенциални заплахи с цел превенция; натоварване на системата; гарантиране на информационната сигурност; статистика и отчетност. Препоръчително е

структурирането на обособените работни места да е в съответствие с добрите европейски практики и стандарти.

Изпълнителят следва да предложи организационна схема на взаимодействие между обособените зони при инциденти.

• Обхвата на поддръжката да е съгласно приложените спецификации и описанието на системите.

• Едно постоянно работно място с длъжност „Супервайзор" с работен режим 8 часа дневно 5 дни в седмицата или 22 работни дни в месеца и на разположение при режим 24 часа х 7 дни

**2. Ресурсна обезпеченост на дейности по експлоатационно осигуряване и поддръжка 24х7 на ТЦЕП – Варна**

За осигуряване на непрекъснатото наблюдение на БЕУ в ТЦЕП „Евксиноград" в гр. Варна е необходимо следното:

- Изграждане на най-малко 2 (две) работни места, както следва:
  - ✓ Едно постоянно работно място с длъжност „Оператор", разположено в Център гр. Варна с 24 часа х 7 дни режим на работа за непрекъсваем мониторинг и администриране, оперативно подчинено на Център Бояна.
  - ✓ Едно постоянно работно място с длъжност „Супервайзор" с работен режим 8 часа дневно 5 дни в седмицата или 22 работни дни в месеца при 24 часа х 7 дни разположение оперативно подчинено на Център Бояна.

**V. Срок за изпълнение:** 24 (двадесет и четири) месеца от сключване на договора.

**VI. Налична инфраструктура в КТЦЕП – Бояна**

Таблица № 3

| Описание | Сериен номер |
|---|---|
| КТЦЕП - Бояна (гр. София) | |
| Сървърни системи | |
| HP ProLiant DL 580 (4x72GB Serial SCSI) | GB87108TCT |
| HP ProLiant DL 580 (4x72GB Serial SCSI) | GB87108TCO |
| HP ProLiant DL 580 (4x72GB Serial SCSI) | GB87108TDC |
| HP ProLiant DL 580 (2x72GB Serial SCSI) | GB87108TE5 |
| HP ProLiant DL 580 (4x72GB Serial SCSI) | GB87108TD5 |
| HP ProLiant DL 580 (8x72GB Serial SCSI) | GB87108TDP |
| HP ProLiant DL 580 (2x72GB Serial SCSI) | GB87108TC9 |
| HP ProLiant DL 380 G5 (4x72GB Serial SCSI) | CZC7103B1J |
| HP ProLiant DL 380 G5 (2x72GB Serial SCSI) | CZC7103B1C |

| Описание | Сериен номер |
|---|---|
| HP ProLiant DL 380 G5 (2x72GB Serial SCSI) | CZC7103BQW |
| HP ProLiant DL 380 G5 (8xl46GB SAS) | CZC8206T6J |
| HP ProLiant DL 380 G5 (8xl46GB SAS) | CZC8210JO3 |
| HP ProLiant DL 380 G5 (8xl46GB SAS) | CZC8206T6D |
| HP ProLiant DL 380 G5 (8xl46GB SAS) | CZC820716B |
| HP ProLiant DL 380 G5 (2xl46GB SAS) | CZC820716B |
| HP ProLiant DL 380 G5 (2xl46GB SAS) | CZC8206T65 |
| HP ProLiant DL 385 (2x300GB Ultra 320 SCSI) | GB8641PPL5 |
| HP ProLiant DL 385 (2x300GB Ultra 320 SCSI) | GB8641PPLP |
| HP Integrity rx4640 | DEH4641H47 |
| HP Integrity rx4640 | DEH4641H46 |
| HP Integrity rx2660 | DEH4731219 |
| HP Server rp 5470 | DEH4402S43 |
| HP Server rp 5470 | DEH4402S45 |
| HP Server rp 5470 | DEH4402S46 |
| HP ML350T03 | 7J33KT43H030 |
| NetHSM | |
| SyncServer s250 Networktime server | |
| MailGate Tumbleweed | |
| MailGate Tumbleweed | |
| IBM System x3650 (4x300 GB/15k SAS) | KDPNWMF |
| IBM System x3550 (2x73.4 GB/k SAS) | KDPMNAF |
| IBM System x3550 (2x73.4 GB/k SAS) | KDPMNPN |
| HP BLp Enclosure w/ 8 BMS Lie ALL | 801FMJS47H |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107HG |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107HP |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107HA |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107EB |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107HO |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107GU |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107HE |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107G9 |
| Cisco Gigabit Ethernet Switch Module p-class blade | |

| Описание | Сериен номер |
|---|---|
| Cisco Gigabit Ethernet Switch Module p-class blade | |
| HP BLp Enclosure w/ 8 BMS Lie ALL | 801EMJS47H |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107HR |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107H9 |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107HH |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107GC |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107GK |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107HD |
| Cisco Gigabit Ethernet Switch Module p-class blade | |
| Cisco Gigabit Ethernet Switch Module p-class blade | |
| HP BLp Enclosure w/ 8 BMS Lie ALL | 8003MJS484 |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ70404DM |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ73304JH |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ70404DP |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ733042E |
| Cisco Gigabit Ethernet Switch Module p-class blade | |
| Cisco Gigabit Ethernet Switch Module p-class blade | |
| HP BLp Enclosure w/ 8 BMS Lie ALL | 801DMJS47H |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107HC |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107EE |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107EL |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107H8 |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64008JN |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64007HJ |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107GX |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107GT |
| Cisco Gigabit Ethernet Switch Module p-class blade | |
| Cisco Gigabit Ethernet Switch Module p-class blade | |
| HP BLp Enclosure w/ 8 BMS Lie ALL | 801CMJS47H |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107GB |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107HM |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107GM |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64008K3 |

| Описание | Сериен номер |
|---|---|
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107HL |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107HN |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ64107EF |
| Cisco Gigabit Ethernet Switch Module p-class blade | |
| Cisco Gigabit Ethernet Switch Module p-class blade | |
| HP BLp Enclosure w/ 8 BMS Lie ALL | 8004MJS484 |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ70404DR |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ70404DN |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ70404DS |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ70404DT |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ70305AF |
| HP Bl 25p (2x72. 8Gb Ultra 320 SCSI) | CZJ70205ES |
| Cisco Gigabit Ethernet Switch Module p-class blade | |
| Cisco Gigabit Ethernet Switch Module p-class blade | |
| HP BLc7000 1 PH 2 PSU 4 Fan Full ICE Kit | GB8824RT85 |
| HP ProLiant BL460c GI | CZJ824078G |
| HP ProLiant BL460c GI | CZJ824078H |
| HP ProLiant BL460c GI | CZJ82409W9 |
| HP ProLiant BL460c GI | CZJ83005H5 |
| HP ProLiant BL460c GI | CZJ830052G |
| HP ProLiant BL460c GI | CZJ830052C |
| HP ProLiant BL460c GI | CZJ83005H3 |
| HP ProLiant BL460c GI | CZJ830052F |
| HP ProLiant BL460c GI | CZJ824078T |
| HP ProLiant BL460c GI | CZJ824078U |
| HP BLc Cisco IGbE 3020 Switch Opt Kit | FOC1215T07M |
| HP BLc Cisco IGbE 3020 Switch Opt Kit | FOC1215T080 |
| Cisco MDS 9124e 24 port Fabric Switch | JAF12122XY4 |
| Cisco MDS 9124e 24 port Fabric Switch | JAF1216478W |
| HP BLc7000 1 PH 2 PSU 4 Fan Full ICE Kit | GB8815K057 |
| HP ProLiant BL460c GI X5355 | CZJ81508BE |
| HP ProLiant BL460c GI X5355 | CZJ81602KA |

| Описание | Сериен номер |
|---|---|
| HP ProLiant BL460c GI X5355 | CZJ8150AMS |
| HP ProLiant BL460c GI X5355 | CZJ81504FG |
| HP ProLiant BL460c GI X5355 | CZJ81508B2 |
| HP ProLiant BL460c GI X5355 | CZJ8150AN1 |
| HP ProLiant BL460c GI X5355 | CZJ8150ANK |
| HP ProLiant BL460c GI X5355 | CZJ8150AMU |
| HP ProLiant BL460c GI X5355 | CZJ81602BY |
| HP ProLiant BL460c GI X5355 | CZJ81602BX |
| HP BLc Cisco IGbE 3020 Switch Opt Kit | FOC1207T13S |
| HP BLc Cisco IGbE 3020 Switch Opt Kit | FOC1207T13U |
| Cisco MDS 9124e 12 port Fabric Switch | 3C62091473 |
| Cisco MDS 9124e 12 port Fabric Switch | 3C62091537 |
| Дискови подсистеми | |
| HP EVA4000 2C4D | GB80641RAO |
| HP ProLiant DL 380 (2x36,4GB Ultra SCSI) | GB80641RA1 |
| HP Storage Works (14 x 300 GB Fiber channel) | SGM0634U90 |
| HP Storage Works (14 x 300 GB Fiber channel) | |
| HP Storage Works (14 x 300 GB Fiber channel) | |
| HP Storage Works (14 x 300 GB Fiber channel) | |
| Cisco MDS 92 16i | USJ037N3NO |
| MDS9000 32port l/2Gbps FC Module w/SFP's | USJ102972Z |
| EVA4100 2C3D | 2S28220R6D |
| HP Storage Works (14 x 300 GB Fiber Channel) | |
| HP Storage Works (14 x 300 GB Fiber Channel) | |
| HP Storage Works (14 x 300 GB Fiber Channel) | |
| HP Storage Works MSA70 (20xl46GB SAS) | |
| HP Storage Works MSA70 (20xl46GB SAS) | |
| HP Storage Works tapearray 5300 | SG03500353 |
| HP Storage Works MSL 6060 Series Library | USX63800AB |
| Tapedrive IBMTS2340 | |
| HP EVA4100 2C1D Array | 2S28140MES |
| HP M5314C FC Drive Enclosure 14xHP EVA 300G/10K FC Add-on Hard Disk Drv | SGM75014FR |

| Описание | Сериен номер |
|---|---|
| HP M5314C FC Drive Enclosure 28xHP EVA 300G/10K FC Add-on Hard Disk Drv | SGM75014H9 |
| Мрежови платформи | |
| Cisco Systems Catalyst 2950series | FOC0949ZOYP |
| Cisco Systems Catalyst 2950 series | FOC0949ZOYK |
| Cisco Systems Catalyst 2950 series | FOC1001Z3GO |
| Catalyst 6500 Series (6506 CoreSwitch 2)with firewall and IPSEC module with: SPA-IPSEC-SSC400-1; WS-SVC-FWM-1-K9; WS-SVC-IDS2-BUN-K9 | SAL1052C9AZ<br>firewall module: SAD11040AC4;<br>IDS: SAD11050B3X |
| Catalyst 6500 Series (6506 EdgeSwitch 1) with firewall and IPSEC module with :SPA-IPSEC-SSC400-1;WS-SVC-FWM-1-K9;WS-SVC-IDS2-BUN-K9 | SAL1052C9AU<br>firewall: SAD110203WG;<br>IDS: SAD11050B3Z |
| Cisco Catalyst 6500 Eseries (6509 CoreSwitchl) | SMG1102NOHT |
| Cisco 11 500 Series | JMX1 2092244 |
| Networking Cisco Catalyst 6506E WS-C6506-E-VPN+-K9 with: WS-SVC-FWM-1-K9 | SAL1212K08J |
| Cisco 11 500 Series | JMX1230501B |
| CP-7940G | FCH12479A33 |
| CP-7940G | FCH12479AEL |
| CP-7940G | FCH12478EV6 |
| CP-7940G | FCH12479ANW |
| CP-7940G | FCH124799XT |
| CP-7940G | FCH1247986C |
| CP-7970G | FCH120281JB |
| 2811 voice bundle | FCZ1232725S |
| 2811 voice bundle | FCZ132570AH |
| 2811 voice bundle | FCZ130771W9 |
| 2811 voice bundle | FCZ1239723Z |
| WS-C6506-E-VPN+-K9 | SAL1212K08J |
| WS-SVC-FWM-1-K9 | SAD1220022X |

## VII. Доставен Хардуер и Софтуер за целите на Проект „Развитие на административното обслужване по електронен път.“

| Описание | Модел | Количество (брой) |
|---|---|---|
| Надграждане (upgrade) на наличен Опорен Комутатор- Cisco Catalyst 6509-E -FWM-K9 | Cisco Catalyst 6509E (VS-S2T-10G=; WS-SSC-600=; WS-X6816-10G-2T=) | 1 |
| Доставка на резервиращ Опорен Комутатор | Cisco Catalyst 6509E | 1 |
| Разширение на 10GE свързаността чрез SAN комутатори | Cisco Nexus 5548UP | 2 |
| Формиране на Интернет Периметър чрез мрежови комутатори | Cisco Catalyst 2960X-24TD-L | 2 |
| Доставка и пускане в експлоатация на блейд шаси | Cisco UCS 5108 Blade Server Chassis | 2 |
| Доставка и пускане в експлоатация на блейд сървъри | Cisco UCS B200 M3 | 16 |
| Доставка и пускане в експлоатация на дискова подсистема | HP 3PAR 7400 2-N | 1 |
| Доставка и пускане в експлоатация на лентова архивираща библиотека за разширение на услугите по архивиране | HP StoreEver MSL Tape MSL4048 Tape Library | 1 |
| Доставка и пускане в експлоатация на управляващ сървър за доставяната лентова архивираща библиотека | HP ProLiant DL380p Gen8 Server | 1 |
| Доставка и пускане в експлоатация на лицензи за HP OpenView Data Protector - за пълното интегриране на лентовата библиотека в съществуващата система за архивиране HP OpenView Data Protector; | HP Data Protector Drive Extension | |
| Доставка и пускане в експлоатация на софтуер за резервни копия и архивиране на виртуална среда - необходимите лицензи за доставяните сървъри | Veeam Backup and Replication | |
| Доставка и пускане в експлоатация на софтуер за сървърна виртуализация - необходимите лицензи за доставяните сървъри | VMware vSphere | |

**VIII. Доставка на хардуерно оборудване и софтуерни лицензи за целите на проект „Надграждане на съществуващите и изграждане на нови централни системи на електронното правителство с оглед на усъвършенстване на информационно-комуникационната среда за по-добро административно обслужване на гражданите и бизнеса”**

| Описание * | Модел | Количество (брой) |
|---|---|---|
| Сървърно шаси за инсталиране на сървъри тип 1 | CISCO UCS | 4 |
| Сървъри тип 1 | CISCO UCS B200 | 30 |
| Сървърно шаси за инсталиране на сървъри тип 2 | CISCO UCS | 4 |
| Сървъри тип 2 | CISCO UCS B22 | 30 |
| Разширение на 10GE свързаността чрез SAN комутатори | CISCO Nexus 5596 | 2 |
| Маршрутизатор ISP/VPN концентратор | CISCO ASR1002-X | 2 |
| Защитна стена | CISCO ASA 5585-X | 2 |
| Система за контрол на правата на потребителите | Cisco Secure ACS | 1 |
| Основна дискова подсистема | HP 3PAR StoreServ 7400 4-N | 1 |
| Резервираща дискова подсистема | HP 3PAR StoreServ 7400 4-N | 1 |
| Устройство за архивиране върху дискове | HP StoreOnce 4500 24TB | 1 |
| Сървърен шкаф | HP Intelligent Rack 642 | 4 |
| Надграждане на съществуващата система за архивиране HP OpenView Data Protector | HP Data Protector | 1 |
| Надграждане на съществуващата подсистема за управление и наблюдение на мрежи, сървъри и приложения в следните модули HP OpenView Operations, HP OpenView Network Node Manager Advanced Edition, HP SiteScope | HP OpenView Operations, HP OpenView Network Node Manager Advanced Edition, HP SiteScope | 1 |
| Автоматизирано решение за наблюдение, анализ и управление на събитията по сигурността –SIEM | IBM SECURITY QRADAR SIEM ALL-IN-ONE 2100; IBM SECURITY QRADAR RISK MANAGER | 1 |
| Изграждане на система за управление на Microsoft Windows среда | Microsoft System Center 2012 R2 Datacenter | 1 |