Р Е П У Б Л И К А Б Ъ Л Г А Р И Я
ДЪРЖАВНА АГЕНЦИЯ „ЕЛЕКТРОННО УПРАВЛЕНИЕ“

АРХИТЕКТУРА НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ В РЕПУБЛИКА БЪЛГАРИЯ

КРАТКО ОПИСАНИЕ

(по Архитектура на електронното управление в Република България
– общо описание версия 1.5)

Одобрена от председателя на Държавна агенция „Електронно управление“
със Заповед № ДАЕУ-5040-11.04.2019 г.

Април 2019 г.
Версия 1.5

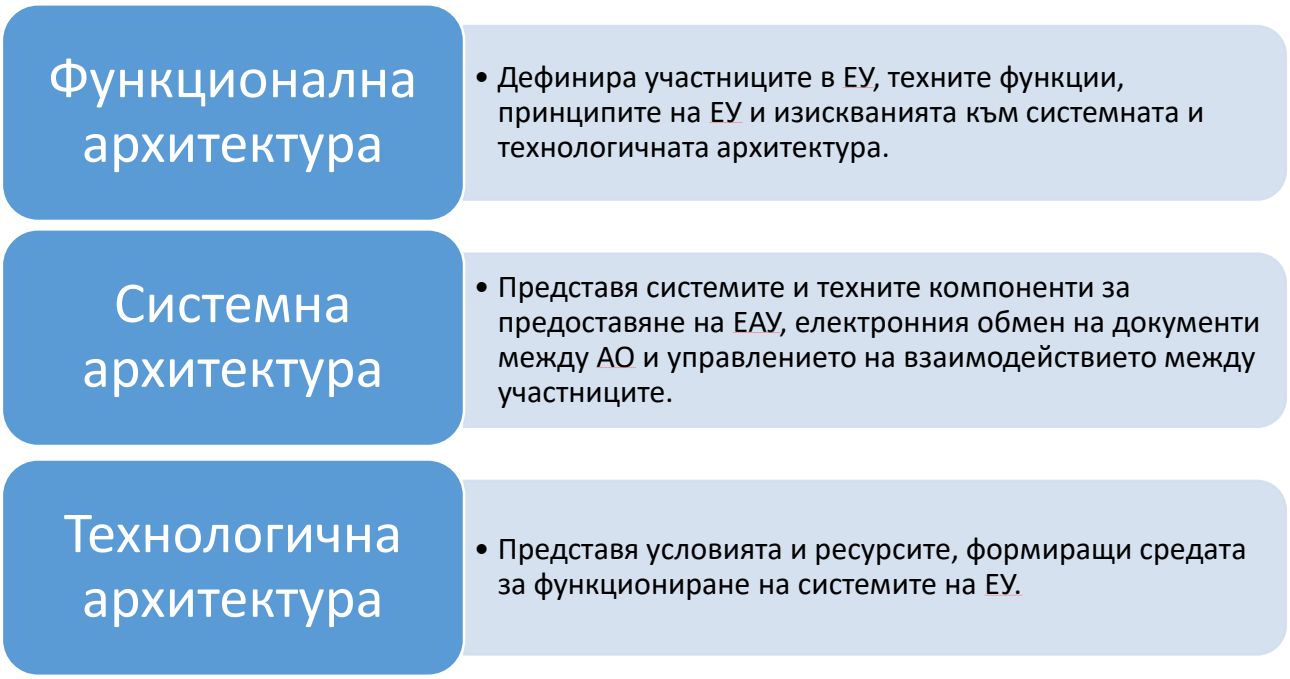
Съдържание:

I. ВЪВЕДЕНИЕ

Информационните и комуникационните технологии (ИКТ) трайно навлизат във всички области на социалния и икономическия живот и дейността на административните органи. Чрез изграждане и развитие на електронно управление (ЕУ) се цели подобряване качеството на административното обслужване и повече публичен контрол върху дейността на административните органи.

Настоящият документ представлява резюме на Архитектурата на електронното управление на Република България – общо описание, за нейното представяне на по-широк кръг държавни служители, граждани и бизнес.

Документът съдържа кратко описание на архитектурата, структурирано в три аспекта – функционална архитектура, системна архитектура и технологична архитектура.



Структура на архитектурата на електронното управление

Електронното управление е процес на реализиране от административните органи, органите на съдебната власт, лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги, на правни взаимовръзки, административни процеси и услуги и на взаимодействието с потребителите чрез използване на информационни и комуникационни технологии, осигуряващи по-високо ниво на ефективност на управлението.

Архитектурата на ЕУ предоставя обща рамка, която дефинира и регламентира нейните елементи, като обхваща целия процес на взаимодействие между участниците в е-управлението.

Архитектурата на ЕУ е насочена към реализирането на:

- цифрова трансформация на администрацията;
- технологични решения за предоставяните административни услуги на основата на комплексно административно обслужване (КАО), „епизоди от живота“ и „бизнес събития“;
- задължително използване от административните органи на хоризонталните системи и споделените ресурси на е-управлението;
- механизми за координация и контрол на изпълнението на архитектурата;
- прилагане на единни стандарти и оперативна съвместимост при проектиране, изграждане, надграждане и внедряване на информационните решения;

- устойчиво високо общо ниво на мрежова и информационна сигурност;
- трансформиране на данните в информация и знания;
- постигане на доверие от гражданите и бизнеса.

Отделните административни органи (АО) запазват обхвата и функционалностите на използваните от тях информационни системи, но прилагат общите принципи и използват споделената инфраструктура и системи на ЕУ. В съответствие с архитектурата на ЕУ се изготвят архитектури по области на политики.

Подходът за реализиране на ЕУ чрез архитектурата се основава на:

- прилагане на единен модел за заявяване, заплащане и предоставяне на електронни административни услуги, който стои зад всяка електронна административна услуга;
- въвеждане на длъжността „главен информационен мениджър (ГИМ)“ към първостепенните разпоредители с бюджет (ПРБ);
- въвеждане на ведомствени експертни съвети към ПРБ;
- преход от фрагментирани и затворени към цялостни и технологично независими решения;
- поетапна промяна на модела на съхранение на данните от децентрализиран към централизиран такъв, като се започва с най-критичните за електронното управление масиви от данни;
- изграждане и развитие на споделени информационни ресурси и предоставянето им за децентрализирано управление и използване;
- централизиран бюджетен и проектен контрол от страна на Държавната агенция „Електронно управление“ (ДАЕУ).

Всички документи по архитектурата се съхраняват в Държавната агенция „Електронно управление“. Достъпът до Архитектурата на електронното управление – общо описание, и до приложенията към нея се извършва по ред, определен от председателя на ДАЕУ.

Архитектурата на електронното управление е неотменима част от изпълнението на политиката за електронно управление, определена в Стратегията за развитие на електронното управление в Република България и Закона за електронното управление (ЗЕУ). Изпълнението на документа е подчинено на ефективната координация между всички заинтересовани страни.

На общата схема на електронното управление са представени основните участници и информационните ресурси, осигуряващи и поддържащи координацията и взаимодействието им в рамките на ЕУ.

Архитектурата на електронното управление е задължителен за изпълнение документ и модел, спрямо който да бъдат разработвани архитектури по области на политики от съответните отговорни административни органи.

Обща схема на електронното управление на Република България

Архитектурата подлежи на развитие – изменение и/или допълнение, като за целта ДАЕУ ежегодно провежда преглед и анализ на:

- организационната структура за изпълнение на политиката за електронно управление;
- нормативната уредба за реализиране на политиката за електронно управление;
- промяната в структурата на администрацията и организацията на работните процеси;
- състоянието, функционирането и използването на информационните ресурси на ЕУ, осигуряващи предоставяне на ЕАУ;
- оперативната съвместимост;
- мрежовата и информационната сигурност;
- използването на нови информационни и комуникационни технологии в ЕУ.

II. ФУНКЦИОНАЛНА АРХИТЕКТУРА

Във функционалната архитектура са дефинирани участниците в ЕУ, техните функции, принципите на взаимодействие и политиките за развитие на ЕУ. Поставят се изискванията към системната и технологичната архитектура.

1. Участници в електронното управление

Участници в електронното управление са гражданите и бизнесът, административните органи, администрацията на изпълнителната власт, органите на съдебната власт, лицата, осъществяващи публични функции, организациите, предоставящи обществени услуги, посредниците при заявяване на електронни административни услуги.

1.1. Граждани и бизнес

Гражданите и бизнесът са основните потребители на административни услуги. Те са в центъра на административното обслужване и дизайнът на административните процеси по предоставянето на ЕАУ следва да бъде съобразен с техните изисквания, очаквания и нужди.

1.2. Административни органи

Административните органи вземат основните решения по всички ключови въпроси, свързани с реализацията на ЕУ в съответната област на политиката и с развитието на администрацията.

От гледна точка на събирането и достъпа до данни, генерирани за гражданите и бизнеса, административните органи са:

- Първични администратори на данни

Първичният администратор на данни (ПАД) е административен орган, който по силата на закон събира или създава данни за гражданин или организация за първи път и изменя или заличава тези данни. ПАД изпраща служебно и безплатно данните на всички лица по чл. 1, ал. 1 и 2 от ЗЕУ, които въз основа на закон също обработват тези данни и са заявили желание да ги получават.

- Потребители на данни

Потребителите на данни са АО и лица по чл. 1, ал. 2 от ЗЕУ, които достъпват данните, предоставени от ПАД, в изпълнение на нормативно определените им задължения. Първичните администратори на данни също са потребители на данните, които се събират, обработват или заличават от тях или от други първични администратори.

От гледна точка на правомощията по отношение на управление и контрол на бюджета, АО се делят на първостепенни, второстепенни и от по-ниска степен разпоредители с бюджет.

1.3. Администрация на изпълнителната власт

Администрацията на изпълнителната власт е централна и териториална. Тя обхваща администрацията на Министерския съвет, министерствата, държавните агенции, администрацията на държавните комисии, изпълнителните агенции, административните структури, създадени с нормативен акт, които имат функции във връзка с осъществяването на изпълнителната власт (централна), областните и общинските администрации и специализираните териториални администрации, създадени като самостоятелни юридически лица с нормативен акт (териториална).

1.4. Органи на съдебната власт

Органите на съдебната власт са съдилищата, прокуратурата и следствените органи. Съдебната власт се представлява от Висшия съдебен съвет.

Органите на съдебната власт, в изпълнение на функциите си, обменят информация както помежду си, така и с органите на изпълнителната власт и взаимодействат с гражданите и бизнеса. Съдебната власт развива активно електронното правосъдие като средство за повишаване на ефективността на сектор „Правосъдие“ и облекчаване на достъпа до правосъдие. Реализацията на мерките за електронно правосъдие е обвързана с цялостното изпълнение на политиката за развитие на електронното управление в Р България.

1.5. Лица, осъществяващи публични функции, и организации, предоставящи обществени услуги

Те са определени в ЗЕУ, а в архитектурата на ЕУ имат двойствена природа и в зависимост от конкретния случай попадат в категорията „бизнес“ (когато аналогично на всички други представители на бизнеса заявяват административни услуги от АО) или в категорията „администрация“ (когато гражданите и другите представители на бизнеса заявяват административни услуги пред тях).

За осъществяването на своята дейност лицата с публични функции и организациите, предоставящи обществени услуги, от една страна, се нуждаят от данни, налични в първични регистри, а от друга – самите те създават и съхраняват първични данни. В този смисъл те също могат да бъдат и ПАД, и потребители на данни.

1.6. Посредници при заявяване на електронни административни услуги

По смисъла на ЗЕУ пълномощник/посредник при заявяване на ЕАУ е лице, което представлява по пълномощно получател на ЕАУ за заявяване и получаване на съответната услуга. Посредникът заявява изпълнението на услугата от името на физическото или юридическото лице, което го е упълномощило. Услугата може да бъде предоставена само след проверка в Регистъра с пълномощни на Нотариалната камара, в Регистъра на овластяванията по смисъла на Закона за електронната идентификация (ЗЕИ) или при създадена възможност за регистриране на пълномощни към профила на потребителя или за заявяване на услугата. Пълномощник може да бъде и посредник за предоставяне на ЕАУ по реда на ЗЕУ.

Взаимодействието между участниците в е-управлението се осъществява:

- синхронно – заявителят получава резултата от услуга от в реално време;
- асинхронно – резултатът от заявената услуга не се предоставя незабавно, а на по-късен етап, чрез уведомяване на заявителя или повторно запитване от негова страна.

2. Управление, координация и контрол

Управлението, координацията и контролът на изграждането и функционирането на е-управлението се осъществява от Държавната агенция „Електронно управление“, главните информационни мениджъри и система от съвети в областта на е-управлението.

2.1. Държавна агенция „Електронно управление“

Министерският съвет посредством Държавната агенция „Електронно управление“ координира дейността на АО за осъществяването на единна държавна политика в областта на електронното управление. ДАЕУ изпълнява функции както по създаване, налагане и контрол на политики, правила и добри практики, стратегическо планиране и законодателни инициативи, бюджетно програмиране и контрол, координация на политиките за е-управление по области и на междуведомствени проекти, така и по поддържане на централизирани регистри за нуждите на е-управлението, Държавния хибриден частен облак (ДХЧО) и Единната електронна съобщителна мрежа (ЕЕСМ) на държавната администрация. ДАЕУ поддържа и развива хоризонталните системи на е-управлението и ръководи дейностите по интеграцията им във всички АО.

2.2. Главен информационен мениджър

Главният информационен мениджър (ГИМ) е ключова длъжност в мениджмънта на ЕУ на национално и секторно ниво. Функциите на главен информационен мениджър в административните органи, първостепенни разпоредители с бюджет, се изпълняват от главните секретари, съответно административния секретар на Министерството на вътрешните работи и на Министерството на отбраната. Във всеки първостепенен разпоредител с бюджет (ПРБ) се създава постоянна длъжност на пряко подчинение на АО, който отговаря и за второстепенните и от по-ниска степен разпоредители с бюджет. ГИМ на ДАЕУ отговаря за прилагането на архитектурата на е-управлението.

Основната функция на ГИМ на ПРБ е да определя единна политика в областта на е-управлението и развитието на ИКТ инфраструктурата, както и да координира и контролира дейностите по придобиване и развитие на информационни системи и ресурси в системата на съответния ПРБ.

2.3. Съвети в областта на електронното управление

Общата политика в областта на развитието на администрацията и административната реформа се ръководи от Съвета за административната реформа към Министерския съвет.

В сферата на електронното управление и ИКТ функционира система от съвети:

- *Съвет на главните информационни мениджъри (СГИМ)* към ресорен заместник министър-председател. Съветът на ГИМ е междуведомствен орган със съвещателни, координационни и контролни функции по отношение на разработването и изпълнението на политиките в областта на електронното управление. Съветът следи за подобряване и уеднаквяване на ведомствените практики, свързани с проектирането, придобиването, развитието, използването, споделянето и ефективността на информационните системи и ресурси в АО. В него участват ГИМ на ДАЕУ и ГИМ на административните органи, първостепенни разпоредители с бюджет.

- *Експертен съвет за интеграция на информационните ресурси* към председателя на ДАЕУ, за координиране на междуинституционалното взаимодействие при изграждането и експлоатацията на споделени информационни ресурси и интеграцията на информационни системи на АО с хоризонталните системи на електронното управление. В него участват ИТ директорите на ведомства, представители на ДАЕУ, както и представители на академични институции.

- *Бизнес съвет* към председателя на ДАЕУ, който дава становища, изразява позиции, прави препоръки по реализацията на политиката за е-управление. В Бизнес съвета участват представители на организации от сектора на ИКТ.

- *Ведомствени експертни съвети* (ВЕС) към ПРБ. Ведомственият експертен съвет се председателства от ГИМ. Съветът разглежда и съгласува всички технически спецификации, както и всички технически проекти на съответните ПРБ и техните разпоредители с бюджет в областта на е-управлението и ИКТ, включително средствата за тях, и ги предлага за утвърждаване от ПРБ. Утвърдените бюджети, проекти и технически спецификации се съгласуват с ДАЕУ в рамките на провежданите контрол по целесъобразност и проектен контрол.

2.4. Основни политики и принципи

Основите политики, обхванати в архитектурата, са:

- електронното управление;
- електронните удостоверителни услуги;
- електронната идентификация;
- мрежовата и информационна сигурност;
- информацията от обществения сектор в машинночетим отворен формат;

Архитектурата включва развитието и управлението на информационните ресурси и използването на информационните и комуникационните технологии в дейността на АО, управлението на споделените ресурси, както и управлението на лицензите за нуждите на държавната администрация.

Всички дейности в областта на е-управлението се базират на принципи, които следва задължително да се прилагат от АО, органите на съдебната власт, лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги. Принципите са дефинирани в Плана за действие на ЕС за електронно управление през периода 2016 – 2020 г. и са напълно припознати и доразвити в Стратегията за развитие на електронното управление в Република България 2019 – 2023 г., както следва:

- неприкосновеност на личността и личния живот;
- поставяне на потребителя в центъра на административното обслужване;
- еднократно събиране и създаване на данни;
- предоставяне на услуги по електронен път;
- мрежова и информационна сигурност;
- откритост и прозрачност;
- оперативна съвместимост;
- трансграничност;
- наличност на информацията онлайн;
- електронна (безхартиена) комуникация;
- отворени данни;
- измеримост.

3. Електронното управление по области на политики

За целите на електронното управление административните органи се групират по области на политики в зависимост от сферата на основната им дейности и функции.

Областите на политики са организирани около конкретни специфични дейности и функции, определящи преки цели и крайни резултати, които трябва да се постигнат от АО по отношение на електронното управление.

Чрез разделението по области на политики ДАЕУ се стреми да катализира цялостното подобряване на организацията по развитието и функционирането на електронното управление на базата на:

- лидерско управление на разработването на съответните архитектури, стратегии и програми;
- централизирано обединение и интегриране на информационните ресурси и децентрализираното им управление и използване;
- прилагане на единни модели и процеси;
- подготовка и развитие на човешки ресурси.

4. Жизнен цикъл на информационните ресурси

Жизненият цикъл обхваща всички етапи, през които последователно преминават информационните ресурси при изграждането или модернизацията на информационно-комуникационната среда, от формулирането на първоначална концепция до времето, когато те са използвани докрай или са свалени от употреба като остарели, неикономични, за ремонт, излишно и негодно имущество, по отношение на изискванията за бракуване на материални средства. Управлението на жизнения цикъл на информационните ресурси за е-управление включва:

- проучване;
- разработка на прототипи;
- избор на образец;
- придобиване;
- експлоатация и усъвършенстване;
- снемане от употреба.

Схема на етапите от жизнения цикъл на ИР

Жизненият цикъл на информационните ресурси е управляем процес. Административните органи трябва да управляват информационните си ресурси и базираната на тях информация, така че да предоставят и поддържат ефективно и ефикасно дейността си и предоставяните услуги, като по този начин осигуряват устойчивостта на инвестициите по реализация и внедряване на информационните си системи. Прилагането на принципите и подходите на проектния мениджмънт осигурява ефективно управление на дейностите през целия жизнен цикъл на информационния ресурс.

За гарантиране на устойчива работоспособност на информационните ресурси и достъпност до предоставяните чрез тях услуги е необходимо те да са обезпечени финансово и с необходимите човешки ресурси за експлоатацията и поддръжката им до извеждането им от реална експлоатация. За всеки информационен ресурс е нужно да се разпишат в процедура: необходимите ресурси, отговорностите на лицата и действията, свързани с неговото изграждане, поддръжка и развитие.

5. Електронни услуги

Електронните услуги в контекста на е-управлението са ИТ услуги и електронни административни услуги (ЕАУ). Тяхното предоставяне е един от основните елементи на електронното управление.

5.1. ИТ услуги

ИТ услугите са независими компоненти, чрез които се предоставят конкретни функционалности на АО за реализиране и управление на достъп до информация или споделени информационни ресурси.

Те може да работят на отдалечено разстояние, достъпни са по електронен път и чрез тях се предоставя инфраструктура или комуникационни услуги.

5.2. Електронни административни услуги

Електронните административни услуги са административни услуги, заявявани и/или предоставяни изцяло или частично по електронен път. При предоставянето им се използват ресурсите на електронното управление. Всяка ЕАУ задължително се вписва в Административния регистър.

Електронните административни услуги се реализират посредством:

- информационни системи;
- регистри;
- бази данни.

Нивата на предоставяне на услугите отразяват нивото на развитие, на което се предоставят услугите по електронен път:

- Ниво 1 – **Информация**: предоставяне на онлайн информация за административни услуги – начини и места на заявяване на услугите, срокове и такси.
- Ниво 2 – **Едностранна комуникация**: информация съгласно дефиницията за ниво 1 и предоставяне на онлайн достъп до шаблони на електронни формуляри.
- Ниво 3 – **Двустранна комуникация**: заявяване и получаване на услуги изцяло по електронен път, включително електронно подаване на данни и документи и/или електронна обработка на формуляри (електронни форми) и електронна персонална идентификация на потребителите.
- Ниво 4 – **Извършване на сделки и/или трансакции** по услуги от ниво 3, включващи онлайн разплащане и доставка.

Основните видове услуги са:

- Първична услуга – административна услуга, която се осъществява в рамките на една географски или функционално обособена администрация като единен процес, започващ със заявление за услугата и приключващ с предоставяне на услугата или постановяване на отказ.
- Комплексна услуга – административна услуга, която се изпълнява като процес, в който достъпът до данни, поддържани от администрациите, се осъществява чрез използване на първични или други комплексни услуги.
- Вътрешна ЕАУ (ВЕАУ) – вътрешна административна услуга, която се заявява и/или предоставя от разстояние чрез използването на електронни средства. При комплексните услуги необходимата за предоставянето им информация се обменя посредством ВЕАУ.

6. Правна рамка на електронното управление

Правната рамка е съвкупността от закони и подзаконови нормативни актове, определящи правомощията, организационния обхват, изискванията, условията за функциониране на АО за реализиране на електронното управление.

През последните години бяха приети основните нормативни актове, с които се положи правната база за цифровизация на процесите в администрацията, както и за улесняване на взаимодействието между администрация, служители, граждани и бизнес чрез използването на електронни услуги.

6.1. Закони в областта на електронното управление

Закон за електронното управление

Законът за електронното управление урежда дейността на административните органи, органите на съдебната власт, лицата, осъществяващи публични функции, и на организациите, предоставящи обществени услуги при работа с електронни документи, предоставянето на административни услуги по електронен път и вътрешния обмен на електронни документи. В обхвата на закона попадат управлението на дейностите в областта на електронното управление, предоставянето на електронни административни услуги, оперативната съвместимост и информационната сигурност, контролът и взаимодействието между ДАЕУ и административните органи. Законът цели да се обезпечи разработването, надграждането и внедряването на необходимите информационни ресурси на електронното управление при спазване на изискванията за мрежова и информационна сигурност и оперативна съвместимост, както и при устойчив модел за дългосрочно управление и финансов ресурс за поддръжка на тези информационни ресурси. ЗЕУ регламентира прилагането от адресатите на закона на основните принципи на е-управлението.

Разпоредбите на ЗЕУ, включително по отношение на други специфични изисквания към информационните системи и електронните административни услуги, са детайлизирани в Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги (НОИИСРЕАУ).

Закон за електронната идентификация

Законът за електронната идентификация урежда функциите, задълженията и отговорностите на всеки участник в процеса на създаване на електронна идентичност на физическите лица и електронната идентификация. В центъра на определената в ЗЕИ схема за електронна идентификация е физическото лице (български гражданин или чужденец, постоянно пребиваващ на територията на Република България) – потребител на електронни услуги. Уредбата е подчинена на принципа за техническа и технологична неутралност на инструментите и механизмите, които се използват за електронната идентификация, включително и на носителя на електронна идентичност. Това обуславя възможността тя да се

съхранява на и активира чрез различни носители, включително документи за самоличност с чип, банкови карти, други смарт карти с чип и мобилни устройства.

Предвидена е и допълнителна възможност за физическите лица да се идентифицират чрез секторни електронни идентификатори. Компетентният административен орган във връзка с издаването и управлението на удостоверенията за електронна идентичност (орган за електронна идентификация) е министърът на вътрешните работи. За български граждани, които пребивават в чужбина, тази дейност ще се подпомага от дипломатическите и консулските представителства на Република България.

В ЗЕИ се уреждат още правилата за извършване на проверка за валидност на издадените удостоверения за електронна идентичност от центрове за електронна идентификация. Предвидено е създаването на център за електронна идентификация в ДАЕУ, като е включена възможност и други лица да осъществяват функциите на такъв център след вписването им в специален регистър, създаден и поддържан от министъра на вътрешните работи.

Закон за киберсигурност

Законът за киберсигурност (ЗКС) транспонира разпоредбите на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 06 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза за постигне на следните цели:

- създаване на условия за изграждане на ефективна институционална система на национално равнище за превенция и борба с кибератаките чрез определянето на компетентни органи в областта на киберсигурността, както и техните функции и правомощия;
- ограничаване на мащаба, честотата и въздействието на инцидентите чрез оценка на рисковете от кибератаки и предприемането на подходящи и пропорционални мерки за измерване на действителните рискове, както и чрез докладване за инцидентите;
- противодействие на инцидентите, които причиняват значителни финансови загуби, подкопават доверието на потребителите и причиняват големи вреди на икономиката на държавата;
- ограничаване на транснационалния характер на инцидентите.

6.2. Законодателство по области на политики

Към настоящия момент част от националното законодателство не е в съответствие с разпоредбите на ЗЕУ и нормативната уредба, регламентираща процесите на електронното управление. С оглед постигане на целите на електронното управление и все по-пълното му навлизане в дейността на административните органи, органите на съдебната власт, лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги, е необходимо да продължат действията по синхронизиране на националното законодателство за целите на електронното управление, за да бъдат преодолени несъответствията.

III. СИСТЕМНА АРХИТЕКТУРА

Системната архитектура представя системните решения за осигуряване на функционирането на ЕУ. Тя описва системите и техните компоненти за реализиране на процеса за предоставяне на ЕАУ, електронния обмен на документи и данни между АО и управлението на взаимодействието между участниците в ЕУ. Архитектурата се състои от интеграционен слой, хоризонтални системи, централизирани системи, регистри и бази данни, приложения, осигуряващи функционирането на ЕУ.

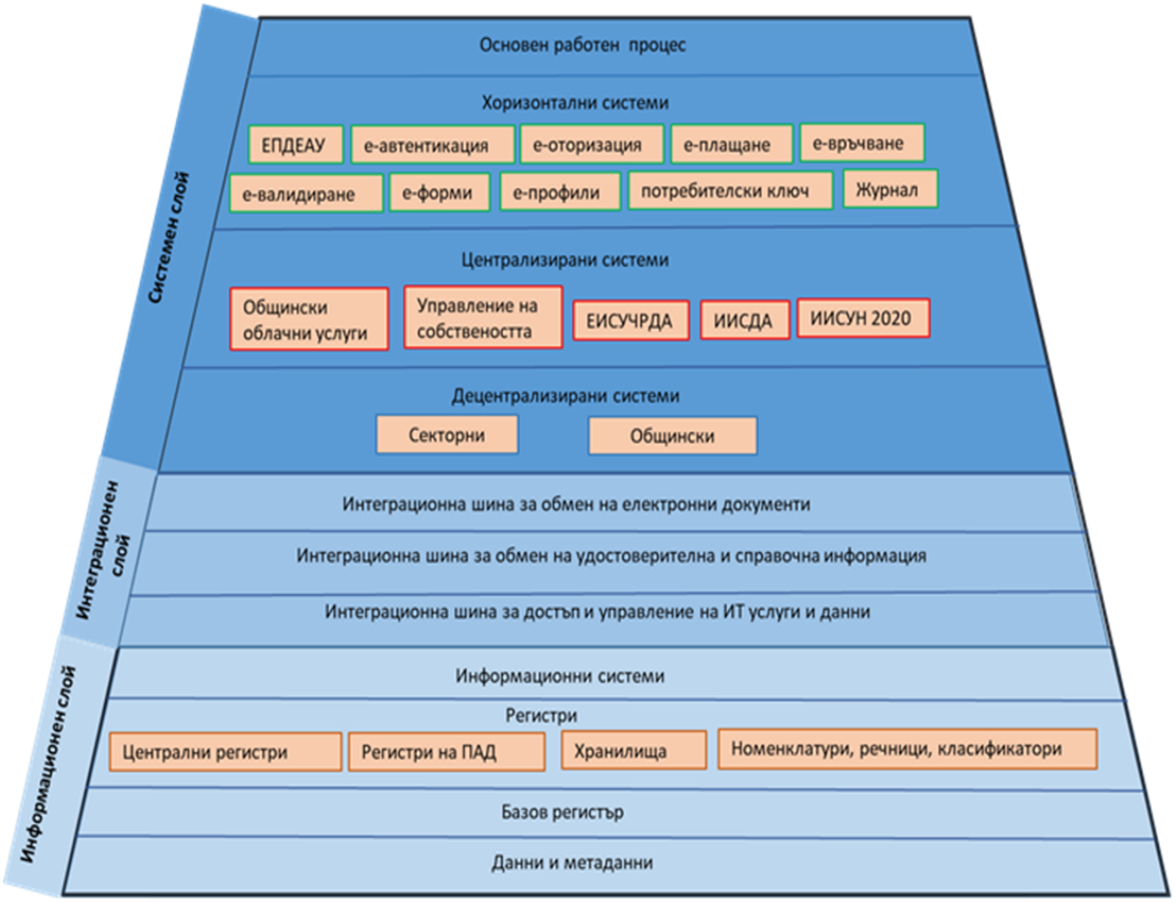


Схема на системната архитектура на електронното управление

1. Основен работен процес

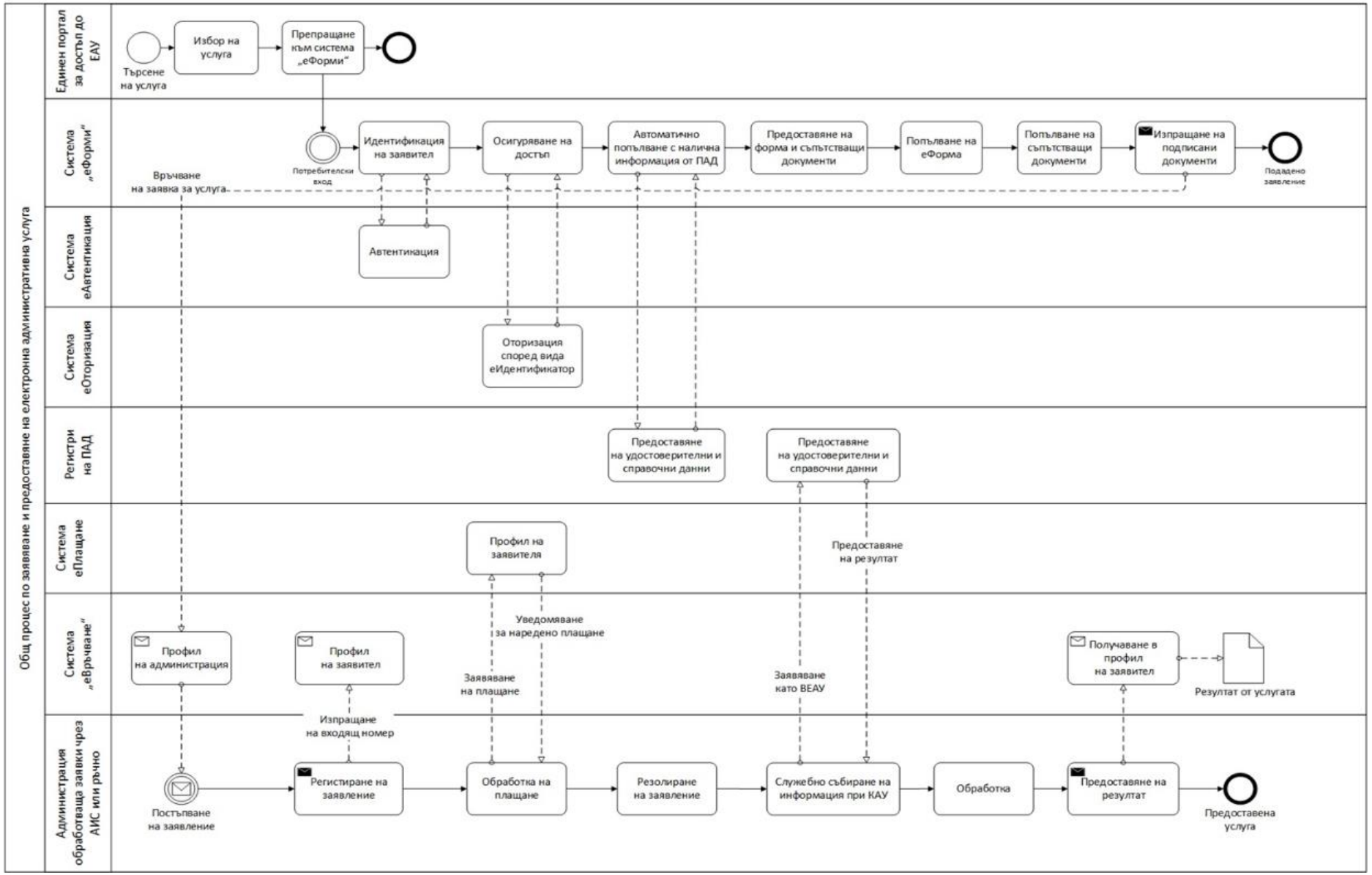
Системната архитектура на ЕУ е процесноориентирана и се базира на работни процеси. Те се характеризират с:

- определеност;
- време за изпълнение;
- потребител;
- доставчик (отговорник за изпълнението);
- собственик на процеса;
- функция, приключваща с конкретен резултат;
- добавяне на стойност за получателя;
- ресурси (технически, човешки и финансов ресурс);
- правна рамка;
- управление.

Основният работен процес е фокусът на системната архитектура и представлява комплекс от логически свързани дейности по заявяване и предоставяне на ЕАУ. На негова база се изгражда Единен модел за заявяване, заплащане и предоставяне на електронни административни услуги. Той описва взаимодействието между всички участници в процеса и действията по заявяване, заплащане, обработка от доставчика на услугата и предоставянето на резултата на потребителите на ЕАУ. Посредством основния работен процес:

- всяка една услуга, която позволява електронна доставка на резултата, може да се трансформира в услуга от ниво 4;

- всяка услуга може да се предоставя като комплексна административна услуга, ако необходимата съпътстваща за предоставянето ѝ информация вече е налична в регистри и бази данни, чрез предоставената възможност за служебно извличане на информация, като вътрешна електронна административна услуга;
- заявяването, заплащането и предоставянето на ЕАУ не зависи от степента на автоматизация и интеграция на доставчика на услугата.



Модел на основен работен процес – заявяване, заплащане и предоставяне на ЕАУ

2. Хоризонтални системи на електронното управление

Хоризонталните системи са информационни системи с функционалности, които са общи при предоставянето на всяка една ЕАУ – автентикация, оторизация, заплащане, връчване и валидиране, и е задължително ИС на АО да са интегрирани с тях.

2.1. Единен портал за достъп до електронни административни услуги

Единният портал за достъп до електронни административни услуги (ЕПДЕАУ, eGov.bg) представлява единна точка за достъп до ЕАУ. Порталът осигурява сигурен и удобен достъп и канал за комуникация с потребителите на ЕАУ – всички лица, които желаят да ги заявят и получат по електронен път. Порталът предоставя информация, която се съхранява в Административния регистър във връзка с предоставянето на електронните услуги.

Порталната платформа съдържа инструменти за създаване и управление на работни процеси и разпределяне на дейности за изпълнение на предвидените потребителски случаи от различните групи потребители.

2.2. Система за е-Автентикация

Системата за е-Автентикация реализира процеса, свързан с еднократна идентификация и автентификация на заявители на предоставяните от администрациите е-услуги или други уеб приложения. Тя предоставя интерфейс, с помощта на който се интегрират външни информационни системи. Системата издава електронни атестати на физически лица и информационни системи и поддържа нормативно установените средства за идентификация. Тя трябва да бъде интегрирана и с центровете за електронна идентификация.

Информационните системи за заявяване на ЕАУ и ИС на лицата по чл. 1, ал. 1 и ал. 2 от ЗЕУ се интегрират със системата за е-Автентикация по стандартизиран протокол. Интеграцията на системата за е-Автентикация с центровете за електронна идентификация се осъществява по стандартизиран, защитен протокол от тип „система–система“ в средата на електронното управление.

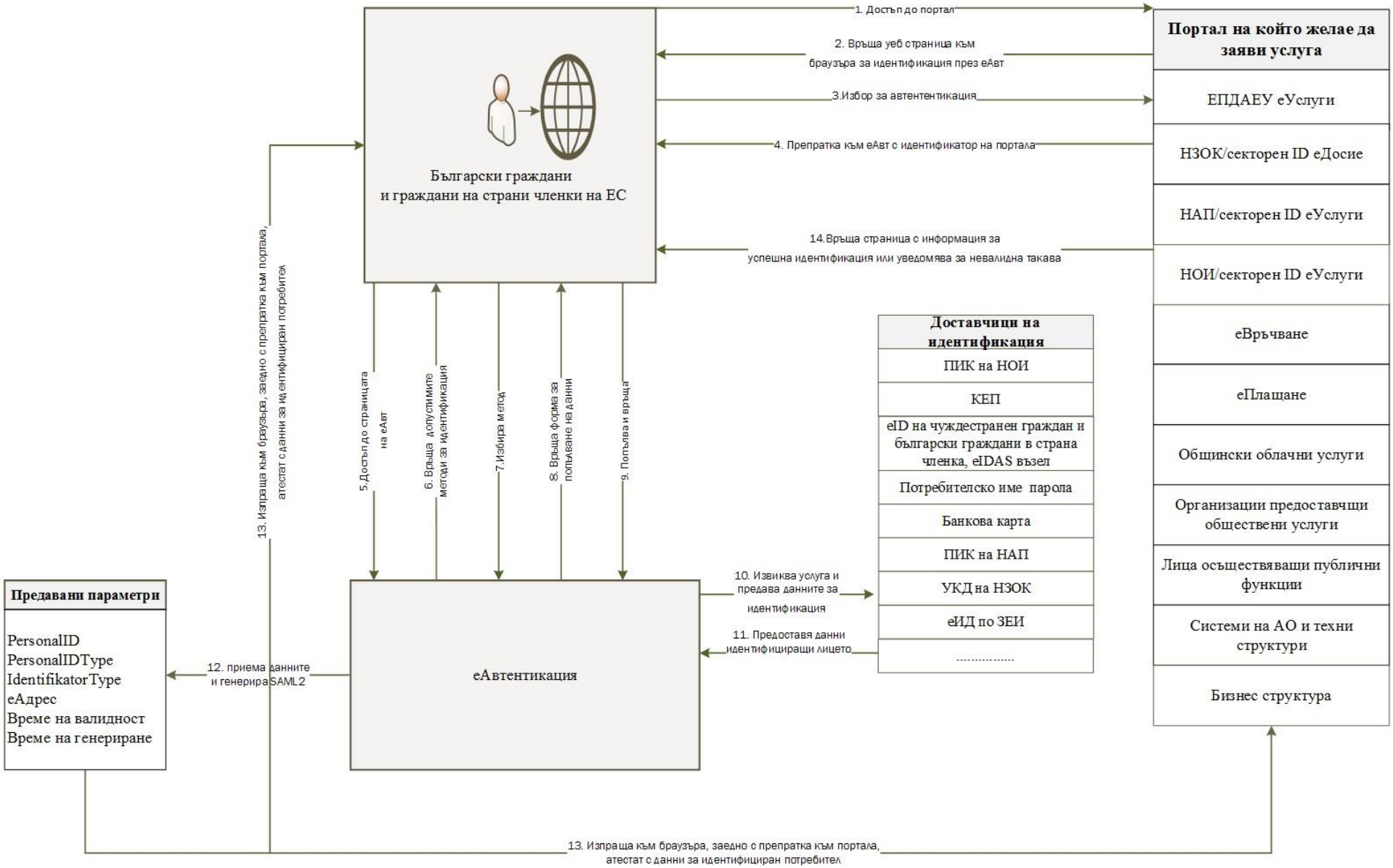


Схема на функционален модел на е-Автентикация и взаимодействие с други системи

2.3. Система за е-Оторизация

Системата за е-Оторизация реализира контрол на достъпа до системите и ресурсите на ЕУ. Тя предоставя уеб интерфейс, с помощта на който външни ИС заявяват оторизация на достъп до системен ресурс.

Системата реализира контрол на достъпа, управляван от политики. Чрез нея се разрешава или отказва достъп до ресурси въз основа на утвърдени политики и изисквания за управление. Администрациите създават и прилагат политики, определящи кой до какви ресурси да има достъп и при какви обстоятелства.

Системата за е-Оторизация способства да се въведат строги и единни политики за контрол на достъпа до ресурсите в администрациите. Тя е контролен механизъм за одит на достъпа до ресурсите на ЕУ.

2.4. Система за електронни плащания към доставчици на услуги

Системата за електронни плащания осигурява по допустим, сигурен и проследим начин създаването на платежен документ от тип „платежно нареждане“ и предаването му за изпълнение от доставчик на платежни услуги. Тя поддържа профили на потребители, в които се съхранява история на заявени и наредени плащания и предоставя потвърждение на информационните системи, заявили плащане, за момента на нареждане на същото. Системата предоставя интерфейс, с помощта на който се интегрират външни информационни системи. Заявителят може да намери информация в профила си, като същият играе роля на „електронен портфейл“.

Системата за електронни плащания се интегрира с ИС на АО, функционалността на които изисква заплащане на суми и осигурява възможност за преминаване на ЕАУ от ниво 3 на ниво 4, като осигурява:

- идентифициране с нормативно регламентирано средство за електронна идентификация;
- регистриране на заявки за плащане от доставчик на услуга;
- предоставяне на възможност за плащане по избран от потребителя платежен канал;
- справка за налични задължения за плащане;
- справка за наредени плащания.

Посоката за развитие е свързана с интеграция с информационните системи на административните структури, функционалността на които изисква заплащане на суми, както и доразвитие с цел осигуряване на възможности за преминаване на услугите от ниво 3 към ниво 4.

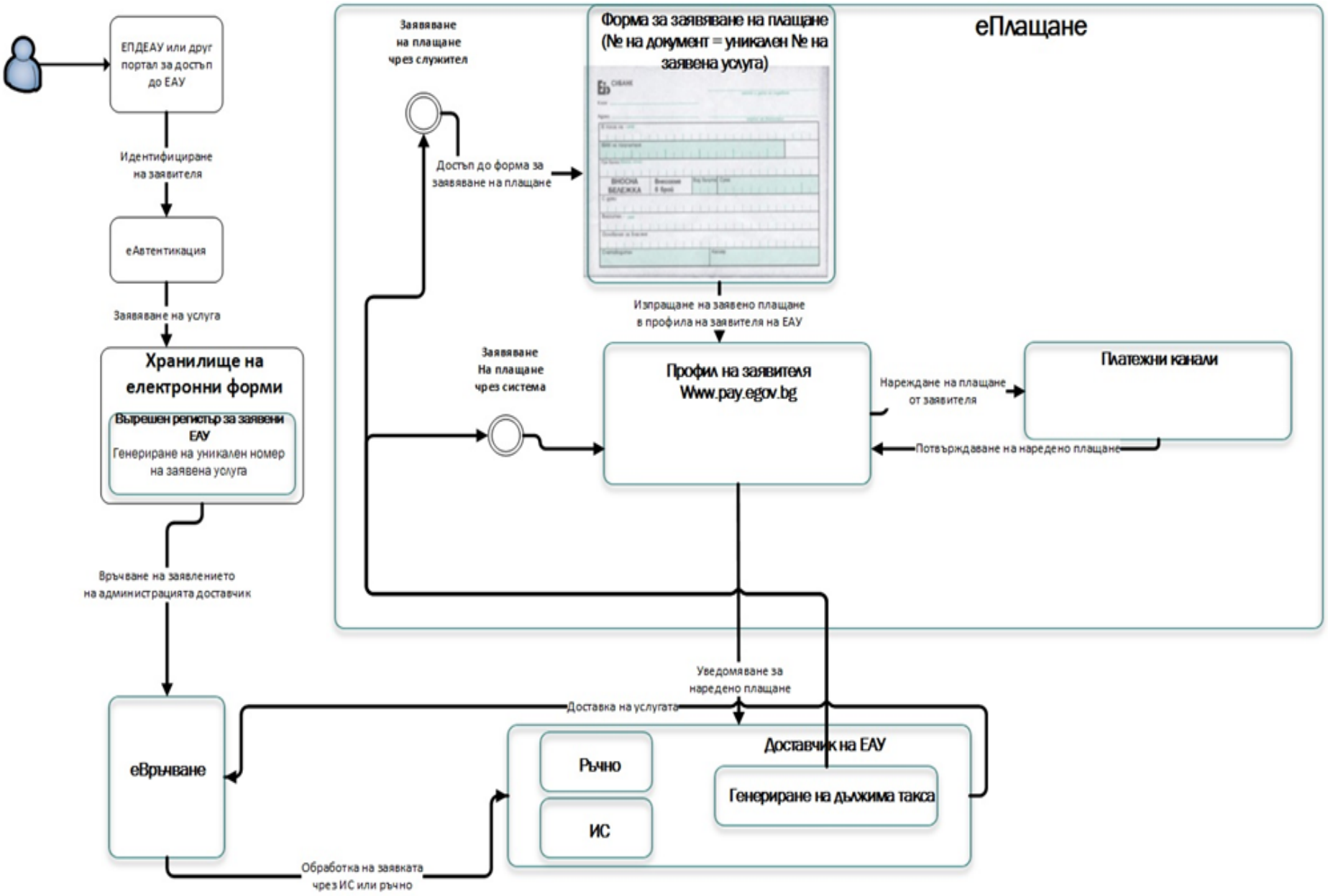


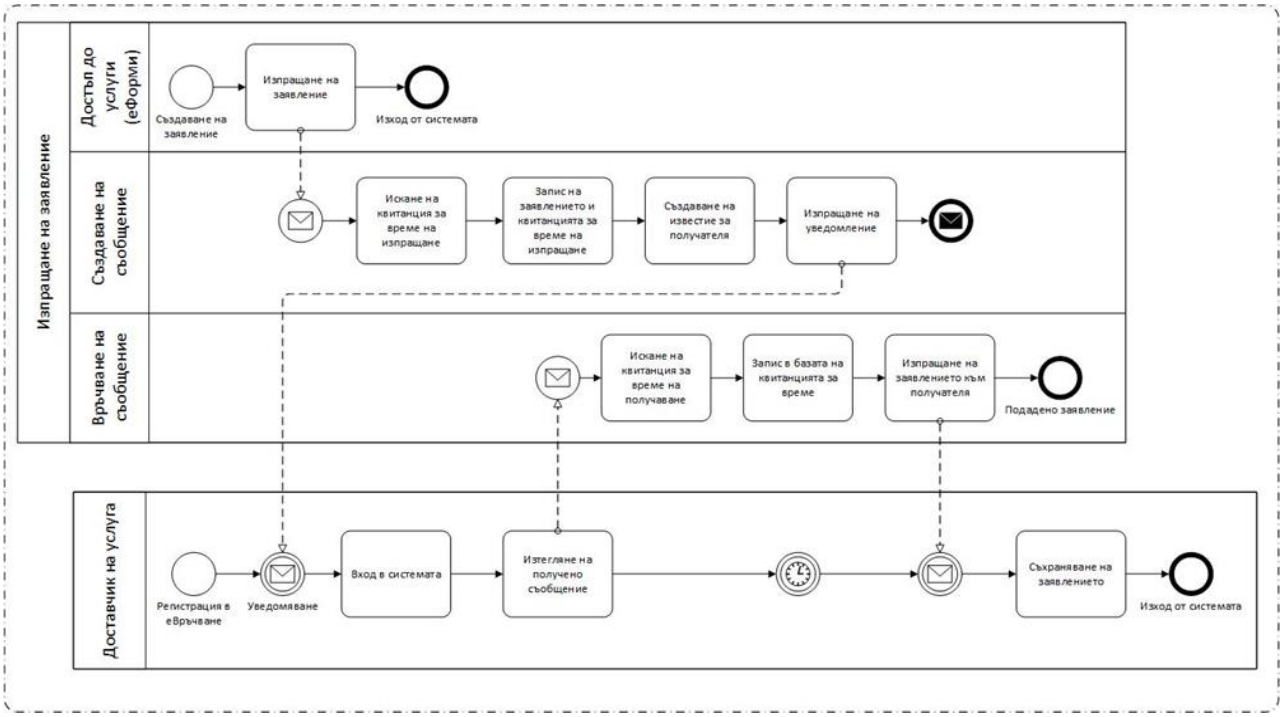
Схема на модела на взаимодействие на системата за електронни плащания

2.5. Система за електронно връчване

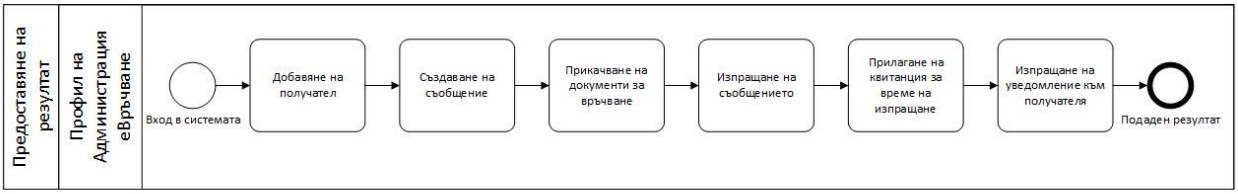
Системата за електронното връчване (е-Връчване) реализира изпращане, получаване и съхраняване на електронни документи за/от публични органи, физически и юридически лица, които са регистрирани и имат персонални профили. Чрез нея се предоставя услугата „електронна препоръчана поща“. Комуникацията чрез системата за е-Връчване замества класическия метод за доставка на писма.

Системата се интегрира със системата за е-Автентикация, интеграционната шина за обмен на справочна и удостоверителна информация и ИС на лица по чл. 1 от ЗЕУ, както и предоставя потребителски интерфейс за директно изпращане и достъп до съобщения, намиращи се в профилите на потребителите. Системата извършва известяване чрез електронна поща или SMS и дългосрочно съхранение на документи и информация за изпратени/получени документи и съобщения.

Документите и информацията относно изпратените/получените документи са защитени. Достъп имат само изпращачът и получателят, както и трети лица, на които получателят е предоставил възможност за достъп.



Процес по заявяване на услуга чрез „Електронна препоръчана поща“



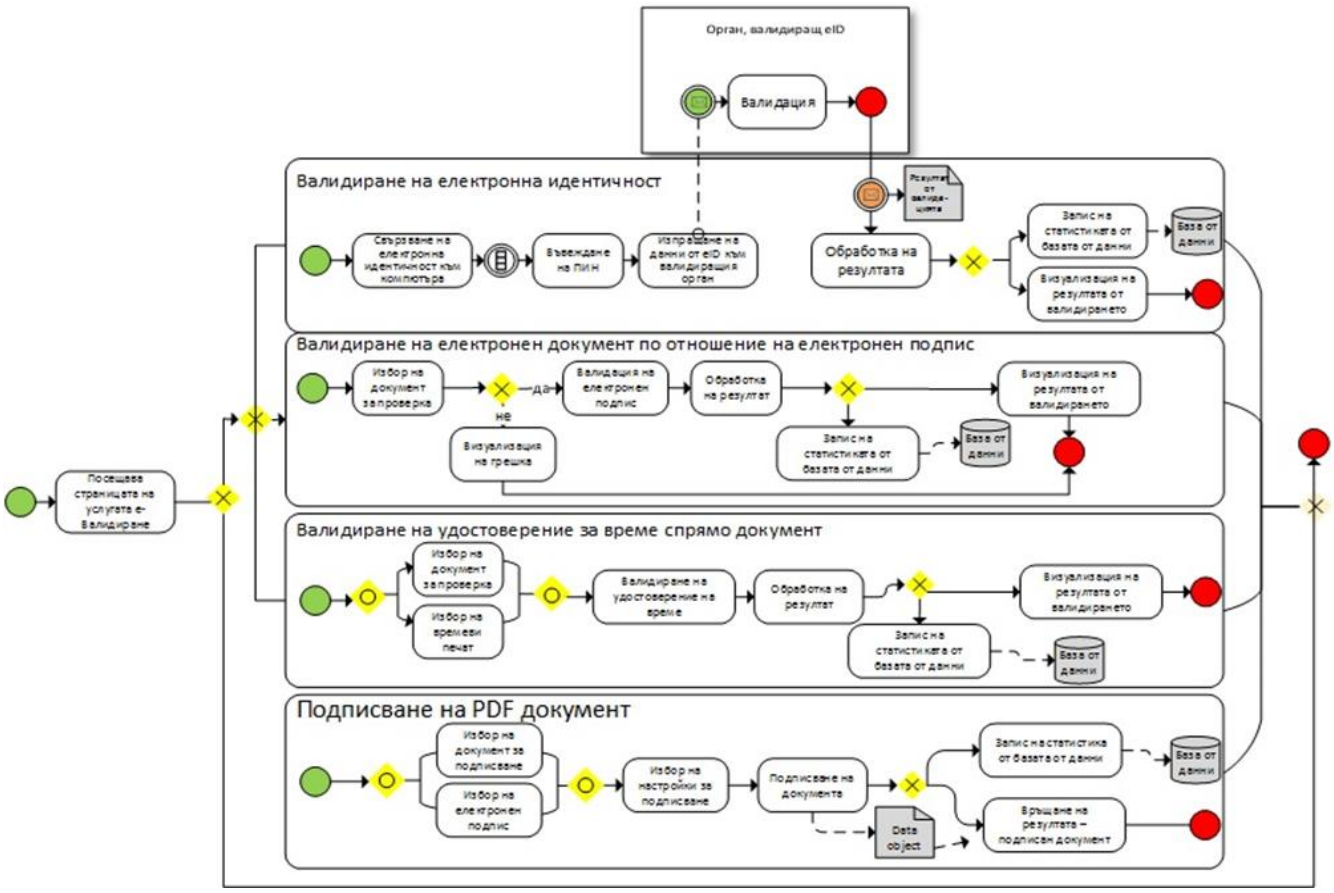
Предоставяне на резултат при липса на интеграция на АИС на доставчик на услугата със системата еВръчване

2.6. Система за е-Валидиране

Системата за е-Валидиране реализира проверка на валидността на персонален сертификат, с който е подписан електронен документ. Тя определя самоличността/идентификацията на автора, осигурява електронно подписване на електронен

документ (в регламентиран файлов формат) и управление на процеса по валидиране на електронно подписан електронен документ, от линк върху електронния документ.

Системата взаимодейства с интеграционния слой, като е достъпна чрез ЕПДЕАУ. Единният портал съдържа кратка информация и хипервръзка за заявяване на услугата за електронно валидиране по същия начин, по който са достъпни останалите електронни услуги.



Описание на процеса по е-Валидиране

2.7. Система за е-Форми

Системата за е-Форми осигурява създаване, редактиране и съхранение на електронни форми с възможност за последваща визуализация. Тя се интегрира с Административния регистър и реализира следните функционалности:

- избор на електронна услуга в зависимост от използваното средство за идентификация;
- визуализация и попълване на електронната форма, с която избраната услуга се заявява;
- извършване на формален контрол на въвежданата информация;
- автоматично попълване на вече налична информация (регистрирана в профила на потребителя), включително от външни регистри и бази данни;
- добавяне на допълнително изискуеми документи чрез техния избор и попълване или като сканирани такива;
- електронно подписване на документите, включително и допълнително изискуемите, когато това се изисква от процедурата по използване на услугата;
- потвърждение от заявителя;

- връчване на пакета документи в профила на доставчика на услугата заедно с генерирания атестат за автентикиран потребител;
- създаване и поддържане на хранилището на е-Форми;
- описание и изпълнение на работни процеси.

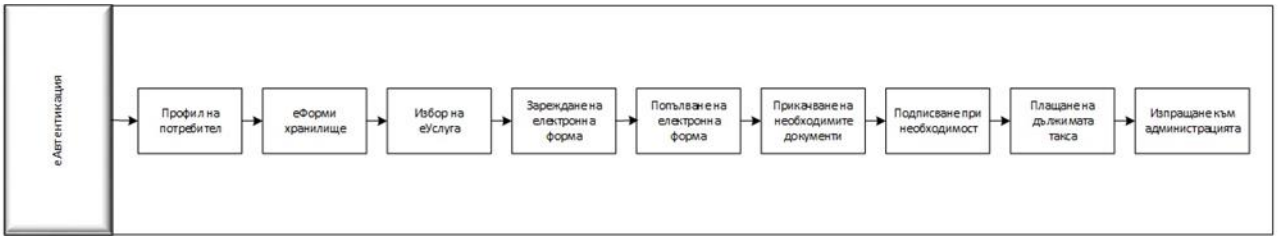


Схема на използването на е-Форми

2.8. Система за управление на потребителски профили

Потребителският профил е набор от данни, съхраняващ характеристиките на конкретен потребител на ЕАУ. Системата за управление на потребителски профили улеснява взаимодействието на потребителите с АО, независимо от мястото, където се намира, канала за достъп и времето на заявяване на услугата.

В системата са дефинирани следни групи потребителски профили:

- външни потребители;
- вътрешни потребители;
- овластени лица, регистрирани в регистъра на овластяването;
- администратори.

Системата има следните функционалности:

- групиране на профилите в роли в съответствие с функциите и дейностите, които се изпълняват;
- дефиниране на права за достъп за всяка група, в зависимост от установени политики за управление и нива на сигурност;
- персонализация на съдържанието на профила и на използваното средство за идентификация;
- извикване и попълване на електронна форма за регистрация или форма за промяна;
- съхраняване на документи, удостоверяващи изпращане на заявления, получаване на справочна информация и удостоверения, платежни документи и др.;
- запазване на информация за незавършени операции или други искания, очакващи да бъдат прегледани;
- поддържане на системен журнал на събития, свързани с потребителски профил;
- поддържане на справочник за атрибути, свързани с предоставяне на допълнителни характеристики;
- интеграция с външни регистри;
- интеграция с директорийна услуга за контрол и управление на достъпа до ресурсите на ЕУ;
- редактиране на профила от страна на потребителя;
- управление на личния е-Архив, достъп до съдържанието на създадени заявления за и получени отговори по е-услуги.

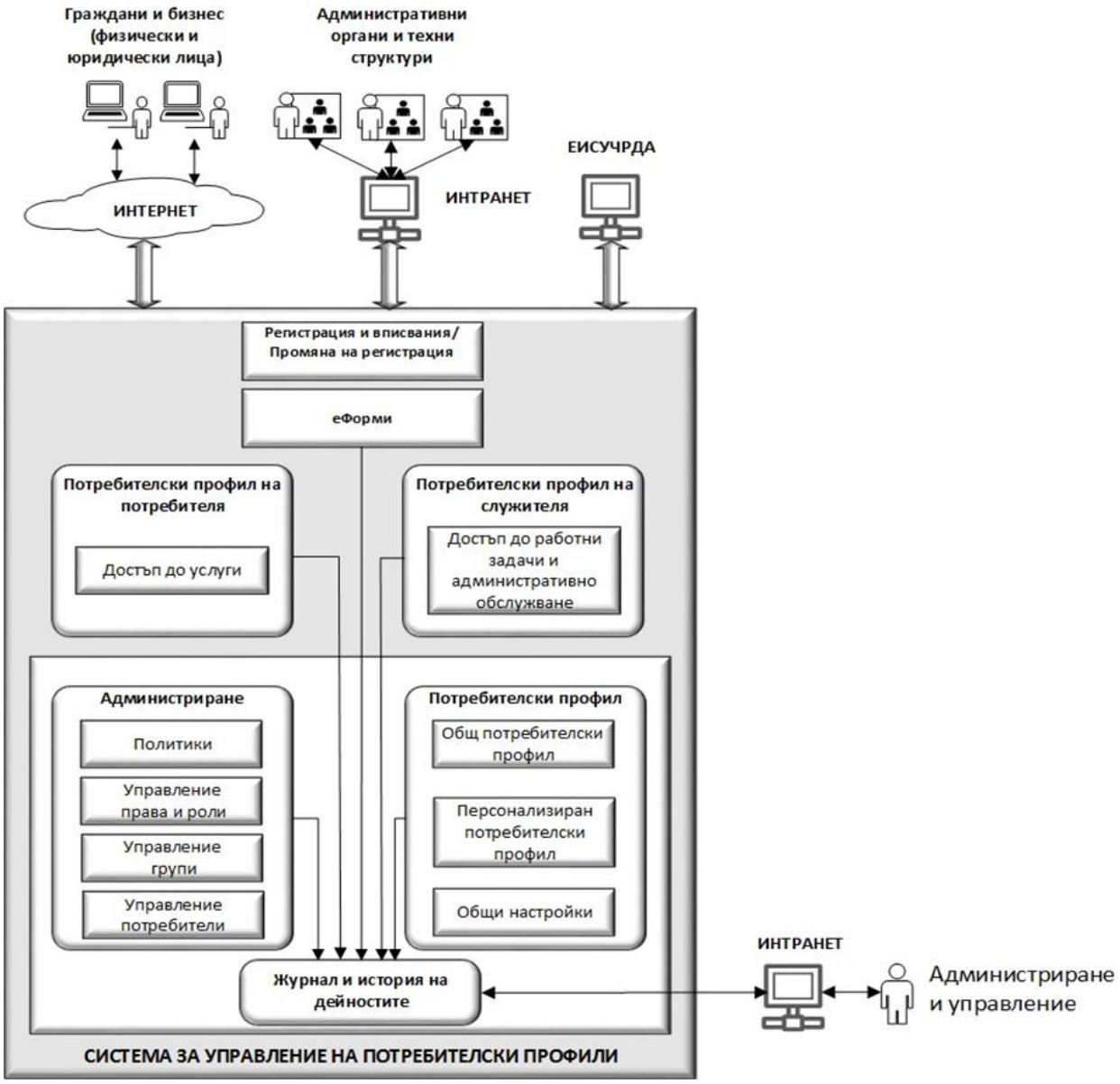


Схема на системата за управление на потребителските профили

2.9. Инфраструктура на публичния ключ

Инфраструктурата на публичния ключ е система за издаването, управлението, разпределението, използването, съхранението и отнемането на цифрови сертификати и реализира технология за проверка на автентичността на електронен документ с помощта на публичен ключ. Всички услуги, ресурси и системи, които изискват сигурност на работата с обменяната и обработваната информация, следва да се интегрират с инфраструктурата за управление на публичния ключ. От гледна точка на крайните потребители цифровите сертификати, които се изискват от системите, се създават на база комбинация публичен и частен ключ.

Инфраструктурата на публичния ключ осигурява:

- конфиденциалност;
- интегритет на данните;
- автентичност на данните;
- автентичност на потребителите;
- легитимация на наличните услуги и информация.

2.10. Система за поддържане на журнал на събития

Системата осигурява одитна следа за всички събития, свързани със заявяване и предоставяне или отказ на достъп до ресурс на електронното управление.

Функционалност на системата:

- регистриране на събития и съхраняване на история за достъпа до ресурс и извършени действия;
- обработка и анализ на събития и предоставяне на справки;
- възможност за уведомяване на лица при достъп до техни лични данни или информация, свързана с тях;
- предоставяне на интерфейс за външни ИС за интеграция със системата.

3. Централизирани системи за електронно управление

Централизираните системи за ЕУ са информационни системи, които се предоставят за споделено ползване на участниците в електронното управление.

3.1. Система за общински облачни услуги

Системата предоставя възможност за автоматизиране на процесите по заявяване, обработка и предоставяне на услуги. С една централизирана инсталация на системата могат да бъдат обслужвани всички общински администрации.

Достъпът се осъществява чрез интеграция на системата с е-Автентикация. Системата е интегрирана и със системите е-Плащане и е-Връчване и предоставя възможност за моделиране и интерпретиране на работни процеси, свързани с услугите.

3.2. Система за управление на собствеността

Системата предоставя възможност за поддръжка на регистри и бази данни, свързани с управлението на общинската и държавната собственост.

Функционалности на системата:

- въвеждане и съхраняване на данни за имоти, собственост на съответния АО;
- преглеждане на детайлите на записани имоти;
- редактиране на въведената информация за имоти в системата;
- търсене в списъка с въведени имоти;
- справки за записаните имоти;
- поддържане на следните регистри:
  - Регистър на общинската собственост;
  - Регистър на разпоредителни сделки;
  - Регистър на разрешителни;
  - Регистър на категоризираните обекти;
- интеграция със системите за е-Автентикация, е-Връчване и е-Плащане, както и с интеграционната шина за обмен на удостоверителна и справочна информация;
- интеграция с кадастър, имотен регистър и нотариална дейност при управление на собствеността;
- оценка на собствеността.

3.3. Единна информационна система за управление на човешките ресурси в държавната администрация

Единна информационна система за управление на човешките ресурси в държавната администрация (ЕИСУЧРДА) е информационна система, предоставяща набор от функции, чрез които се регламентират и администрират отношенията между организацията и служителя от назначаването му до прекратяване на неговите правоотношения.

3.4. Корпоративна електронна поща

Корпоративната електронна поща е създадена съгласно изискванията на НОИИСРЕАУ и дава възможност за: създаване на поддомейни за областните, общинските и районните администрации; проверка за идентичност на заявителя; проверка за редовност и допустимост; създаване и закриване на служебни електронни пощи.

Сайтът за връзка на областните, общинските и районните администрации със системата за Вътрешни електронни административни услуги – електронна поща в продукционна среда е https://veau.egov.bg.

3.5. Интегрирана информационна система на държавната администрация

Чрез Интегрираната информационна система на държавната администрация (ИИСДА) се поддържа и попълва информация на Административния регистър, годишния доклад за състоянието на администрацията и самооценката на административното обслужване. Административният регистър работи в интеграция с ЕИСУЧРДА**.**

3.6. Информационна система за управление и наблюдение на средствата от ЕС в България 2020

Информационна система за управление и наблюдение на средствата от ЕС в България 2020 (ИСУН 2020) е информационна система за управление, изпълнение и наблюдение на одобрените програми, съфинансирани от европейски структурни и инвестиционни фондове. Системата подържа модули за кандидатстване, управление на проекти и отчитане.

4. Децентрализирани ресурси на ЕУ

Децентрализираните ресурси са ИС, разработени в съответствие със специфични нужди на участниците в ЕУ, които са свързани с автоматизиране на конкретни функционални процеси или с изпълнението на специфични нормативни изисквания.

4.1. Общ модел на взаимодействие на АО с информационните ресурсите на ЕУ

Моделът описва взаимодействието между централизираните ресурси на ЕУ и децентрализираните ресурси на административните органи. Взаимодействието обхваща:

- интеграция с хоризонталните системи на ЕУ;
- използване на интегрирана облачна система (ДХЧО) за административни услуги и автоматизация на вътрешноведомствените работни процеси.

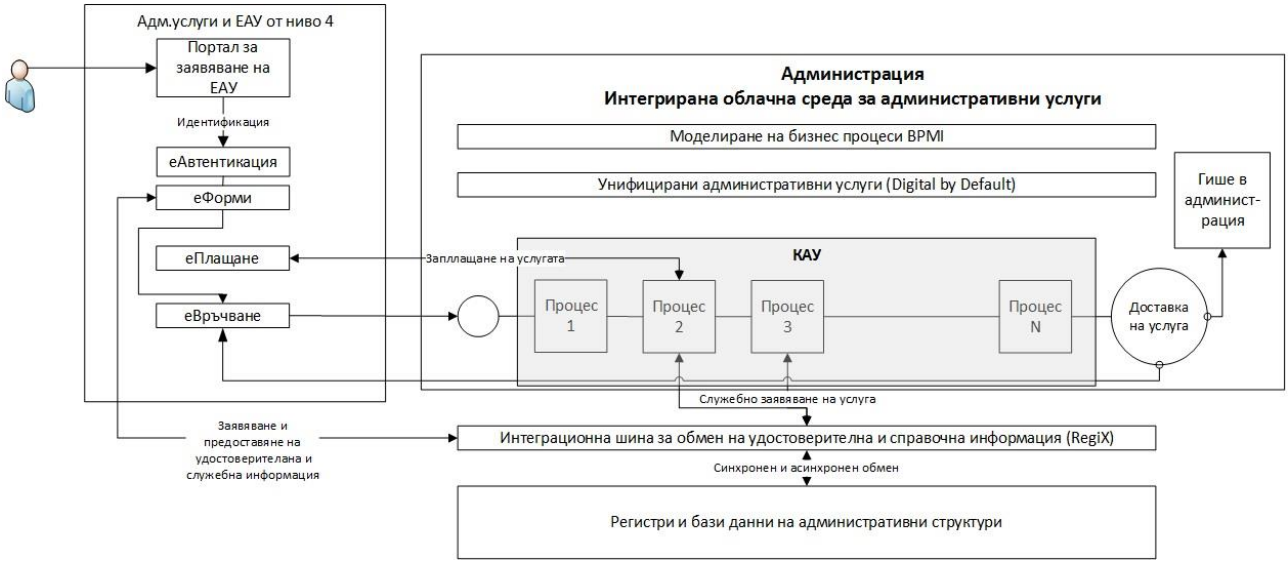


Схема на модела за преминаване на електронните услуги към ниво 4

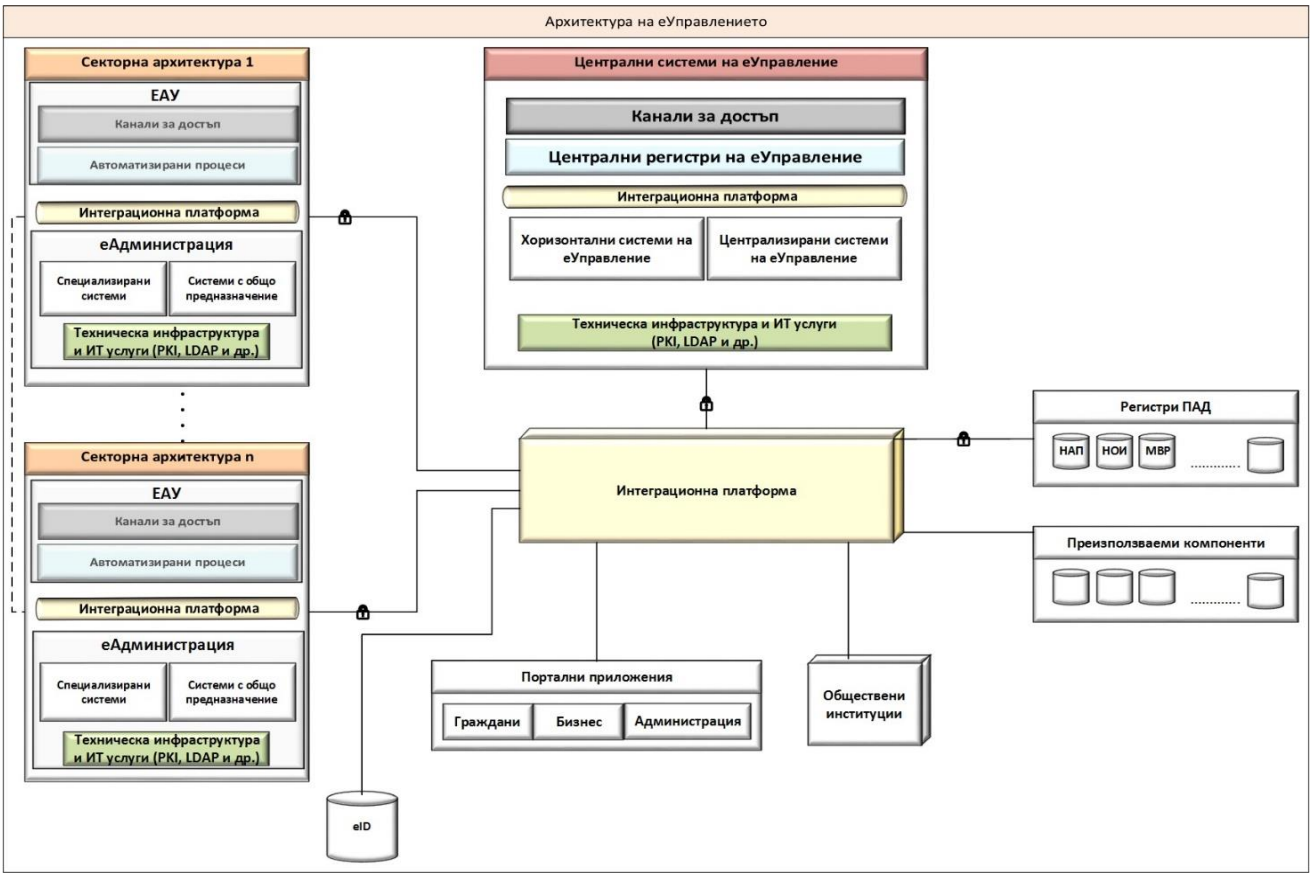
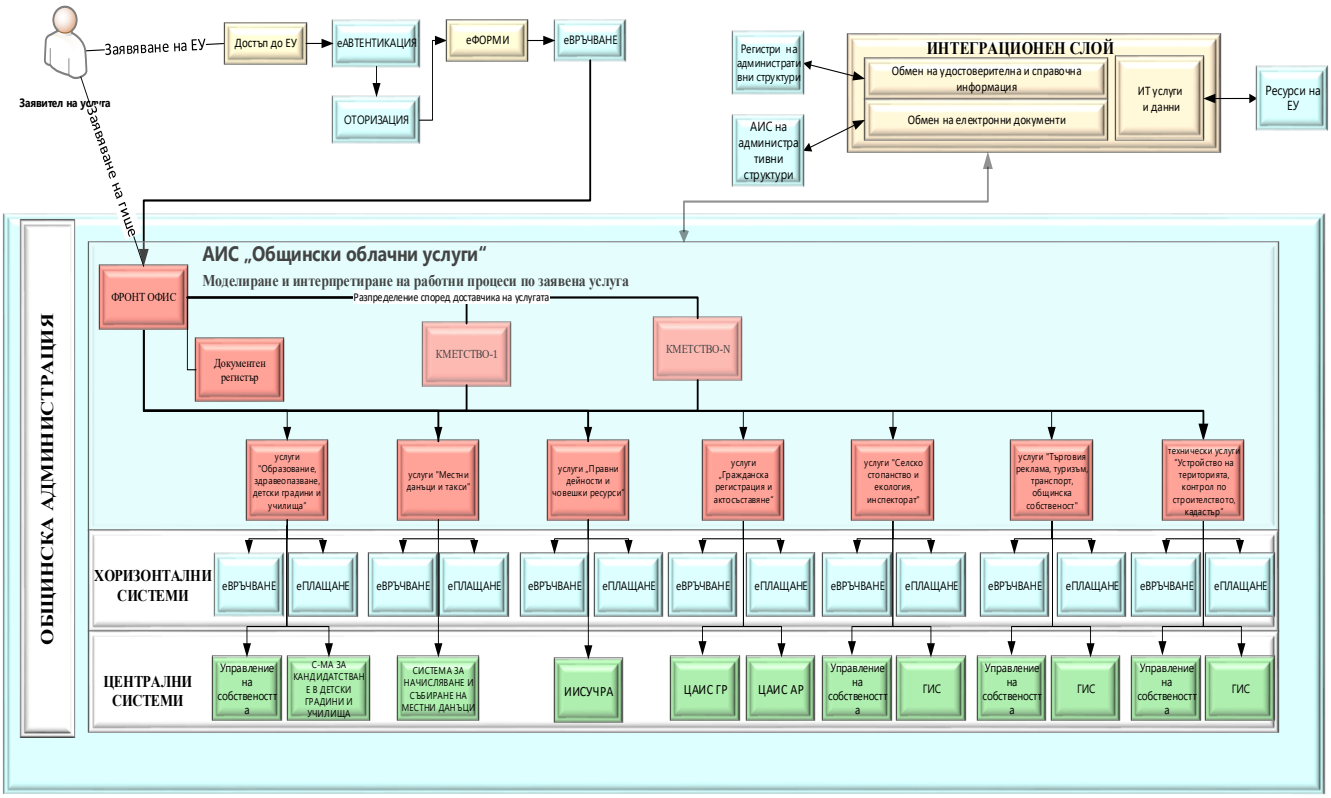


Схема на секторен модел на взаимодействие с централните системи на ЕУ

4.2. Модел на взаимодействие с общински администрации

За намаляване на административната тежест и облекчаване на процедурите при взаимодействие на гражданите с общинските администрации се предоставя възможност на гражданите и бизнеса да заявяват, заплащат и получават услуги по електронен път. Общинската администрация може да използва като средство за автоматизиране на процесите по обработка и предоставяне на електронни услуги автоматизираната информационна система „Общински облачни услуги“. Системата се интегрира с хоризонталните и централните системи на ЕУ и поддържа Единния модел за заявяване, заплащане и получаване на ЕАУ и реализиране на услуги, категоризирани като „епизоди от живота“ и „бизнес събития“.



Общински модел на взаимодействие

5. Интеграционни шини

Интеграционните шини предоставят съвременни средства чрез стандартизирани протоколи за взаимодействие, както между ресурсите на електронното управление, така и с външни за него ресурси, средства за контрол на достъпа до съответните ресурси, управление на натоварването и съхранение на информация, свързана с достъпа до ресурси.

5.1. Интеграционна шина за обмен на електронни документи

Шината осигурява условия за обмен на документи между участниците, вписани в регистъра на участниците, улеснява технологията на деловодната кореспонденция и спестява време и ресурси. Решението се характеризира с висока степен на ефективност, надеждност, сигурност и гъвкавост, което позволява обмен на електронни документи директно система-система или през централен компонент.

Всеки участник в обмена представлява крайна точка под формата на софтуерен компонент, който може да изпраща и получава електронни документи.

Регистърът на участниците поддържа актуални данни за участниците в обмена на съобщения, в т.ч. информация за участниците и техните крайни точки. Регистърът предоставя на участниците програмен интерфейс за извличане на информация за други участници, вписани в него, и интерфейс за актуализиране на информацията, съхранявана за него.

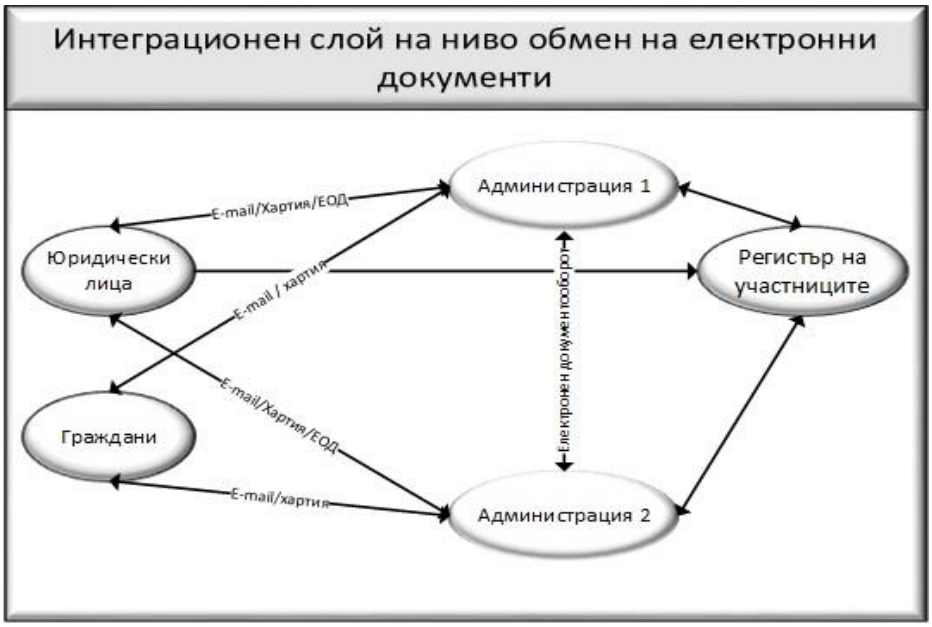


Схема на връзките на ниво обмен на електронни документи

5.2. Интеграционна шина за обмен на удостоверителна и справочна информация

Интеграционната шина за обмен на удостоверителна и справочна информация е реализирана чрез софтуерна система за автоматизиран достъп до данни от регистри – Regix. Основната функция на системата е заявяване от страна на правоимащи лица (консуматори) на удостоверителна и справочна информация от регистри и бази данни на ПАД и нейното предоставяне. Удостоверяването на консуматорите се извършва чрез генерирани от системата и предоставени им цифрови сертификати. Заявяването и предоставянето на информация може да се извършва в синхронен или асинхронен режим, в зависимост от работните процеси при доставчика. Генерираната информация се удостоверява чрез електронен и времеви печат от ПАД.

Използването на системата от лицата по чл. 1, ал. 1 и 2 от ЗЕУ е задължително при обмен на удостоверителна и справочна информация. Процесът по присъединяване, както и правата и задълженията на консуматорите, са част от утвърдените от председателя на ДАЕУ „Общи условия за достъп до данни от регистри на държавната администрация в средата за междурегистров обмен“.

Шината дава необходимата функционалност за разработка на комплексни административни услуги и предоставя ефективен начин за еднократно събиране и многократно използване на информация съгласно принципа на „Служебното начало“.

Консуматори на удостоверителна и справочна информация, съхранявана в регистри и бази данни на ПАД, могат да бъдат всички лица, имащи нормативно основание за заявяването и получаването ѝ. Заявяването и предоставянето на информация е в XML и DOCX формат.

Достъпът на консуматорите може да се реализира по два сценария:

- чрез интегриране на информационната система на консуматора;
- чрез използване на уеб базирано решение, инсталирано и поддържано от ДАЕУ.

Средата поддържа журнал на събитията, в който се записва информация за заявител, правно основание, момент на заявяване и идентификатор на обекта, за който е заявена информацията.

Интеграционните процеси са описани в документацията към системата и се намират на адрес https://www.e-gov.bg/bg/143.

5.3. Интеграционна шина за достъп и управление на ИТ услуги и данни

Интеграционната шина за достъп и управление на ИТ услуги и данни представлява единна точка за достъп до ресурсите и услугите на ЕУ. Шината позволява премахването на P2P връзките между системите и улеснява администрирането на ЕУ, трансформиране на протоколи и данни от един формат в друг, прилагане на политики, валидиране на интерфейси, оторизация на достъп и др. Тя дава възможност за оркестрация на сложни и паралелни процеси. Чрез нея се организира достъпът до централното хранилището на уеб услуги и се предоставя възможност за връзка с поддържаните централизирано номенклатури, класификатори и речници, до резервните копия на критични регистри и бази данни.

Реализирането на шината позволява:

- увеличаване на достъпността на уеб услуги, предоставящи достъп до регистри, номенклатури, класификатори, речници;
- репликиране на данните в инфраструктурата на Държавния хибриден частен облак (ДХЧО);
- разпределение на натоварване и отговорности при поддържане на критични регистри и бази данни;
- пакетиране на данни и предоставянето им за ползване в реално време;

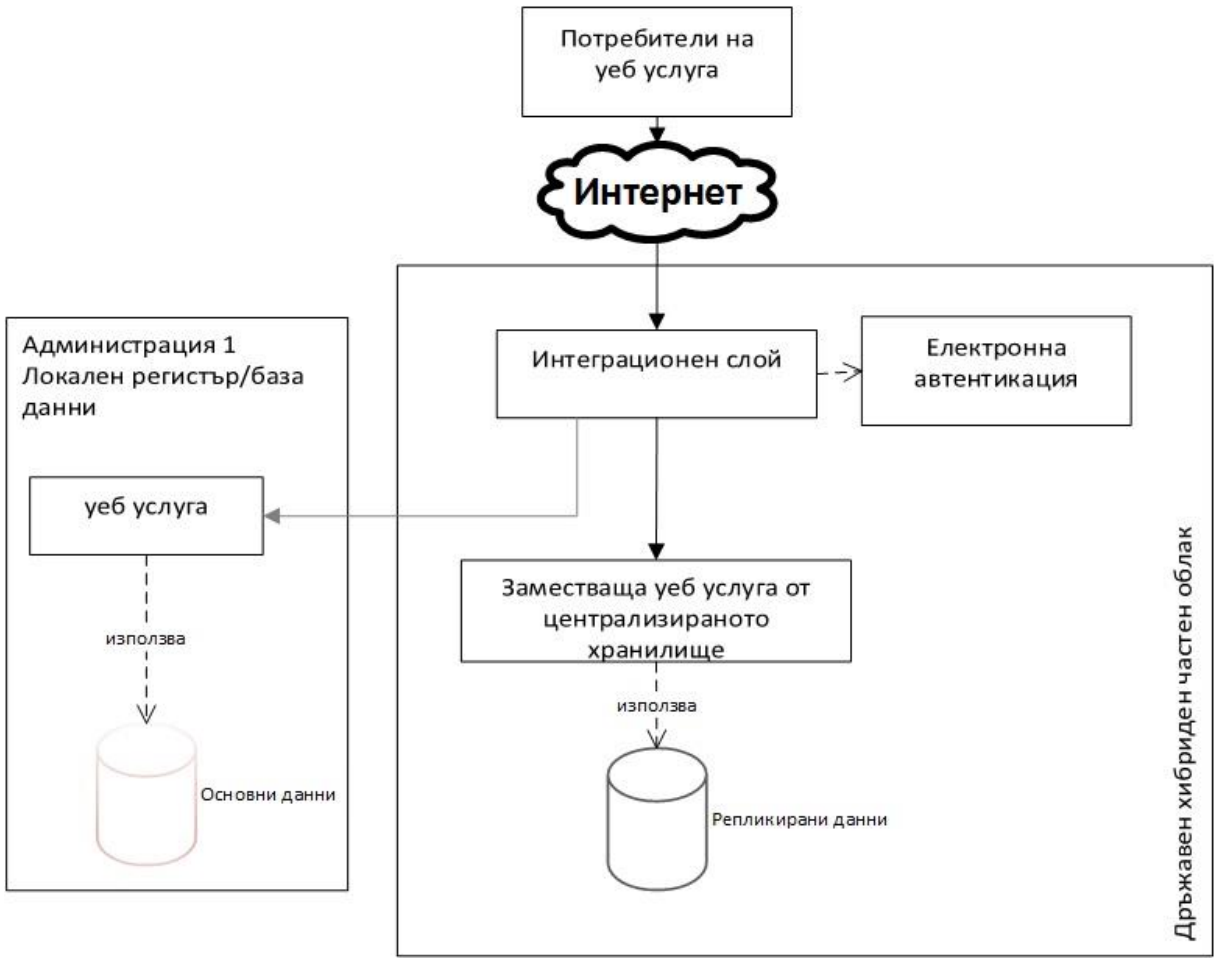


Схема на интеграция на уеб услуги с избор на оптимално маршрутизиране към регистър или към копие на регистър в ДХЧО

Интеграционният слой се грижи за синхронизиране на оригиналните и репликираните копия на данни.

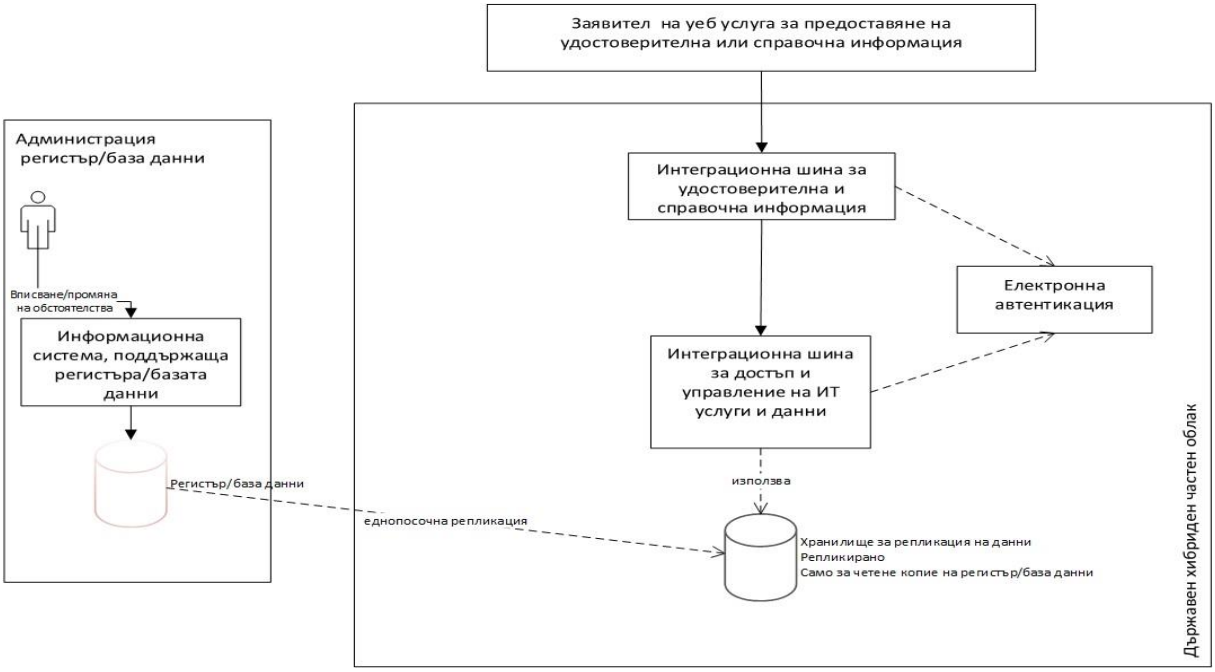


Схема на поддържането на критични регистри и бази данни

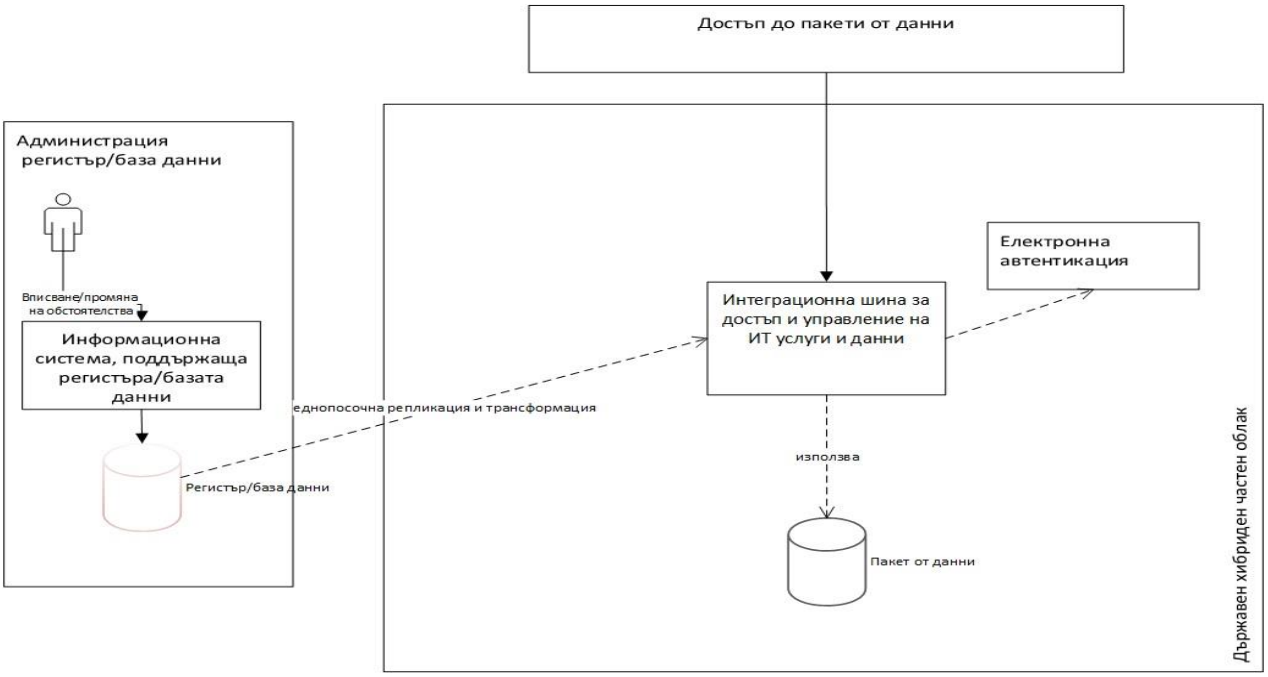


Схема на поддържането на пакети от данни и предоставянето им за ползване в реално време

6. Информационни системи

Информационна система (ИС) е организирана съвкупност от данни, дефинирани дейности по въвеждане, обработка и анализ на информация, методи и процедури, които осигуряват функционирането на АО с оглед постигането на предварително набелязани цели. Информационните системи са основата на автоматизираните системи за управление, които се реализират на базата на високотехнологично хардуерно и софтуерно оборудване. Информационната система се определя чрез данните и/или функциите, които поддържа.

В зависимост от обхвата и предназначението на предоставяните от тях е-услуги, собственик и начин на ползване, информационните системи, използвани от АО за целите на електронното управление, се разделят на:

- национални, на централни органи, или на местни органи на изпълнителната власт;
- фронт офис и бек офис системи;
- специализирани, с общо предназначение и поддържащи системи;
- централни и локални системи;
- хоризонтални, централизирани и децентрализирани системи;
- регистри и бази данни;
- автоматизирани и автоматични системи;
- трансакционни и аналитични системи.

Информационните системи са основните средства, с които се осигуряват процесите, свързани с ЕУ. При тяхната разработка, експлоатация и развитие задължително се спазват заложените стандарти, изискванията за оперативна съвместимост и мрежова и информационна сигурност.

При разработването, развитието и поддържането на информационни системи трябва да се спазват следните изисквания:

- да отговарят на принципите на архитектура, ориентирана към услуги;
- да се базират на отворени технологии и актуални стандарти;
- информационните системи за изпълнение на административни услуги да бъдат достъпни през уеб услуги, като се спазват изискванията за оперативна съвместимост по отношение на стандарти, стандартизирани интерфейси и протоколи, вписани в Регистъра на стандартите;
- информационните обекти се вписват от собствениците на системите в процеса на тяхното проектиране, разработване или експлоатация;
- да поддържат обекти от Регистъра на информационните обекти;
- да съхраняват само идентификаторите на обекти, които вече се съхраняват в регистрите на ПАД, с изключение на обектите и данните, които са необходими за оперативната работа на системата при доказана необходимост, по преценка на ДАЕУ;
- да използват пакетите от данни, дефинирани в РОС и достъпни чрез унифицирани уеб услуги, предоставени от собственика;
- да осигуряват достъп и чрез най-често използваните мобилни устройства;
- да използват интеграционния слой при достъп до ресурсите на електронното управление;
- не се разработват функционалности, които вече са налични в централизираните системи или се предоставят от хоризонталните системи;
- не се разработва функционалност, ако вече такава е налична в друга система и е възможно нейното ползване като споделен ресурс. При необходимост от разширяване на функционалността се разширява тази на споделения ресурс. Нова ИС с необходимата функционалност се разработва само при липса на споделен ресурс, който да предоставя такава, като същата се включва като споделен ресурс, част от ресурсите на електронното управление;
- задължително да притежават интерфейс, чрез който да предоставят информация на журнала на събитията при достъп до ресурсите на ЕУ;
- при изграждането на ИС да се прилага единен подход – всеки проект за ИС да спазва изискванията на архитектурата и да се реализира като част от единна система, осигурявайки съвместимост и недопускане на дублиране на задачи в различните проекти.

Информационните системи се характеризират с жизнен цикъл. Това е управляем процес, който обхваща етапите от вземане на решение за създаване на информационната

система, нейното проектиране, реализация и внедряване, експлоатация и поддръжка, развитие и обновяване до извеждането ѝ от експлоатация.

Собственикът на ИС, с цел гарантиране на нейната работоспособност и достъпността на предоставяните чрез нея услуги, е необходимо да я обезпечи ресурсно с поддръжка до извеждането ѝ от реална експлоатация. За всяка ИС е нужно да се разпишат в процедура необходимите ресурси, отговорностите на лицата и действията, свързани с нейното изграждане, поддръжка и развитие.

Всяка ИС в обхвата на ЕУ следва да спазва изискванията за изграждане, поддръжка и развитие, посочени в настоящата архитектура. Наличните ИС следва да бъдат приведени в съответствие с архитектурата, в зависимост от тяхната значимост и критичност по отношение на ЕУ. Председателят на ДАЕУ издава предписания за привеждане на системите на горепосочените лица в съответствие с архитектурата и с правомощията си по ЗЕУ.

Всяка експлоатирана, надграждана или разработвана ИС, която използва ресурсите на електронното управление, трябва да е удостоверена за съответствие с изискванията на нормативната уредба и архитектурата. Съответствието се удостоверява с вписването ѝ в списъка на удостоверените системи.

Повторно използваеми Модули

Модулите са обособени ИС, които предоставят функционалност или група от функционалности и могат да функционират както самостоятелно, така и да се вграждат в други модули или системи. Те са информационно-технологична предпоставка за оптимизирането на работните процеси и взаимодействието и интеграцията с други системи.

Модулите се характеризират с:

- функционално разделяне на отделни самостоятелни преносими елементи, мащабируеми и за многократна употреба;
- използване на строги, добре дефинирани модулни интерфейси, включително обектно-ориентирани описания;
- съкращаване на времето за разработка чрез прилагане на стандартизирани решения и готови функционалности.

При разработването на ИС задължително се използват наличните модули, предоставящи необходимата функционалност. Когато за нуждите на ИС е необходима функционалност, която не се предоставя изцяло от конкретен модул, то задължително се разширява неговата функционалност. Разработването на нов модул се извършва само и единствено когато липсва модул с необходимата функционалност. Модулите се съхраняват в хранилище, като за всеки се поддържа версия.

7. Регистри

Регистърът е структурирана база данни, чието предназначение е да съхранява и да бъде доверен автентичен източник на данни, за който съществува нормативно основание и нормативно определен ред за вписване, заличаване и/или удостоверяване на обстоятелства.

7.1. Регистри за първични данни

Те съхраняват само първични данни и се поддържат от лица по чл. 1 от ЗЕУ и в съответствие с нормативно вменените им правомощия и при спазване на правилата за сигурност и защита на данните. Регистър на ПАД не трябва да съхранява информация от друг регистър. При необходимост същата се достъпва чрез връзка към друг регистър.

Всеки регистър трябва да използва уникални идентификатори на физическите лица, които да не се използват от друг регистър. ДАЕУ осигурява защитени средства за създаване и

предоставяне на съответствие между различните идентификатори от различните регистри, свързани с едно и също физическо лице.

Вписването и промяната на обстоятелствата в регистрите се извършват чрез ИС на първичните администратори на данни, отговарящи на изискванията на архитектурата и нормативната база.

Предоставянето на справочна и удостоверителна информация се извършва чрез интеграционната шина за обмен на удостоверителна и справочна информация на оторизирани за това АО и лица.

Всяко действие по вписване и промяна на обстоятелство, предоставяне на удостоверителна и справочна информация, задължително се вписва в журнал на събитията. Така се предоставя възможност за уведомяване в реално време на собственика на данните по предпочитан от него канал.

7.2. Централни регистри на ЕУ

- Регистър на информационните ресурси;
- Регистър на овластяванията;
- Регистър на проектите и дейностите;
- Регистър на участниците в електронен обмен на документи;
- Регистър на обектните идентификатори;
- Регистър на ресурсите;
- Адресен регистър;
- Регистър за гражданска регистрация.

7.3. Регистрова реформа

Състоянието на регистрите на АО като основен елемент от архитектурата на ЕУ за предоставяне на електронни услуги налага провеждането на цялостна реформа на модела на организация и поддържане на регистрите в държавната администрация, която да гарантира ефективния обмен на данни.

Регистровата реформа трябва да осигури:

- намаляване на броя на регистрите, като регистрите в една и съща тематична област се обединят;
- оптимизиране на организацията на регистрите на държавната администрация с цел поддръжката им с минимални разходи и предоставяне на качествени услуги;
- преминаване към изцяло цифров вид на всички регистри в администрацията, с изключение на изрично предвидените със закон;
- разширяване броя на регистрите, присъединени към Средата за междурегистров обмен и броя на администрациите, получили достъп до Средата;

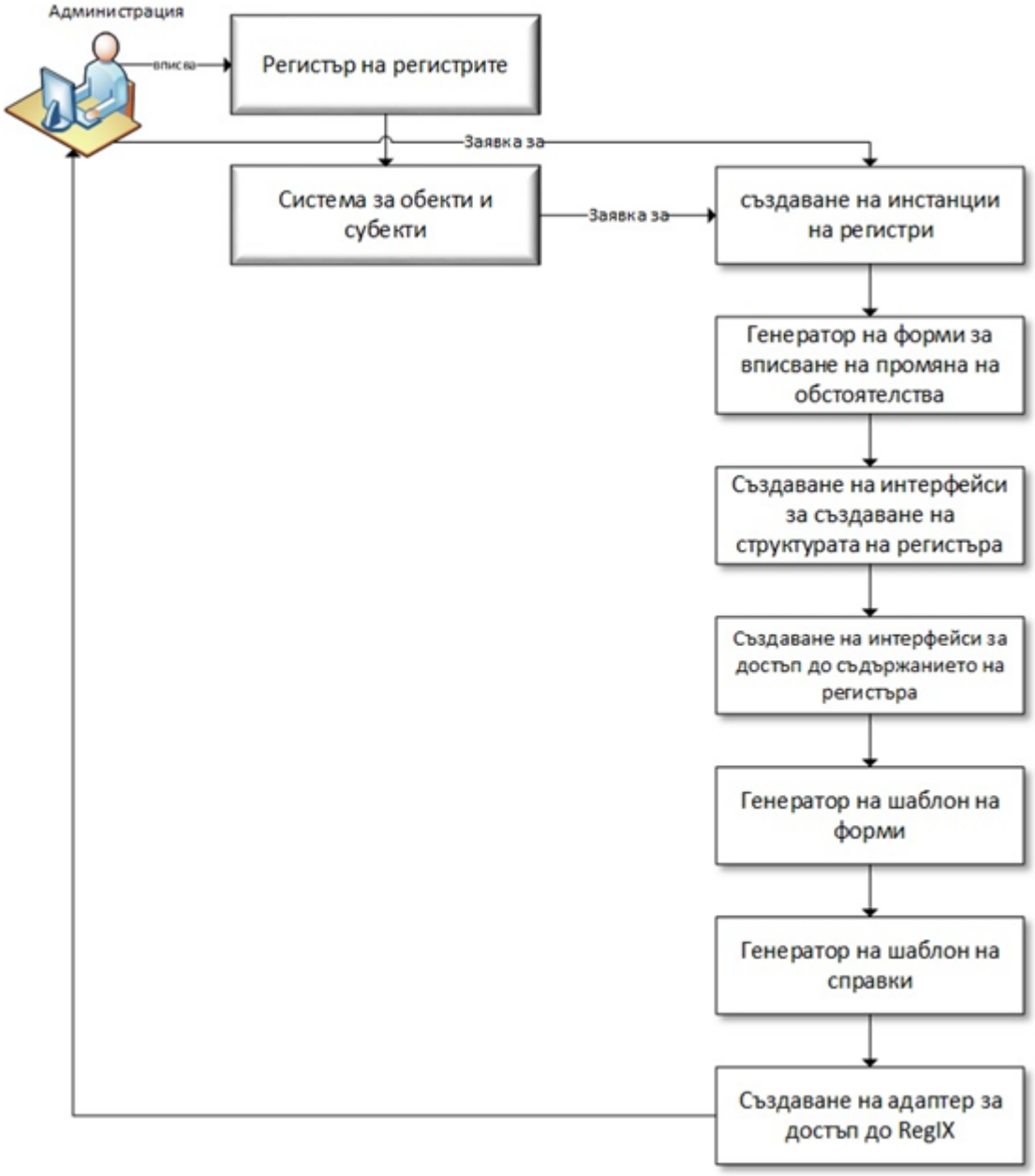
Всички администрации, които изискват данни, налични в публични регистри, трябва да променят съответната нормативна уредба, така че да отпадне изискването за предоставяне на документи или данни, налични в публични регистри.

8. Базов регистър на субекти, обекти и събития

Базовият регистър е информационна multi-tenant система, в която всеки АО може да създава среда за поддръжка на регистър (вписване, промяна и удостоверяване на обстоятелства, генериране на справки и др.), който вече е вписан в Регистъра на регистрите и отговаря на изискванията за оперативна съвместимост. Системата представлява „регистър като услуга“. Чрез интеграционния слой се осъществява достъп до ресурсите на електронното управление, включително до средствата за достъп и обмен на информация.

Системата изпълнява следната функционалност:

- поддържане на интерфейси, специфични за всеки регистър, чрез които се поддържат основните функции по вписване, промяна и удостоверяване на обстоятелства;
- псевдонимизиране при необходимост на съхраняваните лични данни;
- възможност за водене на регистъра едновременно от различни длъжностни лица от един и същи административен орган, които са оторизирани чрез системата за е-Оторизация;
- поддържане на синхронизация при въвеждане и редактиране на информация;
- автоматично предоставяне на данни в отворен формат, включително и в реално време;
- интеграция с интеграционния слой за обмен на удостоверителна и справочна информация;
- поддържане на одитна следа на всяка операция и интеграция със системата за поддръжка на журнал на събития;
- безконфликтно, поетапно добавяне на новосъздадените регистри чрез интерфейсите на системата.



Функционална схема на системата за създаване на обекти, субекти и събития

9. Данни и метаданни

Данните са най-критичният ресурс на електронното управление. От наличността, достоверността и защитеността на данните зависи функционирането на електронното управление и доверието на гражданите и бизнеса.

Лицата по чл. 1 от ЗЕУ са задължени да събират, обработват и предоставят данни само и единствено във връзка с нормативно определените им правомощия.

Първичните администратори на данни задължително поддържат и съхраняват данните в необходимото количество и качество, в машинночетим формат, в съответствие с принципите за оперативна съвместимост. ПАД създават условия и процедури, които предоставят възможност на всяко заинтересовано лице да провери и изиска корекция на данни, които се отнасят до него.

Архивирането е последната фаза от жизнения цикъл на данните и предполага преминаване на данните от активни в неактивни. Архивирането може да се извършва от ПАД при спазване на разработени от него вътрешни процедури или ползване на външна услуга, предоставяна от ДАЕУ.

Управлението на е-архивиране като услуга е важна част от управлението на жизнения цикъл на данните като споделена функционалност, позволяваща постоянното или дългосрочното съхранение на избрани електронни документи или информация. Услугите за съхранение на данни и приложения обхващат: достъп, възстановяване, запазване, съвместимост на ресурсите за съхранение, управление на риска и др.

Целите на електронното управление налагат поетапна промяна на модела на съхранение на данните от децентрализиран към централизиран, като се започне с най-критичните за електронното управление масиви от данни. За съхранение на данни се използват предоставени от средствата за съхранение на информация дискови пространства. Инфраструктурата, върху която се оперира с данните, трябва да бъде резервирана по начин, гарантиращ работоспособност 24/7. Върху нея трябва да се мигрират или да се разположат копия на най-критичните бази данни, поддържани от ПАД. Данните трябва да се достъпват директно през ИС на ПАД или чрез интеграционния слой.

Налагането на централизирания модел ще доведе до чувствително намаляване на разходите за лицензи за СУБД, мащабируемост на изчислителните ресурси, повишаване нивото на сигурност, контрол и наблюдение върху достъпа и разпространението на данни.

Метаданните описват характеристиките на данните с по-високо ниво на абстракция и са критични за интерпретиране на данните, които описват. Те се разделят на три категории:

- служебни метаданни – използват се от приложенията за отчети, служебни анализатори и от крайни потребители за подпомагане на локализирането, разбирането и оценката на информация в средата на администрацията;
- технически метаданни – използват се от администратори и разработчици и включват информация за първоначалните данни, целевите данни и правилата за извличане, филтриране, разширение, почистване и преобразуване на първоначалните данни в целеви данни;
- операционни метаданни – използват се главно от разработчици и включват информация относно статистиките за хода на работата, дати, часове и др.

IV. ТЕХНОЛОГИЧНА АРХИТЕКТУРА

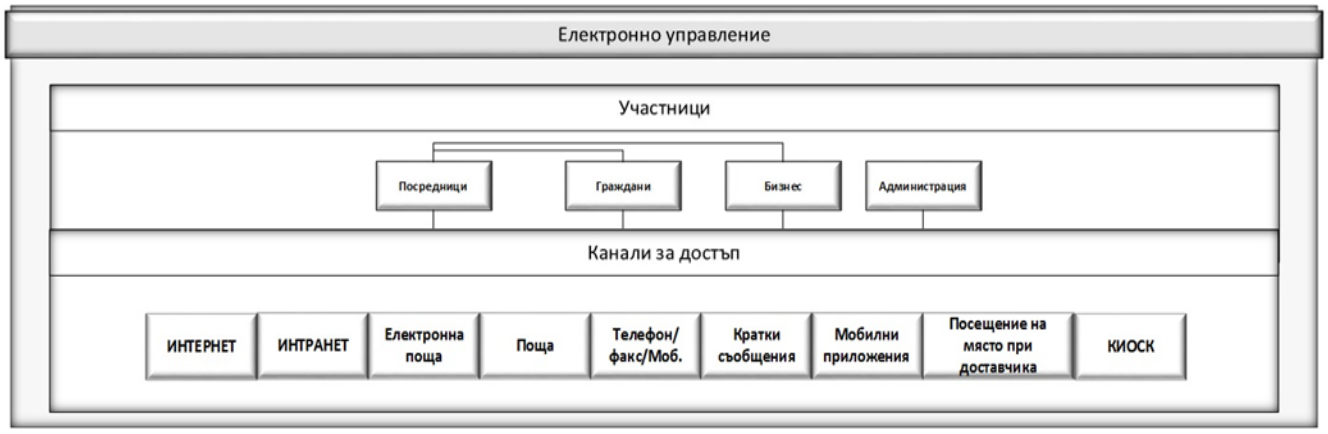
Технологичната архитектура дефинира средствата, системите, информационната и техническата инфраструктура, използвани за функционирането на всички изброени по-горе

информационни ресурси и които осигуряват надеждна, защитена и устойчива среда за предоставяне на услугите на ЕУ в непрекъснат режим. Тя включва:

1. Канали за достъп

Каналите за достъп до ЕАУ са средство за осъществяване на еднопосочна или двупосочна комуникация за взаимодействие между участниците в ЕУ при заявяване и предоставяне на ЕАУ. Каналите за достъп трябва да гарантират високо ниво на достъпност, сигурност и качество и да отговарят на изискванията за оперативна съвместимост.

Каналите за достъп изразяват нуждите и отговарят на изискванията на потребителите, които са определящи при планирането и разработването на ЕАУ.



1.1. Уеб канал за достъп

Уеб каналът за достъп е каналът, чрез който се достъпва ЕПДЕАУ, като единна входна точка от Интернет/Интранет към ЕАУ, където потребителите се идентифицират по различни способи и с различни средства.

1.2. Нотификационни механизми

За предоставянето на различни нотификации и услуги, свързани с тях, се използват различни механизми за уведомяване на участниците. В процеса на предоставяне на е-услуги системите или съответните служители от администрацията уведомяват потребителите за различни събития, настъпили в хода на предоставяне на е-услугите, по електронна поща, телефон, SMS, факс.

1.3. Изнесени общи точки за административно обслужване

Изнесени общи точки за административно обслужване се изграждат, като се използват вече налични мрежи. Те предоставят достъп на гражданите и бизнеса до административни услуги чрез ресурсите на електронното управление. Целта им е да се освободят АО от неприсъщите им дейности по директно обслужване на гражданите и бизнеса на място, свързани със съществен разход на ресурси за всеки АО поотделно.

1.4. Посредници

ЗЕУ създава възможност електронните услуги да бъдат заявени и чрез посредник. Посредникът е овластен да заяви от името на и за сметка на заявителя ЕАУ.

1.5. Киоск

Специализирано терминално устройство, чрез което се предоставя възможност в реално време за заявяване, заплащане и предоставяне на ЕАУ.

1.6. Мобилни устройства

Предлагане и предоставяне на ЕАУ чрез инсталирани приложения на мобилни устройства, посредством които е възможно заявяване, заплащане и предоставяне на ЕАУ.

2. Електронна идентификация

Електронната идентификация (ЕИ) е процес на използване на данни в електронна форма за идентификацията на лица. Предоставянето на електронни услуги изисква наличието на средство (или средства) за правно призната ЕИ за сигурно установяване и проверка на самоличността на гражданите от разстояние.

Електронната идентификация осигурява:

- надлежно взаимодействие по електронен път между гражданите, бизнеса и публичните органи;
- увеличаване на ефективността и ползването на ЕАУ;
- правна сигурност при електронните трансакции;
- облекчаване на административната тежест;
- достъп до трансгранични онлайн услуги.

2.1. Национална схема за ЕИ

Основополагащ елемент за електронното управление е схемата за ЕИ, уредена в ЗЕИ.

Съгласно нея физическите лица се идентифицират в електронна среда чрез електронен идентификатор, който се съдържа в удостоверение за електронна идентичност и се осигурява възможност за физическите лица да използват издаденото им удостоверение за електронна идентичност при заявяването на всички електронни административни услуги, за предоставянето на които по закон се изисква идентификация.

Субекти в схемата са: органът за ЕИ, който е издател на удостоверенията за електронна идентичност, помощни органи (администратори на електронна идентичност) и центровете за ЕИ.

2.2. Налични средства за ЕИ

До въвеждането на националната схема за ЕИ се използват няколко средства за идентификация с различна степен на осигуреност – квалифициран електронен подпис, различни персонални кодове (ПИК, УКД), потребителско име и парола. Те следва да бъдат интегрирани със системата за е-Автентикация.

В срок от една година след въвеждането на националната схема за идентификация, освен по реда на ЗЕИ и други методи определени със закон, може да се прилага и прочитане на уникален идентификатор от квалифициран електронен подпис.

В срок от три години от въвеждането на националната схема за идентификация при заявяването на електронни административни услуги може да се използва и персоналният идентификационен код, издаван от Националната агенция за приходите или Националния осигурителен институт, както и уникалният код за достъп, издаван от Националната здравноосигурителна каса, след интеграцията им със системата за е-Автентикация.

2.3. Частни средства за електронна идентификация

Регламент (ЕС) 910/2014 допуска да бъде нотифицирана национална схема, при която средствата за ЕИ се издават от частния сектор, при условие тези средства да са признати от държавата, но ЗЕИ не предвижда други методи освен националната схема, при която средствата за ЕИ се издават от държавата.

2.4. Трансгранична електронна идентификация

Една от целите на Регламент (ЕС) 910/2014 е да се премахнат съществуващите бариери пред трансграничната употреба на използваните в отделните държави членки средства за ЕИ, за да се гарантира, че при достъпа до трансгранични електронни услуги, предлагани от държавите членки, е възможно да се осъществят сигурна ЕИ и сигурно електронно удостоверяване на автентичност на гражданите на ЕС.

ДАЕУ осигурява интеграция на информационните системи на АО с тези на държавите членки на ЕС с цел създаване на възможност за предоставяне на трансгранични електронни административни услуги.

Държавите членки задължително признават средствата за електронна идентификация, издадени в друга държава членка в рамките на схема за електронна идентификация, за която е извършено уведомяване и която отговаря на изискванията на регламента. За да се реализира взаимно признаване, е необходима национална технологична инфраструктура, която да осигури надеждно трансгранично удостоверяване на автентичност и да гарантира оперативната съвместимост със схемите за електронна идентификация, за които е извършено уведомяване. Централен компонент на тази инфраструктура е **eIDAS** възелът, който участва в трансграничното удостоверяване на автентичността на гражданите. Чрез него се приемат, обработват и препращат данни към други възли, с което се дава възможност на националната инфраструктура за електронна идентификация на една държава членка да се свързва с инфраструктурата на други държави членки.

3. Споделени ресурси на ЕУ

Споделените информационни ресурси на електронното управление представляват стандарти, протоколи, интерфейси, софтуерни продукти и оборудване, както и инженерно-технически съоръжения, които осигуряват сигурната и надеждна работа на информационните системи и регистри. Основните им компоненти включват софтуерни платформи, сървъри, пространство за съхранение на данни и приложения за тяхното управление, комуникационни мрежи и инженерно-технически съоръжения, осигуряващи разполагането на оборудването. Те формират физическата среда за събиране, обработка, съхранение и разпространение на информацията, свързана с ЕУ. Споделените ресурси се изграждат и развиват от ДАЕУ и се използват споделено от всички държавни органи.

Обща архитектура на споделените информационни ресурси

Споделените ресурси на ЕУ осигуряват:

- централизиране на информационните ресурси на ЕУ в няколко локации, отговарящи на изискванията за физическа, мрежова и информационна сигурност;
- защитена комуникационна среда за нуждите на ЕУ;
- икономия на инвестиции и поддръжка на хардуер и софтуер, режийни разходи и разходи за персонал;
- подобряване на предоставянето на електронните услуги и повишаване на прозрачността на управлението.

Споделените информационни ресурси на ЕУ се състоят от:

- Държавния хибриден частен облак (ДХЧО);
- Хранилището за данни на електронното управление;
- Центровете за данни;
- Единната електронна съобщителна мрежа на държавната администрация;
- Съобщителните обекти;
- Инженерно-техническата инфраструктура.

Споделените ресурси са гръбнакът на ЕУ и критичен фактор за реализацията на всички е-услуги.

3.1. Центрове за данни

Центровете за данни са инженерно-технически съоръжения, предназначени да осигуряват информационни ресурси за нуждите на ЕУ с високо ниво на наличност и сигурност. Инфраструктурата на всеки център за данни се състои от две основни групи компоненти: компоненти на инженерно-техническата инфраструктура и ИКТ компоненти.

Първата група компоненти включва сградния фонд, резервирано електрозахранване, климатизация, инфраструктурно окабеляване, апаратни шкафове, пожароизвестяване, пожарогасене, наблюдение, контрол на достъпа и др.

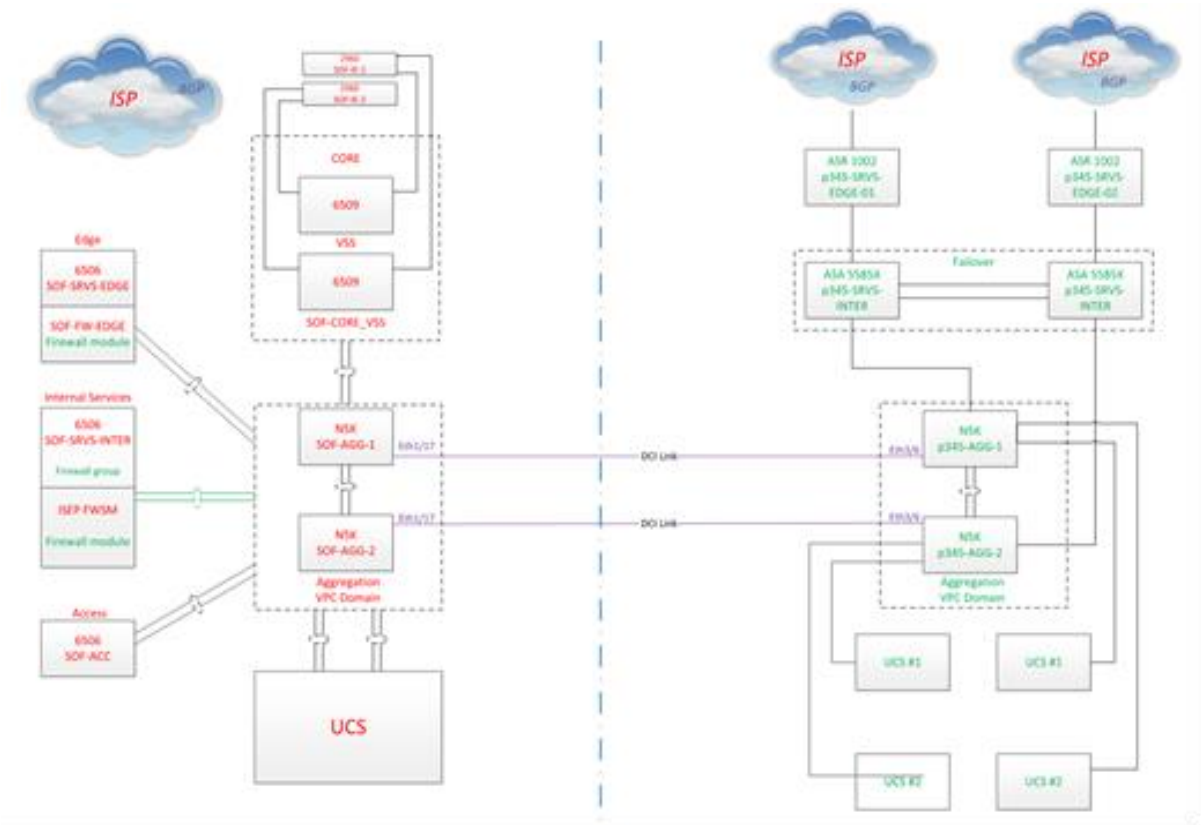
Втората група компоненти се формира от изчислителен ресурс, дисково пространство, компютърни мрежи, компонентите за информационна сигурност, средства за виртуализация и средства за автоматизиране и управление на процесите.

Информационните компоненти на споделените информационни ресурси се разполагат в няколко центъра за данни:

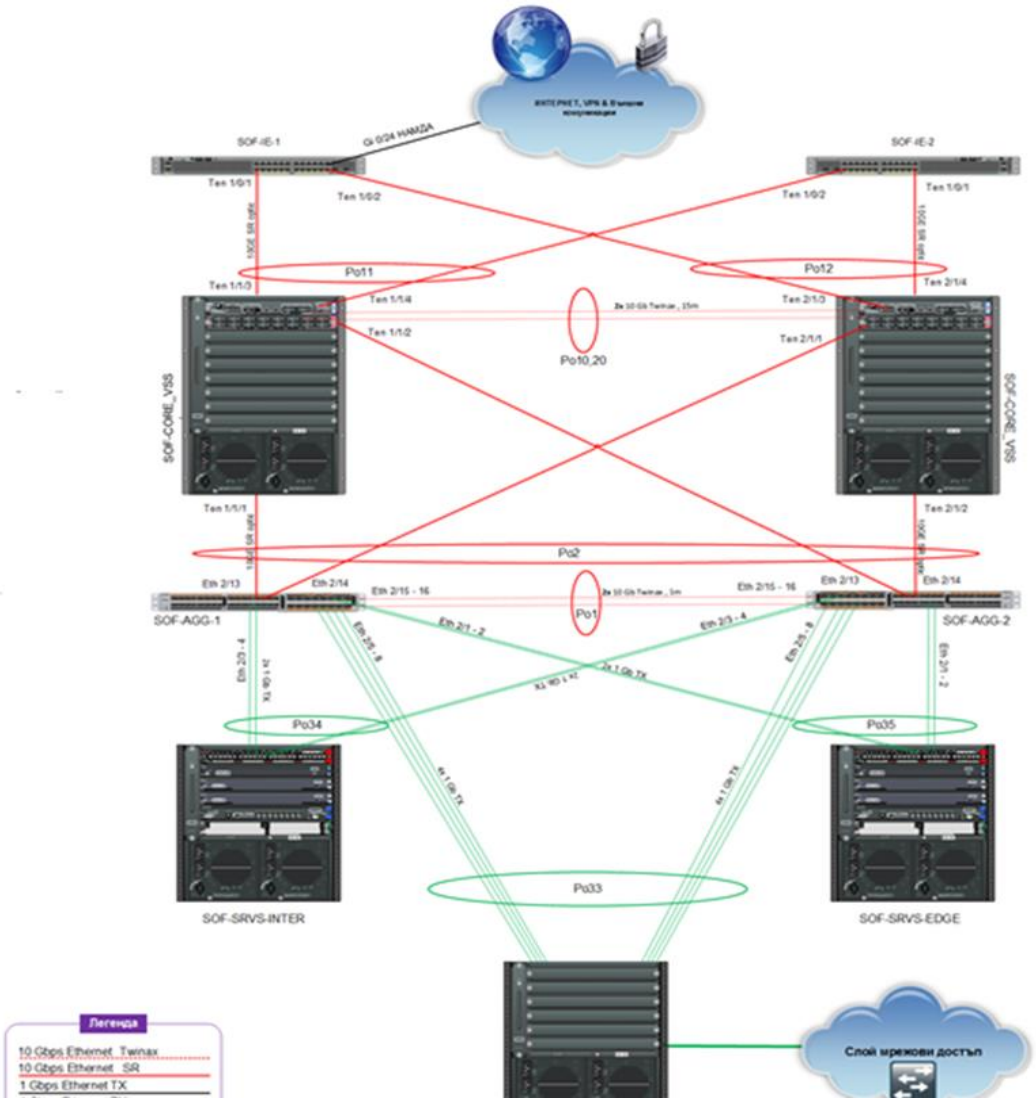
- два взаимнозаменяеми центъра за данни в режим „актив-актив“ за ДХЧО;
- център за възстановяване при бедствия и аварии;
- център за наблюдение и управление;
- центрове за колокация за разполагане на ИКТ инфраструктура на АО.

В центровете за данни са инсталирани следните основни системи:

- комуникационна система, осигуряваща мрежова сигурност и защитен мрежов достъп;
- система за оторизация и автентикация на потребителите;
- система за управление на достъпа до интернет и сигурен достъп до системата за електронна поща;
- система за електронна поща и съвместна работа с потребителите;
- система за оперативни актуализации на системите и приложните софтуерни пакети;
- система за архивиране и възстановяване на критични данни.



Принципна схема на свързаност на центровете за данни

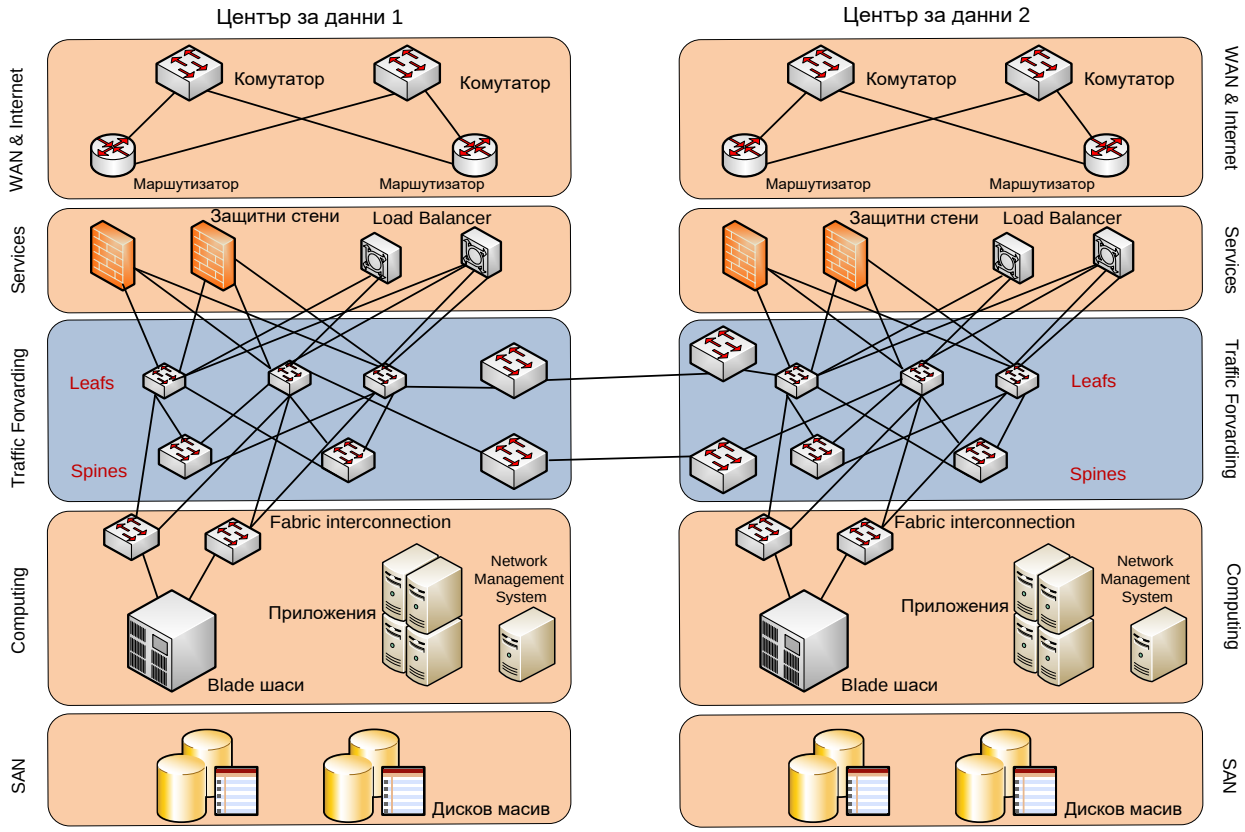


Топология на преносната среда на центровете за данни

За всеки от проектите, свързани с ЕУ, се предоставя IP адресно пространство в четири логически разделени среди с условното наименование „тестова“, „разработване“, „продукционна“ и „демилитаризирана зона“. В зависимост от заявената необходимост един проект може да има компоненти във всяка една среда или само в някои от тях.

Достъпът до мрежовите услуги, e-mail, между IP мрежите на една среда, както и между мрежите на отделните среди се контролира от защитни стени с помощта на листи за достъп. Същите устройства се явяват и gateway на IP мрежите на всяка среда. Логическото разделение на мрежовите сегменти се осъществява чрез VLAN технология.

Изчислителните ресурси се осигуряват от клъстери за виртуализация, на които са конфигурирани съответните виртуални мрежи със зададена IP адресация съгласно възприетия адресен план. Свързаността на клъстерите към общата мрежова инфраструктура се осъществява посредством система от виртуални и хардуерни комутатори и защитни стени.



Принципна схема на планираното сървърно оборудване в центровете за данни

3.2. Държавен хибриден частен облак

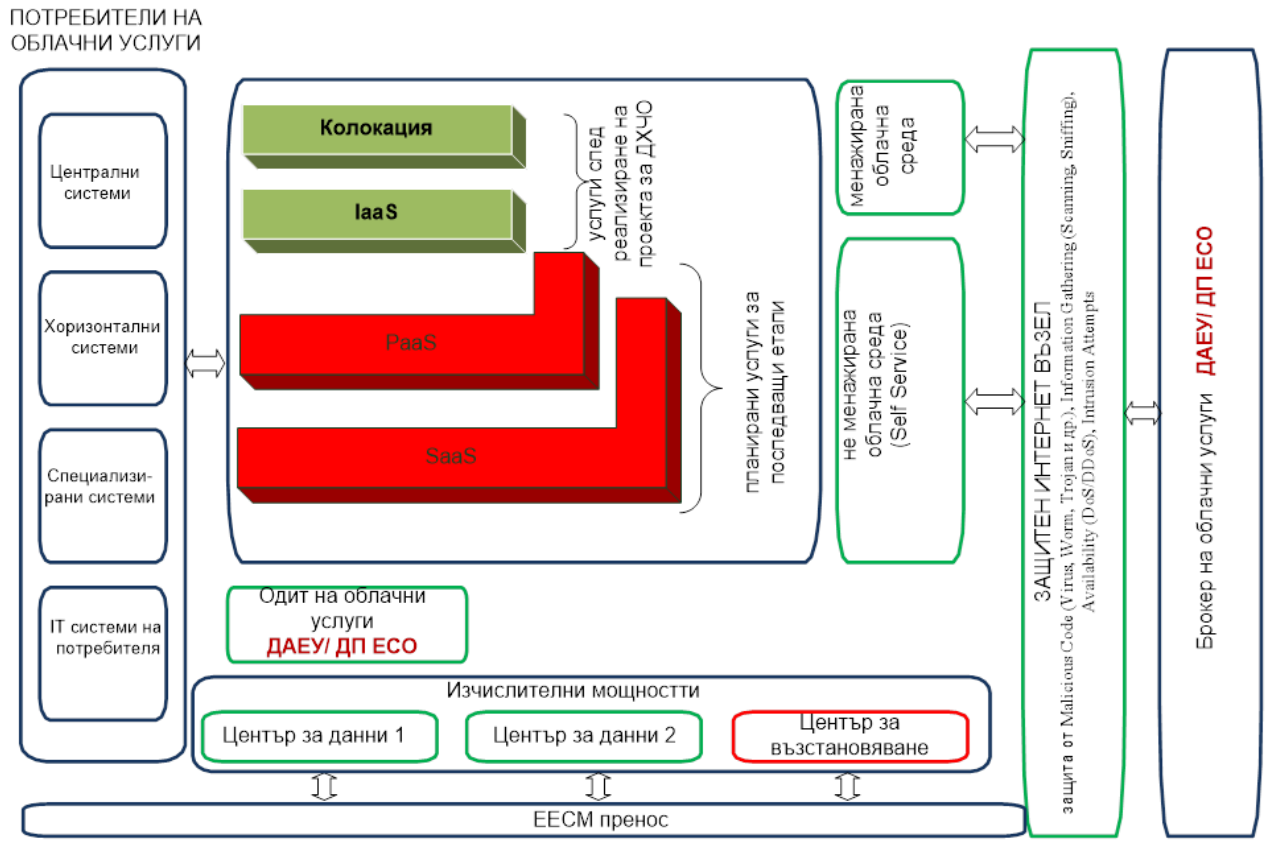
Държавният хибриден частен облак се изгражда за предоставяне на облачни услуги. Той позволява лесно, бързо, сигурно, гъвкаво, икономично и оптимално предоставяне на виртуален ресурс на АО за нуждите на ЕУ.

Миграцията към услуги в облака се извършва поетапно. Започва от тези с най-ниска натовареност и най-малки изисквания за непрекъсваемост. На втори и следващ етап процесът продължава с мигриране на по-сложни компоненти и системи, като се избягват действия от типа „виртуализация на всяка цена“. При проектиране и въвеждане в експлоатация на нови ИС, както и при подобряване на същите, се анализира първо възможността за използване на облачни услуги.

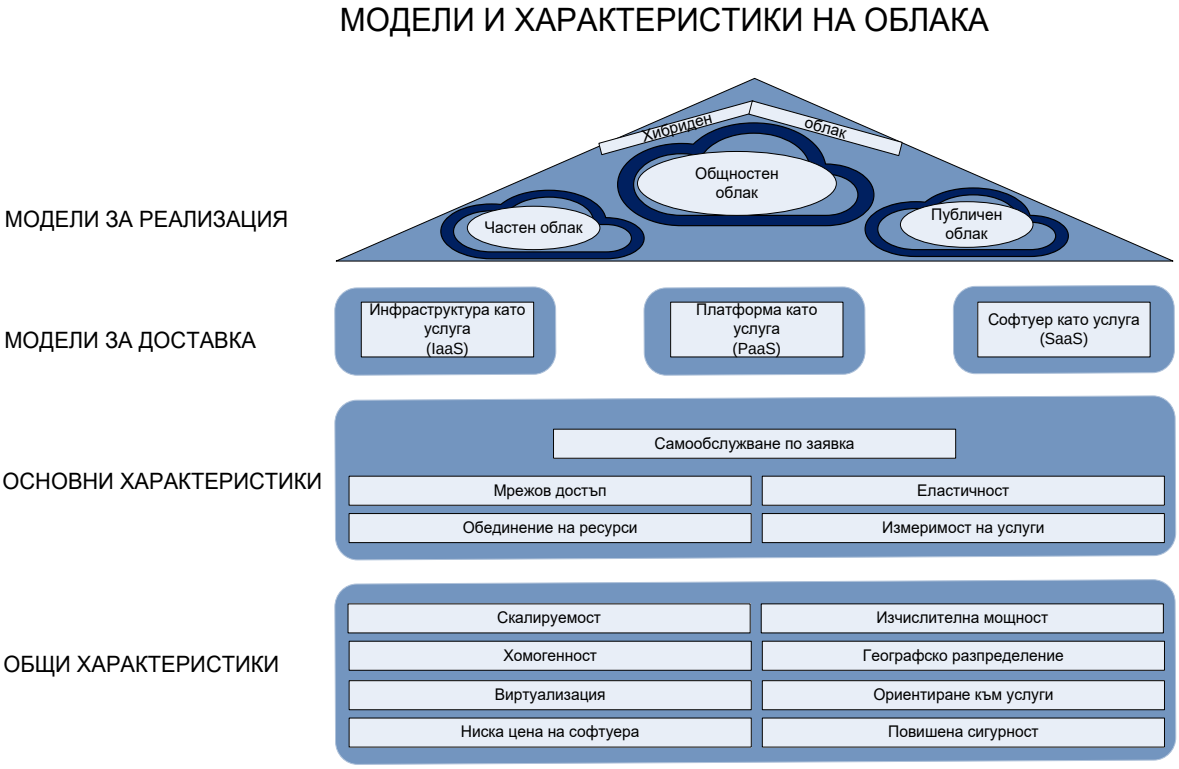
Като модел на реализация на ДХЧО се използва общностен модел и модели за доставка на облачни услуги „Инфраструктура като услуга“, „Платформа като услуга“ и „Софтуер като услуга“. Предоставя се и услугата „колокация “ на информационни ресурси.

ДХЧО се определя като хибриден облак, защото част от ИТ оборудването на ЕУ е инсталирано в центовете за данни, а друга част е разположена локално в административните органи и управлението на облака се извършва както в менажирана среда, така и в неменажирана среда.

Преки потребители на споделените изчислителни ресурси и предоставяните облачни услуги са административните органи.



Обща схема на ДХЧО



Функционалности на ДХЧО

- Самообслужване по заявка на потребители. Порталът осигурява възможност потребителите на облачната платформа да изискват и да получават инфраструктура, приложения и други услуги, без намеса на администраторите на ДХЧО. Порталът за

самообслужване съдържа каталог от услуги и е интегриран с модулите за автоматизация и оркестрация, и предоставя на потребителите възможност за наблюдение и управление на поисканите ресурси – например графична конзола на виртуална машина, защитена връзка (VPN) за достъп, събиране на статистики и др.

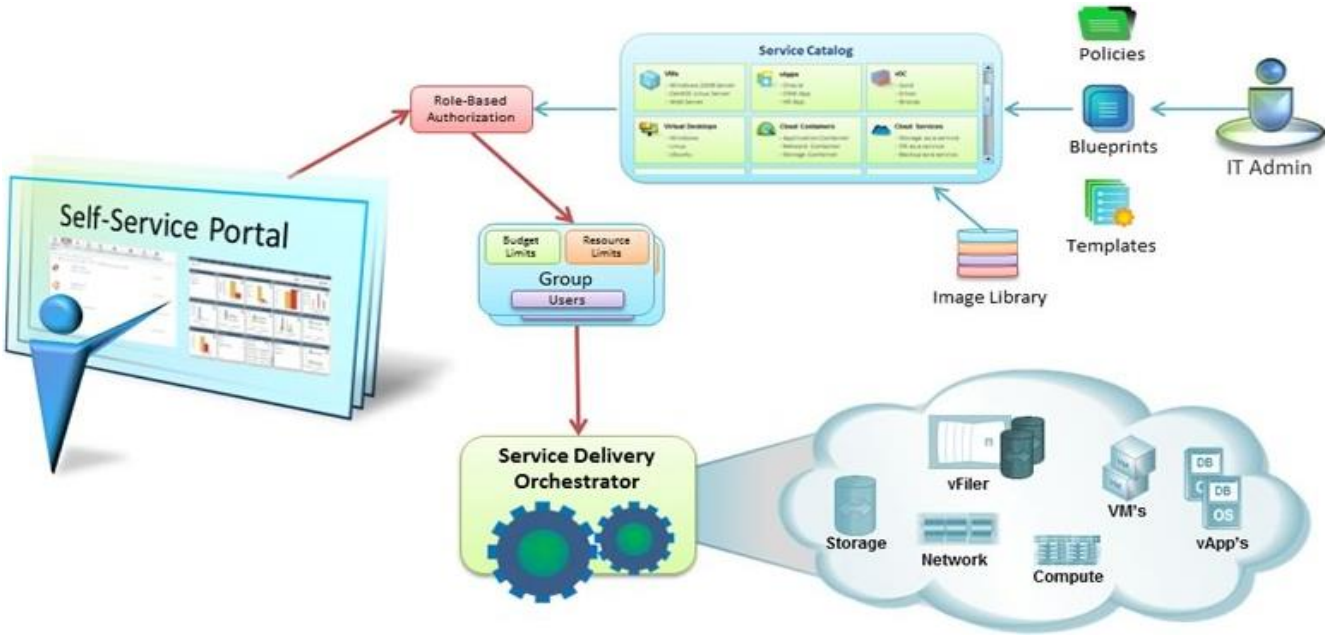


Схема на портал за самообслужване

- Обединяване на изчислителни ресурси и наличност на ресурси. Основната изчислителна мощност се осигурява от хардуерни средства с висока производителност – сървъри, дискови системи, мрежово оборудване и др., които по правило са проектирани за непрекъсната работа.

За осигуряване на висока наличност изчислителните ресурси са логически обединени в клъстери, което позволява еднородни изчислителни компоненти да се разглеждат като самостоятелна единица, притежаваща определени свойства и висока производителност. Клъстерът наследява параметрите на всеки един от неговите единични компоненти, но превъзхожда всеки един от тях. В този смисъл клъстерът от сървъри е основен източник на изчислителна мощ и подобрява производителността и достъпността.

- Формиране на пулове от ресурси и многопотребителски среди. Обединяването на ресурси позволява информационните и изчислителните ресурси на ДХЧО да се групират в широк мащаб, така че да обслужват множество потребители едновременно. Различните физически и виртуални ресурси динамично се предоставят или се отнемат според потребителското търсене. Обединяването на ресурси се постига чрез многопотребителска технология. Многопотребителският подход позволява да се обслужват множество АО – получатели на ресурсите, при което всяка организация се изолира от другите.

Схема на вариант за прилагане на технология за многопотребителска среда

На виртуалните сървъри е инсталирана инфраструктура за съвместна работа с използване на видео и аудио комуникации и е конфигурирана услуга за електронна поща. Регистриран е интернет домейн, като ресурсите на отделните организации са обхванати в поддомейни на основния домейн. Използвайки многопотребителски портал за самообслужване по заявка, отделните АО имат възможност да управляват локално собствените си потребители.

За обединяването на ресурси в ДХЧО се използват различни технологии за виртуализация, поради което логично такова обединяване може да се прилага за изчислителна мощ, мрежи и място за съхранение.

- Автоматизация на задачите и оркестрация на процесите. Двата компонента се използват за създаване и управление на всякакъв вид виртуални ресурси в ДХЧО – сървъри с приложения, уеб сървъри, устройства за балансиране на натоварването, бази от данни и др. Основната цел е това да се извършва бързо, автоматично и без човешка намеса.

Характеристики на ДХЧО

- мащабируемост и еластичност – определят приспособимостта на ДХЧО да разширява или да освобождава (отнема) изчислителни ресурси според търсенето и натоварването;

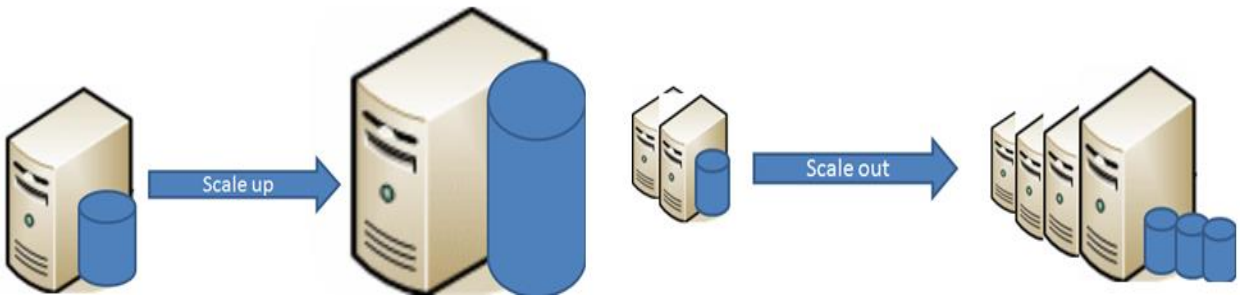


Схема на вертикално и хоризонтално скалиране

- измеримост – измерването на услугите в ДХЧО се възприема като способност, чрез която може да се контролира използването на ресурси от потребителя или от АО-получател на ресурси. Реализира се посредством софтуер, който е част от технологичното решение или е интегриран допълнително за следене на показатели, пряко свързани с използваните ресурси;

- мрежов достъп до ДХЧО – комуникационната свързаност на центровете за данни осигурява използване на споделен изчислителен ресурс от АО за осигуряване на ЕАУ за гражданите и бизнеса, ВАЕУ и среда за съвместна работа.

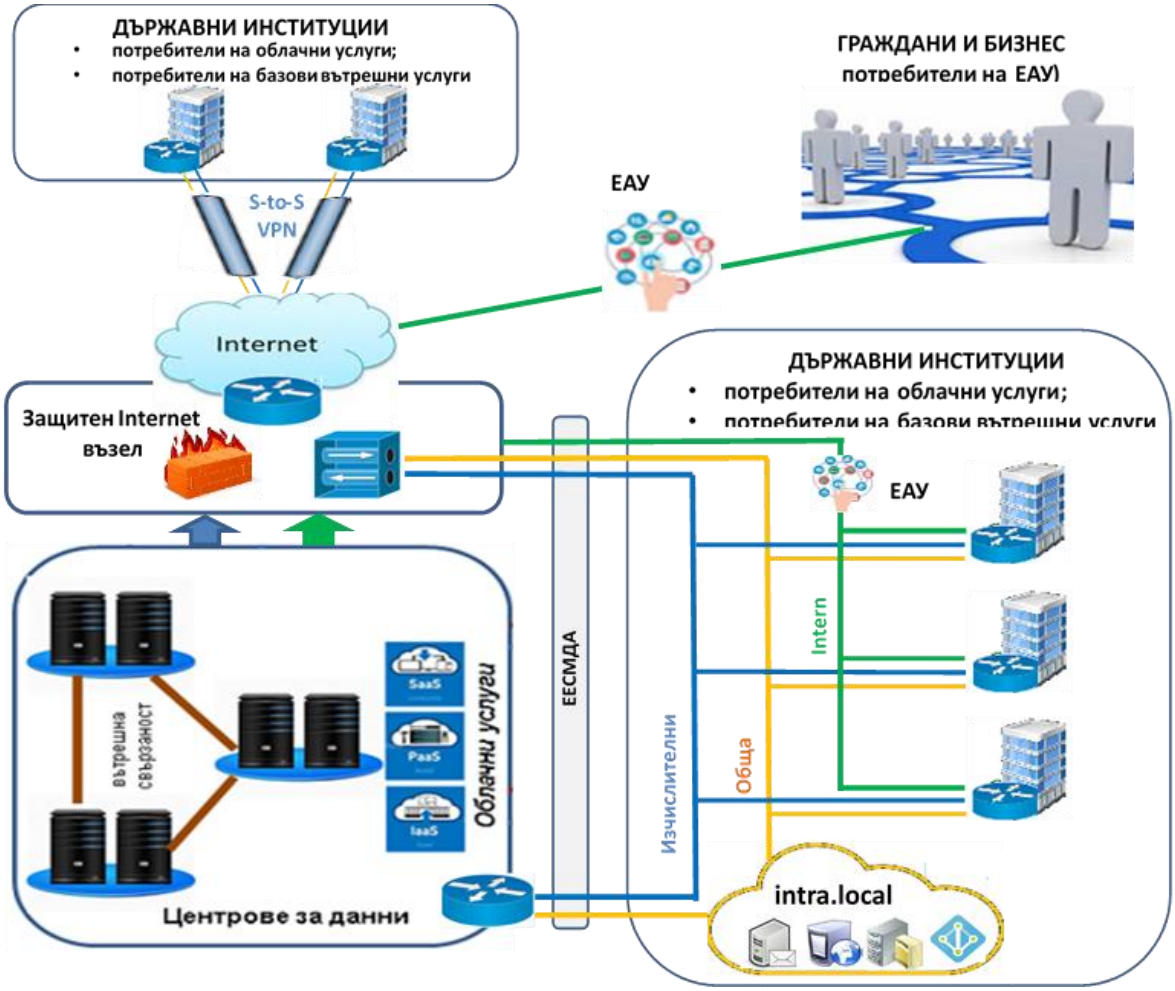


Схема на основния вариант за свързаност на центровете за данни

Потребители на изчислителни ресурси се явяват държавните институции, като са осигурени връзки чрез мрежите на ЕЕСМ.

Управление на облачните услуги и работните процеси

Управлението на облачните услуги е организиран и регламентиран, непрекъснат процес с участие на заинтересованите страни и включва:

- заявяване и осигуряване на услугите по определена процедура;
- измерване на услугите по дефинирани параметри;
- оценка на състоянието на услугите в резултат на измерването;
- управление на ресурсите при отклонение от зададените параметри.

Технологичната реализация на системата за управление на услугите обхваща инсталиране, конфигуриране и настройка на софтуерни компоненти, които влияят на експлоатацията на облачната среда. Компонентите дават възможност за дефиниране на абонаментни планове, на механизми за измеряемост, на системата за контрол на достъпа до ресурсите, налагане на политики и др.

Управлението е интегрирано в портал за администриране и потребителски портал за самообслужване, както и други технологични инструменти.

Схема на портала за администриране и самообслужване

Сигурност на информацията и услугите в ДХЧО

Системата за сигурност на информацията в ДХЧО гарантира достъпността, целостта, конфиденциалността и наличността на информацията, създавана, пренасяна и съхранявана в облака.

Администрациите, които не са свързани към ЕЕСМ, ще имат достъп до ДХЧО през Интернет посредством Защитения интернет възел (ЗИВ). За целта ЗИВ ще осигури защита от основните видове заплахи и възможни атаки в Интернет. Предвижда се и използването на хардуерни устройства за защита на достъпа до облака.

Управление на ДХЧО

- управление в менажирана среда – ДАЕУ хоства и управлява предоставения на АО облачен ресурс. Този ресурс е отделен от ресурсите, предоставени на други АО.
- управление в неменажирана среда – предоставяне на самообслужваем облак.

Предоставянето на инфраструктура като услуга се състои от следните елементи:

- хардуерен слой;
- слой виртуализация;
- слой за автоматизация и оркестрация;
- потребителски портал за самообслужване.

Услугата позволява на потребителите да създават виртуални сървъри с изчислителни ресурси (процесор, памет и дисково пространство) и операционни системи по тяхно решение. Осигурена е възможност да дефинират необходимите им виртуални мрежи с IP адресен план по техен избор, в които могат да свържат своите сървъри. За всяка потребителска мрежа облачната платформа автоматично създава виртуални мрежови устройства – комутатор, маршрутизатор, защитна стена и устройство за балансиране на трафика.

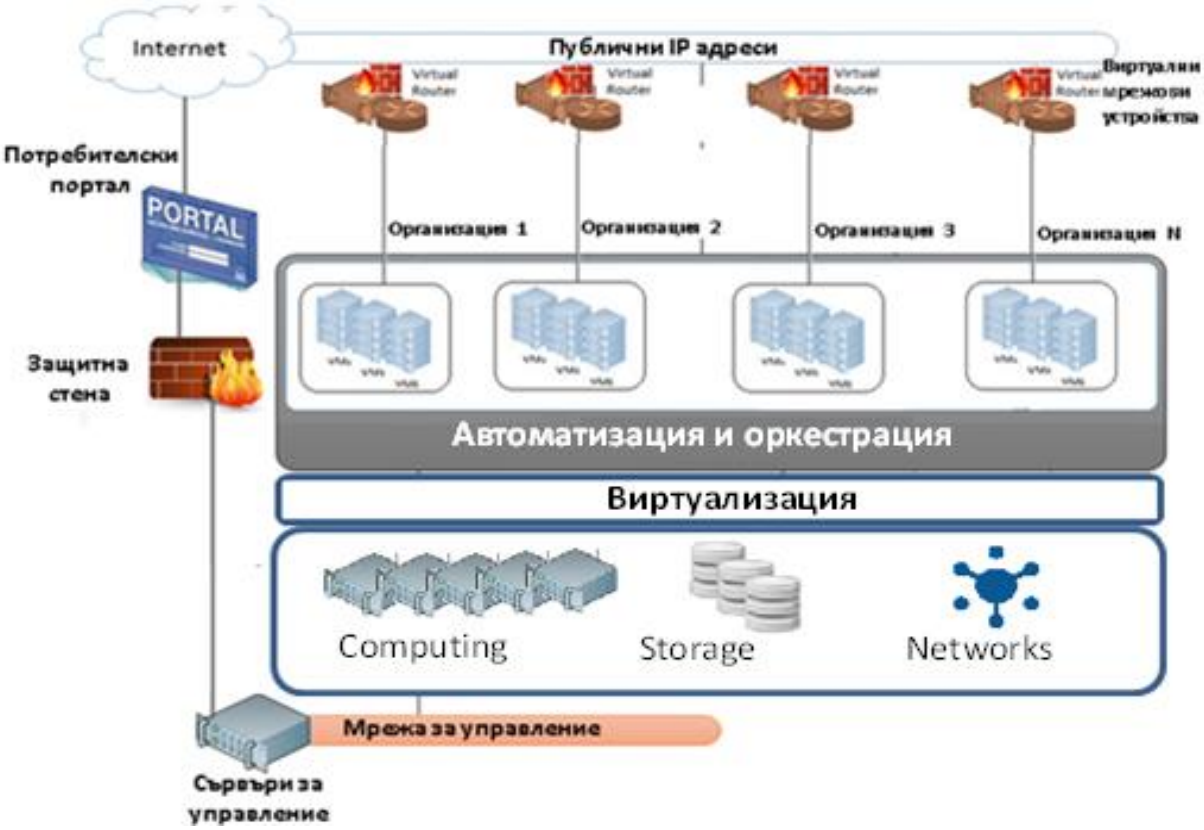


Схема на примерна среда за предоставяне на „инфраструктура като услуга“

Използване на ДХЧО за предоставяне на публична услуга

ДХЧО може да се използва за предоставяне на публична услуга. Организация 1 в рамките на предоставените квоти има възможност да създаде собствено обкръжение от виртуални ресурси (сървъри), които да са достъпни в публичното Интернет пространство. Администраторът на организацията следва да конфигурира защитен VPN тунел чрез използване на възможностите на облачната платформа. Заедно с това има възможност да разреши в защитната стена достъп до порта, по който ще изгради сесията за управление.

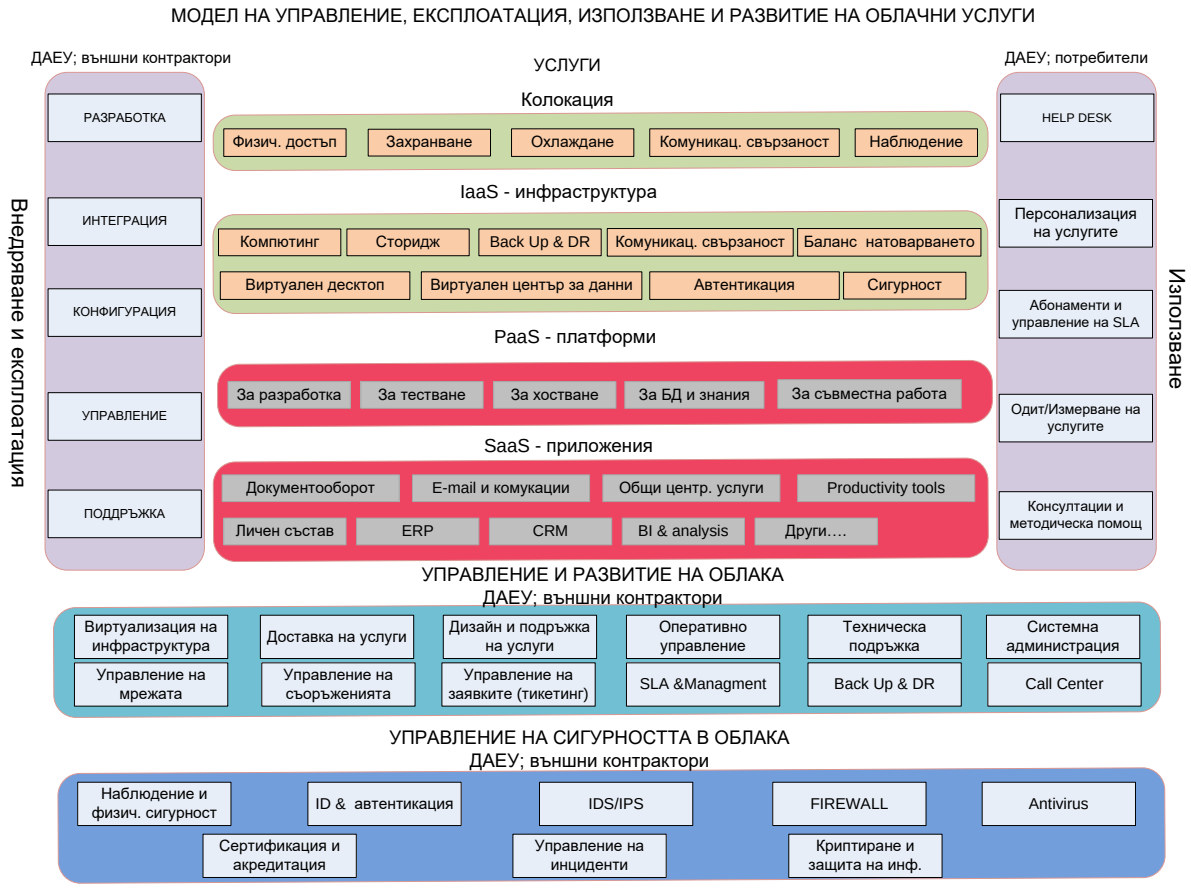
Схема на предоставянето на публична услуга

Използване на ДХЧО като локални ресурси

ДХЧО може да се използва и като локални ресурси. В този случай Организация 1 в рамките на предоставените квоти има възможност да създаде собствено обкръжение от виртуални ресурси (сървъри), които да са обхванати в частен виртуален облак. Чрез инструментариума на облачната платформа потребителят може да създаде защитена мрежова свързаност, така че мрежовият сегмент на виртуалните сървъри да се свърже към частната локална мрежа на потребителя и логически да стане част от неговата инфраструктура.

Схема на използване на инфраструктурата като локални ресурси

Инфраструктурата на Организация 1, която до този момент е разполагала с определени хардуерни ресурси, се разширява до всички виртуални сървъри, които се намират в нейния виртуалния частен облак. Хардуерните сървъри и виртуалните сървъри са достъпни както помежду си, така и за всички потребители от Организация 1.



3.3. Управление на софтуерните лицензи

Чрез софтуерните лицензи се предоставя правото за ползване за определено време или безсрочно на приложен или системен софтуер. Прилагането на централизиран подход за осигуряване на софтуерни лицензи за нуждите на ИС в рамките на ЕУ дава възможност за договаряне на благоприятни функционални и финансови условия и води до икономия на средства.

Управлението на софтуерните лицензи се отнася до процесите и инструментите, използвани за документиране и проследяване на портфолио от използвания софтуер на дадена АО и включва:

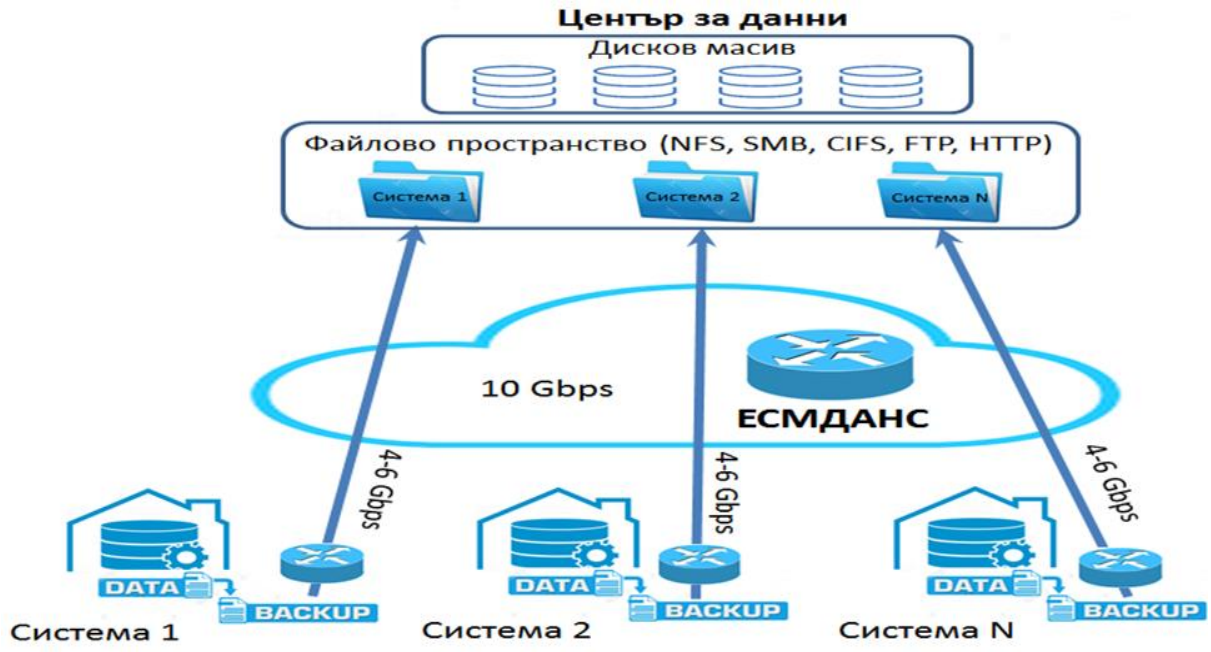
- политики и процедури за използването на лицензите;
- инструмент за инвентаризиране на целия софтуер;
- ИС за управление на ИТ активи.

3.4. Хранилище за данни на електронното управление

Хранилището за данни има за цел повишаване на устойчивостта на критичните информационни системи и регистри на ЕУ посредством резервиране и съхранение на данните им. Постигането на целта се реализира чрез:

- надграждане на съществуваща инфраструктура в Център за данни на електронното управление, за хранилище за данни;

- поддържане на резервни копия на данни от критичните системи и регистри и съхранението им в хранилището от отговорните АО;
- увеличаване на преносния капацитет на ЕЕСМ;
- поддръжка за интегриране на системите за резервиране на критични данни в хранилището.



Логическа схема на хранилището за данни

Отговорността за запазване и възстановяване на данните на АО принадлежи на самия административен орган. Всеки АО трябва да има план за действие и възстановяване на критичните данни и ИС от аварии и бедствия.

3.5. Комуникационна инфраструктура на електронното управление

Комуникационната инфраструктура е базов елемент и критичен фактор на инфраструктурата на ЕУ. ДАЕУ управлява и развива комуникационна инфраструктура като споделен ресурс на ЕУ с цел постигане на устойчивост, качество на услугите и минимизиране на публичните разходи.

Свързването на всички АО посредством ЕЕСМ е основна предпоставка за функционирането и развитието на ЕУ.

ЕЕСМ осигурява електронни съобщения за нуждите на ЕУ. Тя се състои от оптична кабелна инфраструктура с дължина около 7700 км и активно оборудване, разположено в помещения държавна или общинска собственост, и Съобщителни обекти със специално предназначение, където са обособени главни опорни възли, агрегиращи възли и възли за достъп.

Модел на комуникационната инфраструктура

ЕЕСМ се изгражда на база йерархичен модел, който включва следните слоеве:

- преносен слой – оптични кабелни линии (ОКЛ), DWDM (Dense wavelength division multiplexing) технология и SDH (Synchronous digital hierarchy) технология;
- опорен слой – изграден е с помощта на високоскоростни маршрутизатори. Опорната мрежа обхваща 28-те областни центъра на Република България. Важна част от опорния слой са IP/MPLS маршрутизаторите, които осигуряват надеждна информация за маршрутите и VPN мрежите;

- агрегиращ слой – изграден е с помощта на високоскоростни комутатори, разположени в областни и общински центрове;
- слой за достъп – изграден е с помощта на високоскоростни комутатори с разширена функционалност;
- DWDM осигурява голямо уплътнение на оптичното влакно и има висока надеждност. Преносната DWDM среда е изпълнена като отделна система. DWDM технологията има изградени няколко рингови структури. Това позволява да се гарантира надеждността на преноса при отпадане на основно трасе поради авария, като се избира алтернативен маршрут.

За осигуряване на широк и равнопоставен достъп до услугите на ЕУ се осъществяват връзки с комуникационните инфраструктури на действащите оператори с приоритетност опорен, агрегиращ слой или слой за достъп в съответствие с техническата възможност и целесъобразност.

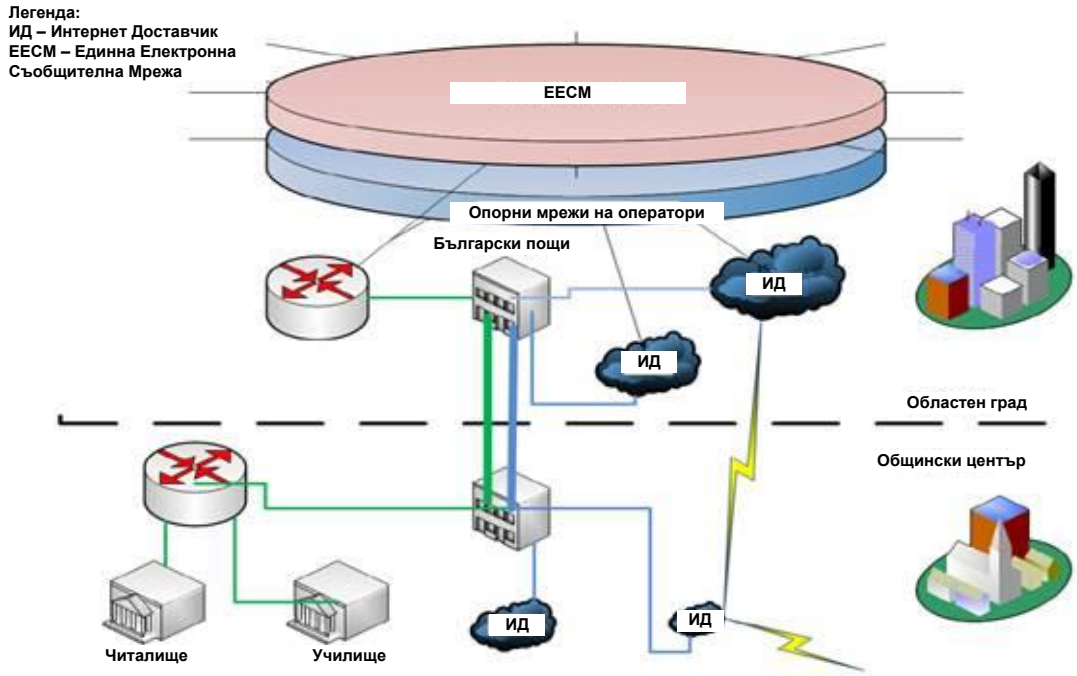


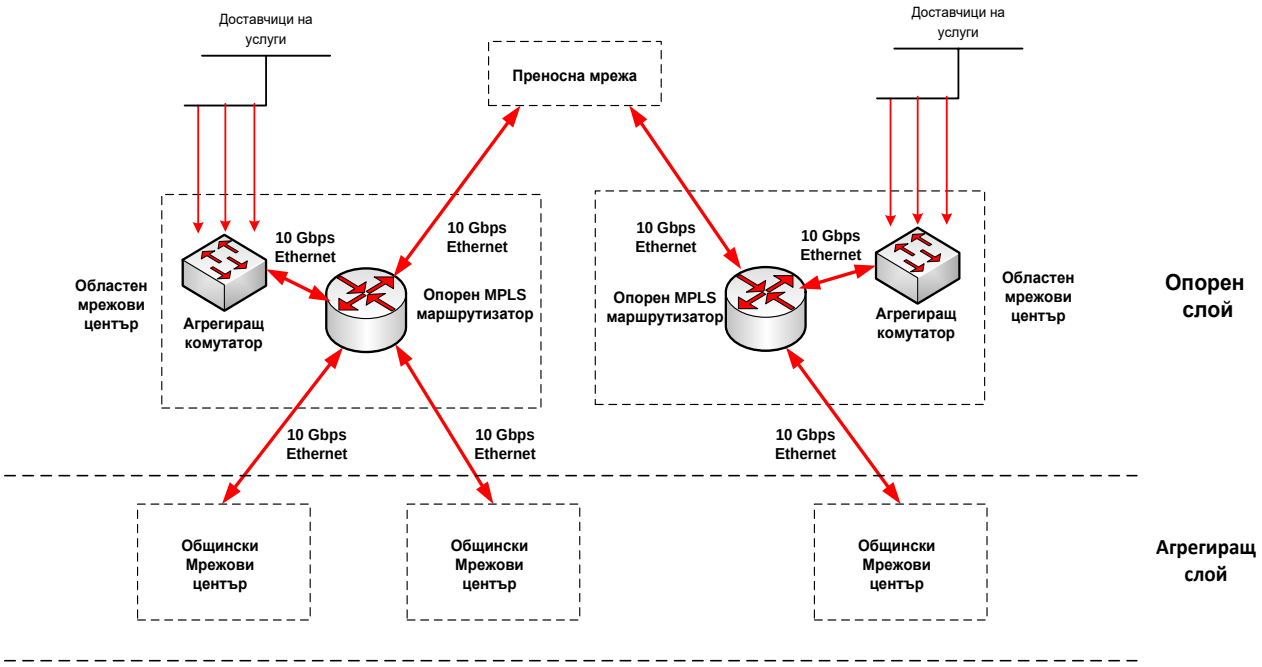
Схема на връзки с комуникационни инфраструктури

ДАЕУ развива мрежата, като изгражда поетапно оптична свързаност до сградите на общинските и другите администрации, осигурява необходимото оборудване и увеличава преносния капацитет на мрежата.

Единна електронна съобщителна мрежа на държавната администрация

Единната електронна съобщителна мрежа осигурява електронни съобщения за нуждите на органите на държавната власт, органите на местното самоуправление и юридическите лица – разпоредители с бюджет, създадени със специален закон. Тя се състои от следните елементи:

- оптична кабелна инфраструктура с дължина около 7700 км;
- DWDM и SDH преносни среди;
- IP/MPLS опорна мрежа;
- системи за наблюдение и управление.

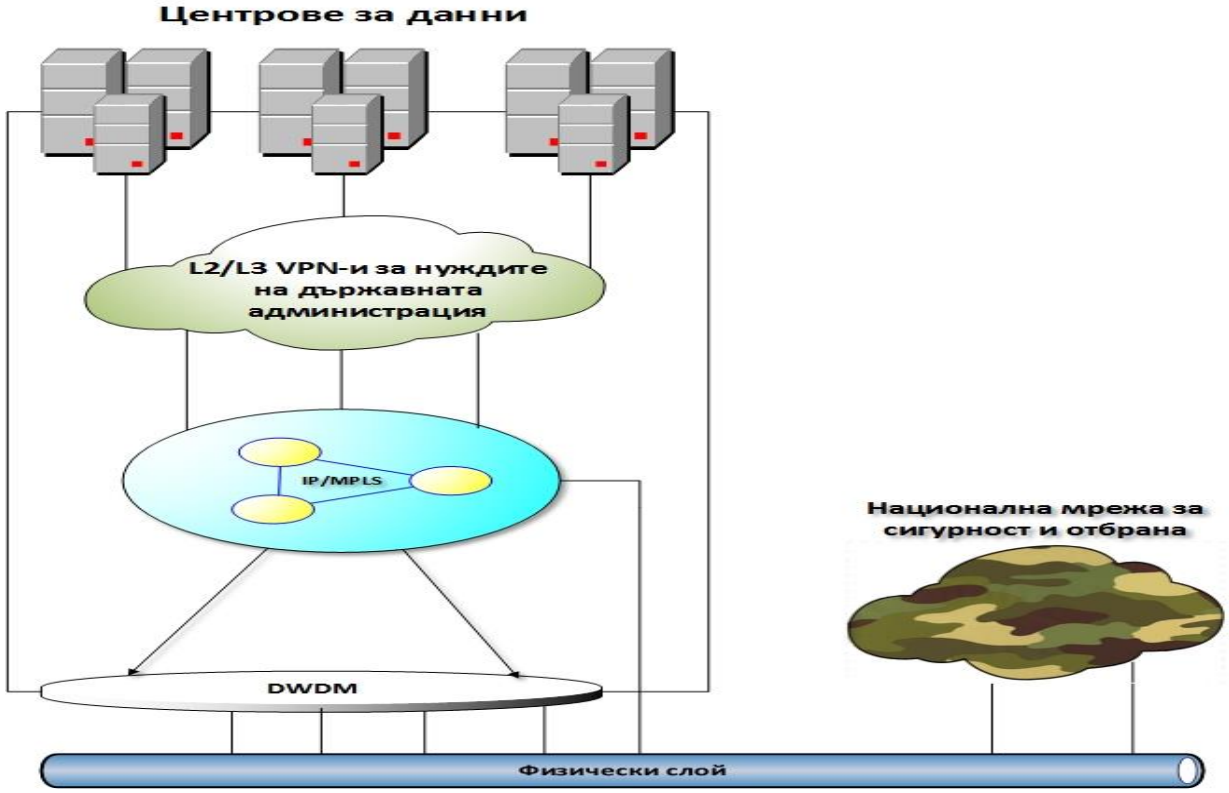


Архитектура на IP/MPLS опорна мрежа

Активното оборудване на ЕЕСМ е разположено в:

- помещения държавна или общинска собственост;
- съобщителни обекти на ДАЕУ, където са обособени главни опорни възли, агрегиращи възли и възли за достъп.

ЕЕСМ е част от Интегрираната комуникационно-информационна система за управление на страната и въоръжените сили при обявяване на „извънредно положение“, „военно положение“ и/или „положение на война“ и има стратегическо значение за отбраната и сигурността на страната.



Обща схема на ЕЕСМ и свързването на центрове за данни

ЕЕСМ изгражда и поддържа следните видове мрежи:

- „Изчислителни ресурси“ (Интранет) – затворена частна мрежа между центровете за данни, формиращи инфраструктурата на ДХЧО, други центрове за данни на ЕУ и локалните инфраструктури на АО;
- „Обща среда“ (Екстранет) – затворена частна мрежа за съвместна работа между инфраструктурите на АО и ДХЧО. Чрез нея се осигуряват стандартни мрежови услуги (DNS, NTP и др.), централизирано управление на потребителите, базови услуги за съвместна работа;
- „Интернет“ – свързаността на АО към интернет се осъществява през защитен възел за достъп, където са наложени политики за контрол на мрежовия достъп и механизми за защита от кибератаки;
- „VPN“ – затворена частна мрежа, между центровете за данни и инфраструктурите на администрациите, които нямат физическа свързаност към интранет мрежата, изградена през транспортната среда на Интернет.

Транспортната среда за мрежи „Изчислителни ресурси“ и „Обща среда“ се осигурява от ЕЕСМ, като тези мрежи са логически разделени.

Оптични кабелни линии

Преносният слой на ЕЕСМ е реализиран с междуградски и градски оптични кабелни линии (ОКЛ) с приблизителна дължина 7700 км. Междуградските ОКЛ са изградени между областните градове и съобщителните обекти на ДАЕУ с оптични кабели тип G.652 и G.655. Градските ОКЛ са изградени във всички областни градове до държавните структури със сингълмодови и мултимодови ОКЛ.

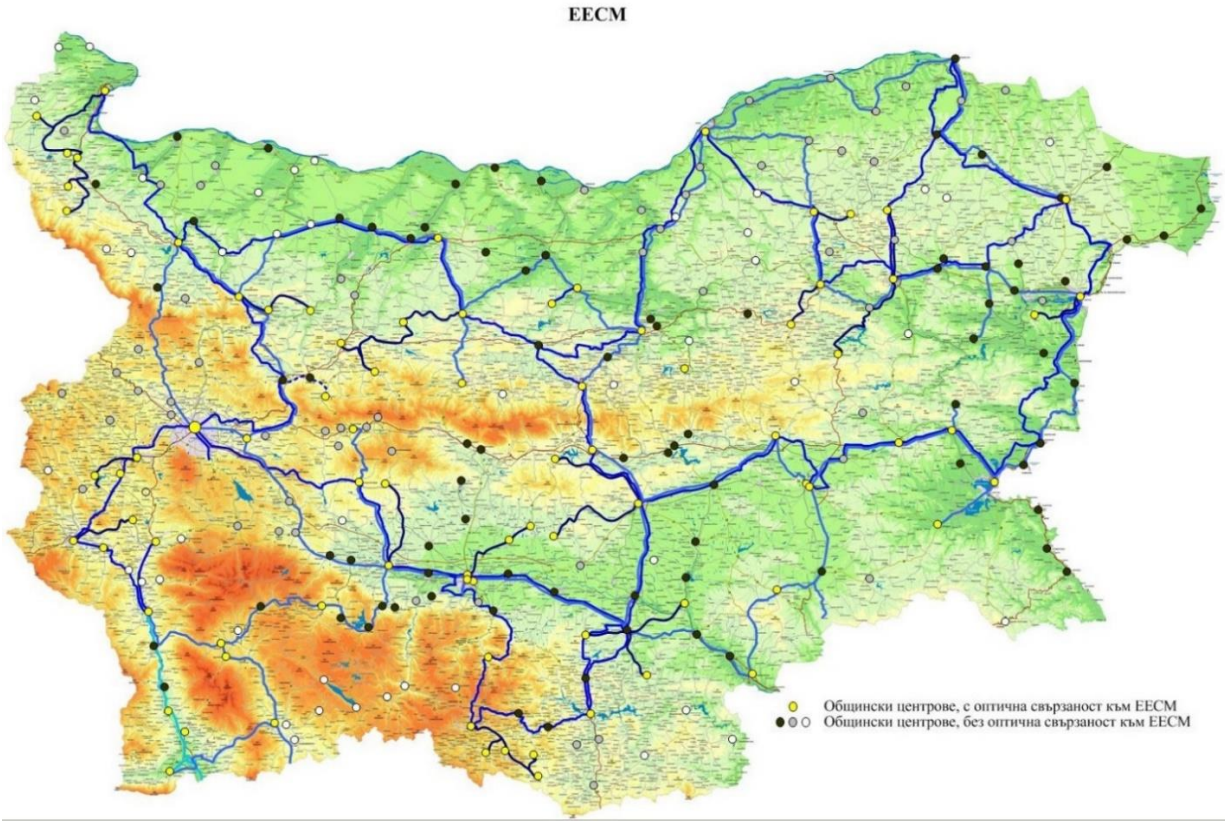


Схема на оптичната кабелна свързаност на ДАЕУ

3.6. Инженерно-техническа инфраструктура на споделените ресурси на ЕУ

Инженерно-техническата инфраструктура е комплекс от:

- строителни конструкции;
- системи за основно, автономно и непрекъсваемо електрозахранване;
- системи за климатизиране и вентилиране на оборудването и технологичните помещения;
- системи за пожароизвестяване и пожарогасене;
- системи за контрол и мониторинг на състоянието на инженерната инфраструктура.

Инженерно-техническата инфраструктура осигурява работна среда за непрекъснато функциониране на информационното и комуникационното оборудване – непрекъсваемо токозахранване, климатизация, филтриране, вентилиране и поддържане на параметрите на въздуха, пожароустойчивост и пожарозащита, физическа защита от несанкциониран достъп, сеизмична устойчивост и др.

Елементите на инженерно-техническата инфраструктура се изграждат на основата на унифицирани изисквания към центровете за особено чувствителна информация, в съответствие с изискванията за оперативна съвместимост и информационна сигурност.

4. Мрежова и информационна сигурност в електронното управление

Мрежова и информационна сигурност (МИС) на ЕУ е съвкупност от взаимосвързани механизми: изисквания за сигурност, принципи, системи, изпълняващи задачи по МИС, зони за сигурност и процеси, свързани със сигурността по защитата на информационните ресурсите на ЕУ.

Целта на МИС е да гарантира достъпността, целостта, автентичността и конфиденциалността на информацията по време на създаването, обработването, съхранението, пренасянето и унищожението ѝ, намаляване на щетите от реализиране на заплахи и намаляване броя на измамите.

МИС се организира и функционира в съответствие с изискванията, заложени в нормативните документи и общоприетите стандарти по МИС.

Стандарти от серията ISO/IEC 27k.

4.1. Общи изисквания за мрежова и информационна сигурност на ЕУ

- най-малката привилегия – достъпът да се ограничава само до това, което е необходимо за изпълнение на одобрените функции;
- защита в дълбочина – защитата да се реализира на последователни нива, така че при компрометиране на едно ниво да не се компрометира сигурността на ЕУ;
- среда за предаване на данни между доверени зони – да принуждава атакуващите да използват тесен канал за достъп, при който действията им могат да бъдат наблюдавани и контролирани;
- най-слаба връзка – общото ниво на сигурност да се определя от сигурността на най-слабата връзка;
- безопасност при отказ – ако системите откажат неочаквано, информацията да не бъде разрушена и да няма неоторизиран достъп до нея;
- всеобщо участие – всеки участник в ЕУ да е ангажиран със сигурността;
- разнородност на защитата – защитата на ЕУ да се реализира с многостранни механизми за сигурност;
- опростеност – за гарантиране на ефективна сигурност на ЕУ да се търси опростена ИКТ инфраструктура;
- разделяне на сектори, сегментиране, изолиране – за минимизиране размера на щетите от реализиране на заплаха, информационният ресурс да се разделя на колкото е възможно повече обособени единици;
- защита срещу заплахи от вътрешни и външни лица – защитата да е такава, че да не прави разлика между вътрешен и външен източник на атаката.

4.2. Принципи на мрежовата и информационната сигурност на ЕУ

Принципите на мрежовата и информационната сигурност са основните правила, по които трябва да се водят участниците в ЕУ на всички нива и етапи от реализирането и функционирането на системите на ЕУ. Те включват:

- системен подход към МИС;
- разпределени отговорности;
- поддържане на актуална информация за всички активи, участващи в ЕУ;
- управление на риска;
- управление на достъпите и нивата на защита;
- осигуряване на правилна и надеждна работа.
- защита срещу заплахи;
- проследимост;
- наблюдение;
- контрол и одит;
- сигурност при придобиване, разработване и поддържане на ИКТ системи;
- управление на сигурността на веригата за доставки.

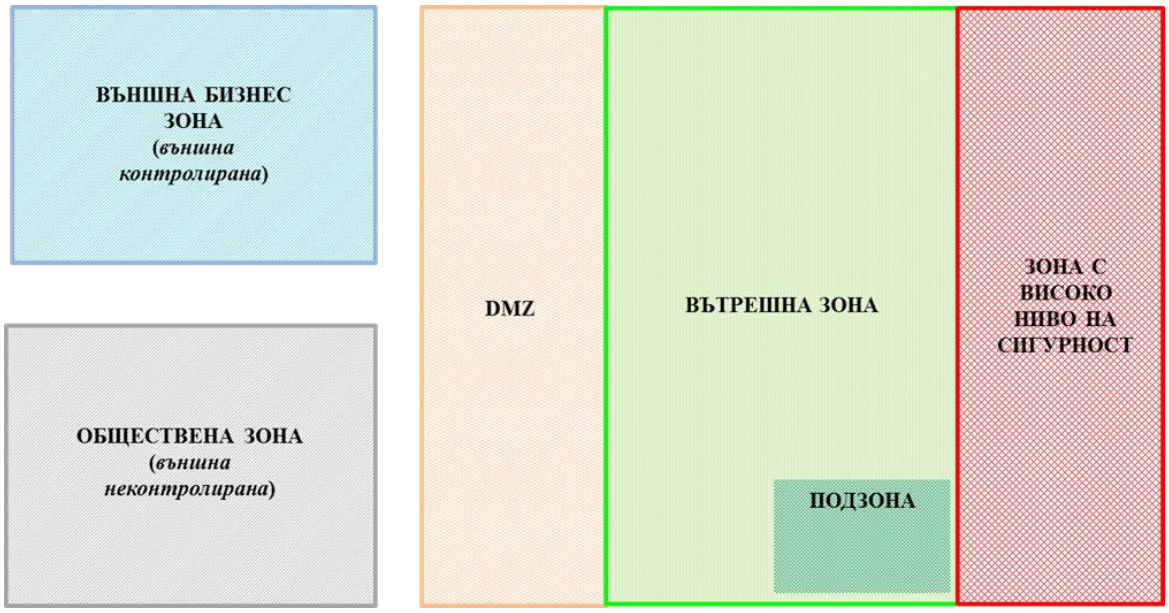
4.3. Основни елементи на архитектурата на МИС и техните взаимоотношения

4.3.1. Зони за сигурност

Използването на зони за сигурност гарантира, че възможността за достъп до информация и системи в една зона за сигурност не предоставя възможност за достъп до друга. Достъпът между зоните се контролира чрез използването на подходящи технологически и технически контролни механизми за физическа и логическа защита.

Въвеждането на зоните за сигурност включва:

- дефиниране на подходящите зони спрямо характеристиките за сигурност;
- отнасяне на информационните ресурси към зоните за сигурност.



Принципна схема на зоните за сигурност на АО и организациите, предоставящи е-услуги

Определени са следните зони за сигурност:

- зона с висока сигурност– съхранява се или се обработва чувствителна, лична или конфиденциална информация. „Ниво 2“ и „Ниво 3“;
- вътрешна зона – съхранява се или се обработва чувствителна или конфиденциална информация;
- външна бизнес зона (външна контролирана зона) – ИКТ инфраструктурата на друга организация (друг АО, организации), която се свързва с инфраструктурата на ЕУ;
- обществена зона (външна неконтролирана) – информацията и системите в нея са открити и неконтролирани. В нея не могат да бъдат приложени и/или проверени политики и стандартите за сигурност;
- демилитаризирана зона – DMZ е буферна зона, която обезпечава е-услуги чрез наличните връзки с външни мрежи. Не се допуска пряка връзка между обществената и външната бизнес зона с вътрешната зона;
- подзона –логически обособена част, използваща набор от ресурси, които поради специални изисквания следва да са отделени от останалата част на вътрешната зона. Подзоните може да изискват допълнителни контролни мерки за сигурност, за да бъдат изолирани от общата структура на вътрешната зона. Подзоната не трябва да бъде уязвима точка във вътрешната зона.

4.3.2. Системи на мрежова и информационна сигурност

Мрежовата и информационната сигурност в ЕУ се състои от голям брой механизми (процеси и технологии), действащи заедно за гарантиране на конфиденциалността, интегритета и достъпността на информацията. Изграждането на ефективна структура на МИС на ЕУ се основава на пет основни системи.

Системи на МИС

Система за автентикация

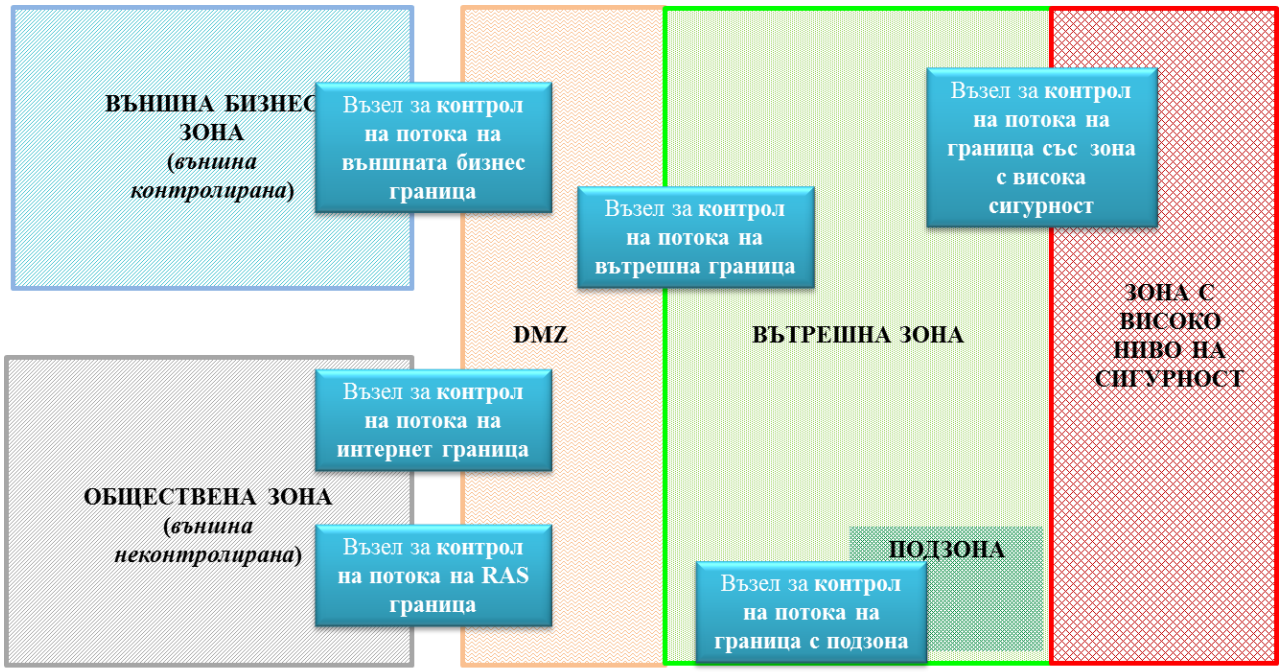
Системата гарантира, че дадено лице или система, които работят в даден контекст за сигурност, са лицето или системата, за които се представят. Елементите на системата за автентикация се използват в комбинация с политиките за контрол на достъпа и контрол на информационния поток, за да се предотврати заплахата от маскиране на потребителска идентификация. Тя взаимодейства с подсистемите за одит, е-оторизация и контрол на информационния поток, за да управлява разпространението, интегритета и прецизността на идентификациите.

Система за оторизация (контрол на достъпа)

Системата предоставя достъп до информационните активи на лица, системи и процеси въз основа на одобрени и съгласувани политики. След като идентичността бъде установена в рамките на системата за автентикация, тя може да се използва (във времето за изпълнение на заявката) от система за оторизация. Системата се използва в комбинация със системата за автентикация и контрол на информационния поток Тя подава информация за събитията към системата за одит, която може да осигури анализ на събитията в реално време или след приключването им.

Система за контрол на информационния поток

Системата гарантира сигурното пренасяне на информация от една точка до друга, като управлява пропускането на информационния поток въз основа на класификацията, достъпността и интегритета на информацията в рамките на дадена информационна система и зависи от регистрационните данни в подсистемата е-автентикация и механизмите за контрол на достъпа в подсистема е-оторизация. На местата, където трафикът влиза или излиза от определена зона, са въведени сигурни контролни мерки. Подсистемата подава информация към системата за одит.



Разположение на възлите на системата за контрол на информационния поток

Система за интегритет

Системата за интегритет отговаря за правилната и надеждна работа на критичните компоненти и процеси в рамките на информационна система, което включва управление на ресурси, управление на интегритет, управление на непрекъснатостта, управление на възстановяването, единно време, антивирусна защита, откриване на проникванията, наблюдение. Тя взаимодейства с останалите системи за МИС.

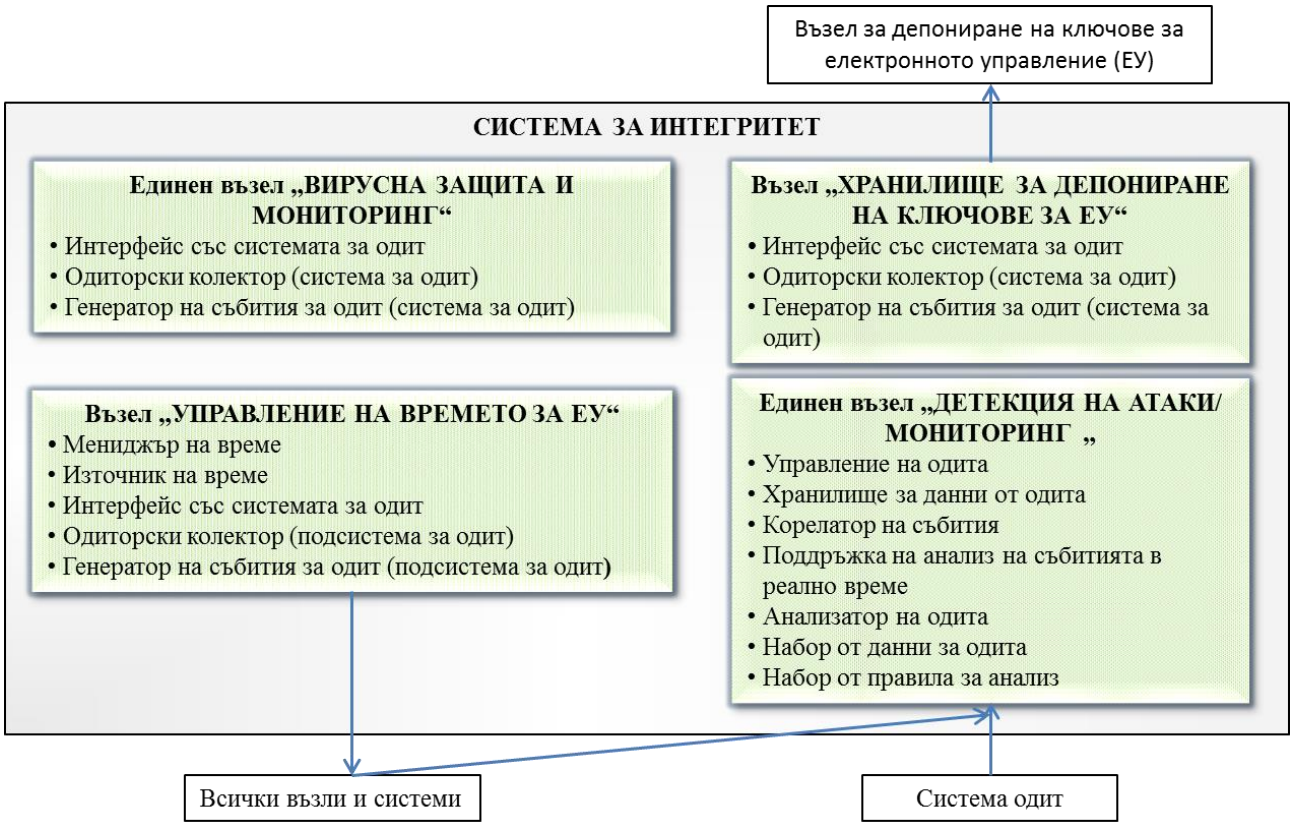


Схема на системата за интегритет

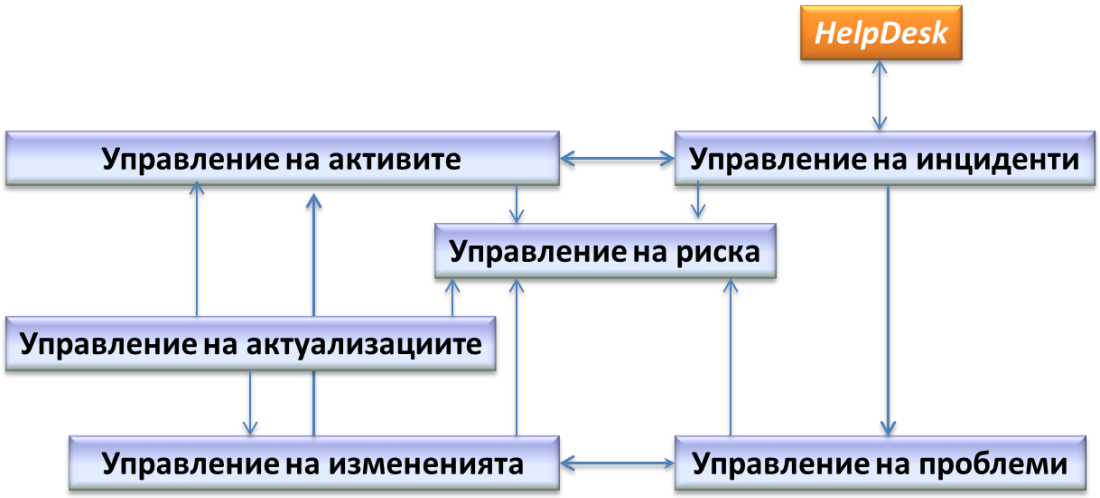
Система за одит

Системата осигурява събиране, анализ, отчитане, архивиране и възстановяване на записи за събития и обстоятелства в рамките на дадена информационна система. Анализът и отчитането могат да включват преглед в реално време или след приключване на дадено събитие, свързано със съдебен анализ в подкрепа на защитата срещу искове за отричане. Преглед и анализ на контролните записи може да установи неоторизирани дейности.

Възлите на системата за събиране и съхранение на данни за одит и управление се разполагат във вътрешна зона за сигурност, а хранилището на информация за одита – в зона с високо ниво на сигурност. Системата има връзка с всички останали системи за МИС.

4.4. Основни процеси, свързани с МИС

Прилагането на процесен подход гарантира, че изискванията за сигурност на информацията и очакванията на заинтересованите страни ще бъдат посрещнати чрез прилагането на необходимите действия и процеси, гарантиращи управлявана сигурност на информацията и предвидими резултати. За постигане на високо ниво на МИС на ЕУ описаните в ITIL процеси са задължителни за всички, участващи в предоставянето на е-услуги. Спазването им се контролира чрез сертификация по стандарт ISO 2000-1 и/или чрез проверки, осъществявани от ДАЕУ.



Основни ИКТ процеси, свързани със сигурността, и взаимовръзките между тях

Високото ниво на МИС се гарантира посредством:

- **HelpDesk** е функционално звено – единна точка за контакт между потребителите на услугите на ЕУ и АО, отговорни за предоставянето и поддържането на тези услуги.

- **Управление на информационните ресурси (активите)** – осигурява точна и вярна информация за информационните активи, участващи в предоставянето на е-услуги, за техните конфигурации и документация, която да е в помощ на всички други процеси за управление на услугите.

Основните компоненти на процеса са:

- Регистър на информационните ресурси;
- софтуерна библиотека;
- базово ниво на конфигурациите;
- правила за управление на жизнения цикъл на информационните системи, гарантиращи конфиденциалността на информацията, която се създава, съхранява, пренася и унищожава с тях.

- **Управление на инцидентите** – осигурява намаляване на загубите чрез минимизиране на времето на влошаване на качеството на е-услугата или нейната недостъпност.

Основни дейности в процеса са:

- откриване на инцидент;
- регистриране на инцидент;
- докладване на инцидента на CERT;
- класифициране на инцидент;
- приоритизиране на инцидент;
- ескалация на инцидент;
- разследване на инцидент;
- събиране на доказателства;
- разрешаване на инцидент;
- затваряне на инцидент;
- регистриране на начините за разрешаване;
- последващи действия.

Всеки участник в предоставянето на услуги на електронното управление е длъжен да поддържа процес за управление на инциденти и да докладва всеки инцидент с мрежовата и информационната сигурност на екипите за реагиране при инциденти с компютърната сигурност по отрасли или на националния CERT.

- **Управление на проблеми**

Управлението на проблеми се дели на два типа – **реактивно** (разрешаване на проблеми след възникването на един или повече инциденти) и **проактивно** (идентифициране и решаване на проблеми, преди да са настъпили инциденти). Целта е да се намали до минимум въздействието на заплахите, да се повиши наличността и качеството на услугите, да се намали времето за разрешаване на проблеми, броят на инцидентите и разходите и загубите.

Процесът включва следните дейности:

- откриване на проблем;
- регистриране на проблем;
- категоризиране на проблем;
- приоритизиране на проблем;
- анализиране и диагностика;
- временно решение на проблем;
- създаване на запис за „известна грешка“;
- разрешаване на проблем;
- затваряне на проблем;
- основен преглед на проблемите;
- контрол на проблемите и управление на грешки.

- **Управление на измененията**

При всяко планирано изменение на хардуер, софтуер, свързаност, услуги и др. в инфраструктурата на ЕУ се прави анализ на риска, измененията се тестват и се информират всички засегнати страни. Целта е да се гарантира, че чрез стандартизирани методи и процедури ефективно и навременно се правят всички изменения, които няма да повлияят върху качеството на услугите, да се намали въздействието на инцидентите, свързани с измененията, и др.

Участници в процеса са представители на всички основни ИКТ структури, представители на бизнеса, представители на различни групи потребители и представители на разработчиците.

Процесът включва следните дейности:

- регистриране на изменение;
- одобрение на изменение;

- класификация на изменение;
- категоризация на изменение;
- планиране и одобрение;
- координация.

- **Управление на риска**

Анализ и оценка на риска се извършва съгласно стандарти ISO/IEC 27050-1:2016 и ISO 31000:2018. Процесът включва следните стъпки:

- идентифициране на ИС;
- идентифициране на уязвимости на тези ИС;
- идентифициране на заплахите към тези ИС;
- оценяване на риска за ИС;
- идентифициране на приложените мерки за защита;
- определяне на остатъчните рискове;
- определяне дали остатъчните рискове са приемливи;
- определяне на допълнителни защитни мерки за неприемливите рискове;
- планиране на прилагането им;
- прилагане на допълнителни защити;
- наблюдение.

- **Управление на актуализациите**

Фирмите, производители на софтуерни продукти, регулярно публикуват изменения (пачове, ъпдейти, нови версии) на софтуера, с които отстраняват известните уязвимости в сигурността. За гарантиране на високо ниво на защита от кибератаки е важно да се познава в детайли целият спектър софтуер, който се използва в предоставянето на е-услуги, неговите версии и къде е инсталиран.

Процесът включва следните дейности:

- проучване за актуализации на софтуерни продукти;
- тестване;
- планиране на актуализирането;
- извършване на актуализирането;
- наблюдение на функционирането.

- **Управление на непрекъснатостта**

За постигане на високо ниво на наличност на е-услуги се прилага:

- резервиране/архивиране на информация;
- планиране на информацията, технологията, периода и др.;
- проверка на годността на резервните копия;
- резервиране на системи;
- резервиране на устройства;
- балансиране на натоварването;
- резервиране на центрове за данни;
- планове за непрекъснатост на дейността.

5. Оперативна съвместимост

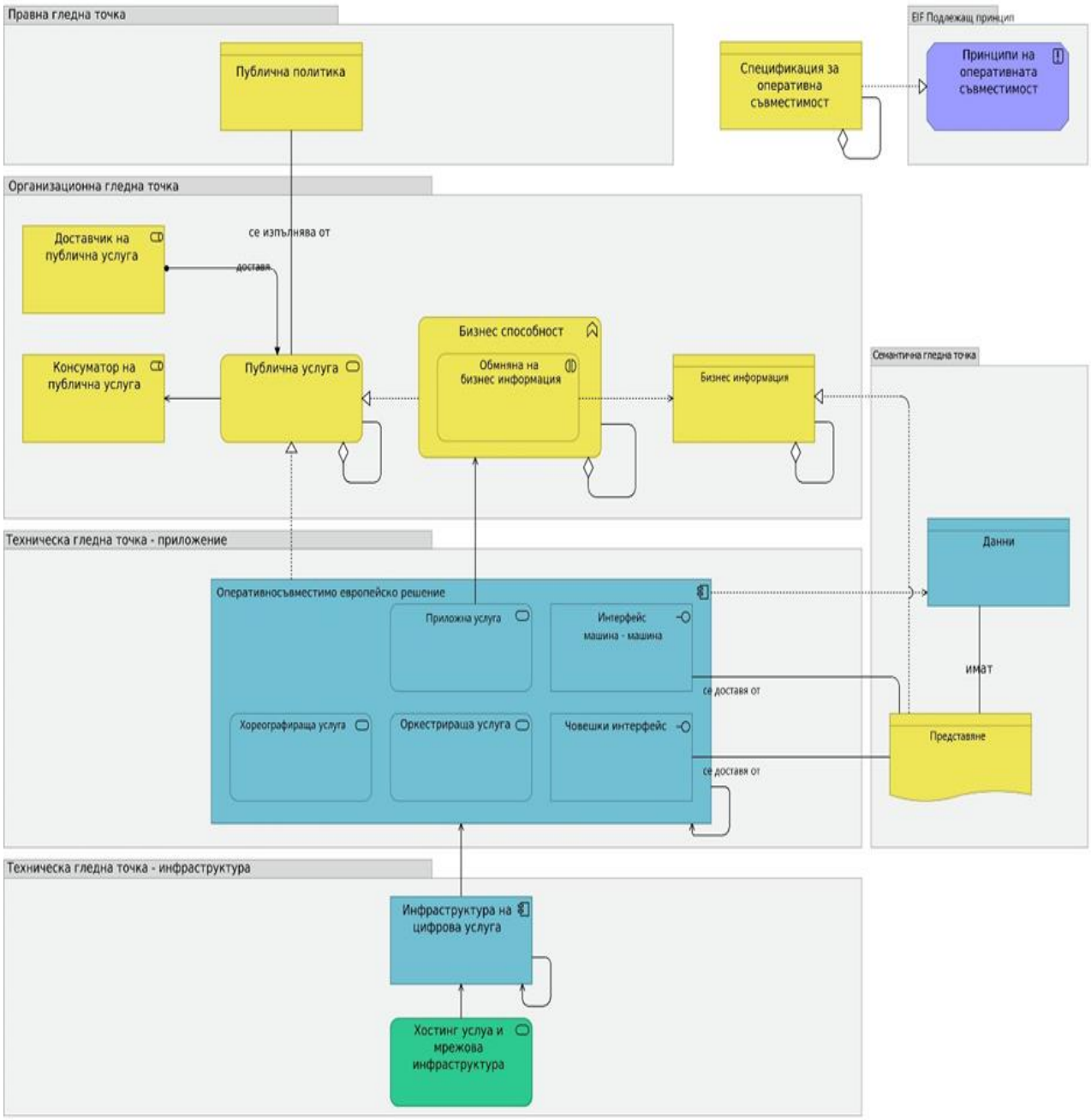
5.1. Същност на оперативната съвместимост

Оперативната съвместимост (ОС) е способността на организациите да си взаимодействат посредством обмен на данни между техните системи, базирани на ИКТ, за постигане на взаимно изгодни цели, включващи обмен на информация и знания между организациите чрез работните процеси, които те поддържат.

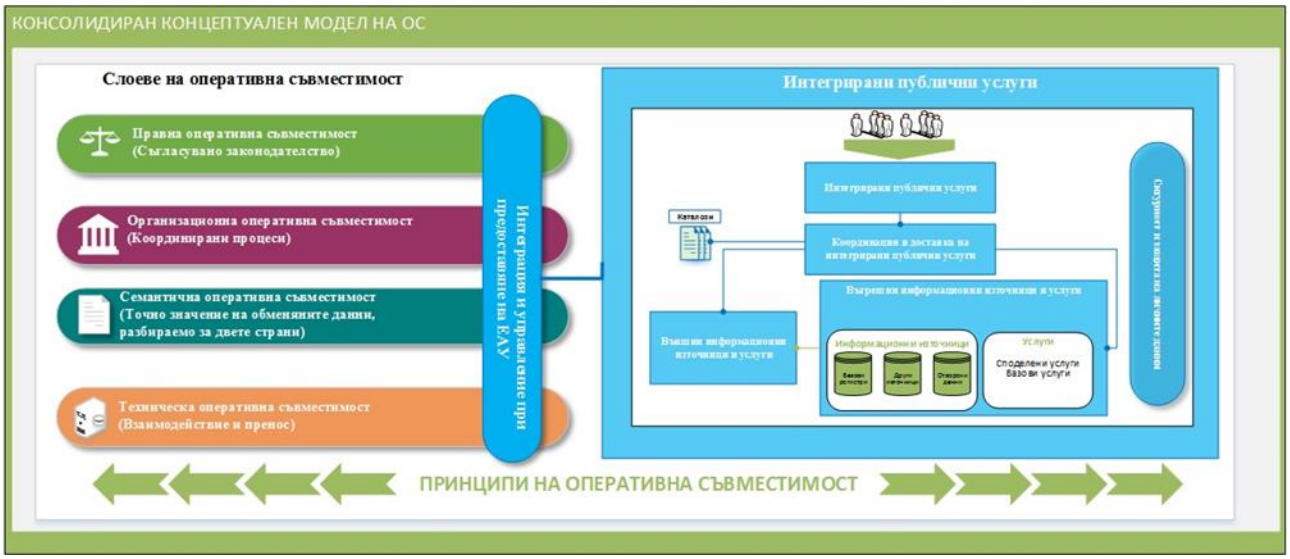
Оперативната съвместимост обхваща следните слоеве, които оказват въздействие върху ЕУ:

- *правна оперативна съвместимост (съгласувано законодателство)*;
- *организационна оперативна съвместимост (координирани процеси)*;
- *семантична оперативна съвместимост (точно значение на обменяните данни, разбираемо за страните*);
- *технологична оперативна съвместимост (взаимодействие и пренос)*.

Общ компонент на четирите слоя е процесът на интеграция и управление на ЕУ.



Мета модел на ОС (съгласно EIRA)



Консолидиран концептуален модел на ОС

Спазването на изискванията за оперативна съвместимост на национално ниво се гарантира в ЗЕУ чрез определяне на изискванията за:

- интеграция с хоризонталните системи на ЕУ;
- използване на централизирани системи на ЕУ;
- взаимодействие с ресурсите на ЕУ, единствено чрез интеграционния слой;
- удостоверяване на съответствието на информационните системи с изискванията за оперативна съвместимост, мрежова и информационна сигурност;
- контрол на спазване на изискванията за мрежова и информационна сигурност и оперативна съвместимост.

Семантична оперативна съвместимост

Семантична оперативна съвместимост е елемент на оперативната съвместимост, означаващ способността за еднаква интерпретация на едни и същи данни от различни информационни системи, като гарантира запазването и разбирането на точния им формат и значение при обмен. Семантичната оперативна съвместимост може да обхваща както семантичен, така и синтактичен аспект.

Информационните ресурси на семантичната оперативна съвместимост са метаданните за многократна употреба и сравнителните данни (класификатори, таксономии и др.). Метаданните са първоначалното ниво за постигане на семантична оперативна съвместимост. За да се постигне оперативна съвместимост на нивото на синтаксиса, предпоставката е създаване на хранилища на XML схеми. За целите на ЕУ съществуват следните видове семантични активи за оперативна съвместимост: метаданни, речници, класификации, таблици за преобразуване.

5.2. Регистри за оперативна съвместимост

Регистрите за оперативна съвместимост (РОС) и вписваните в тях обстоятелства и обекти са определени в ЗЕУ и подзаконовите нормативни актове към него. Свързан с РОС е Административният регистър, поддържан от АМС, част от който е Регистърът на услугите.

Достъпът до данните в РОС е чрез уеб услуги. Информацията за регистрите се съхранява в база данни. Обособени са области, които съхраняват данните за Регистъра на регистрите (РР), Регистъра на информационните обекти (РИО) и Административния регистър (АР).

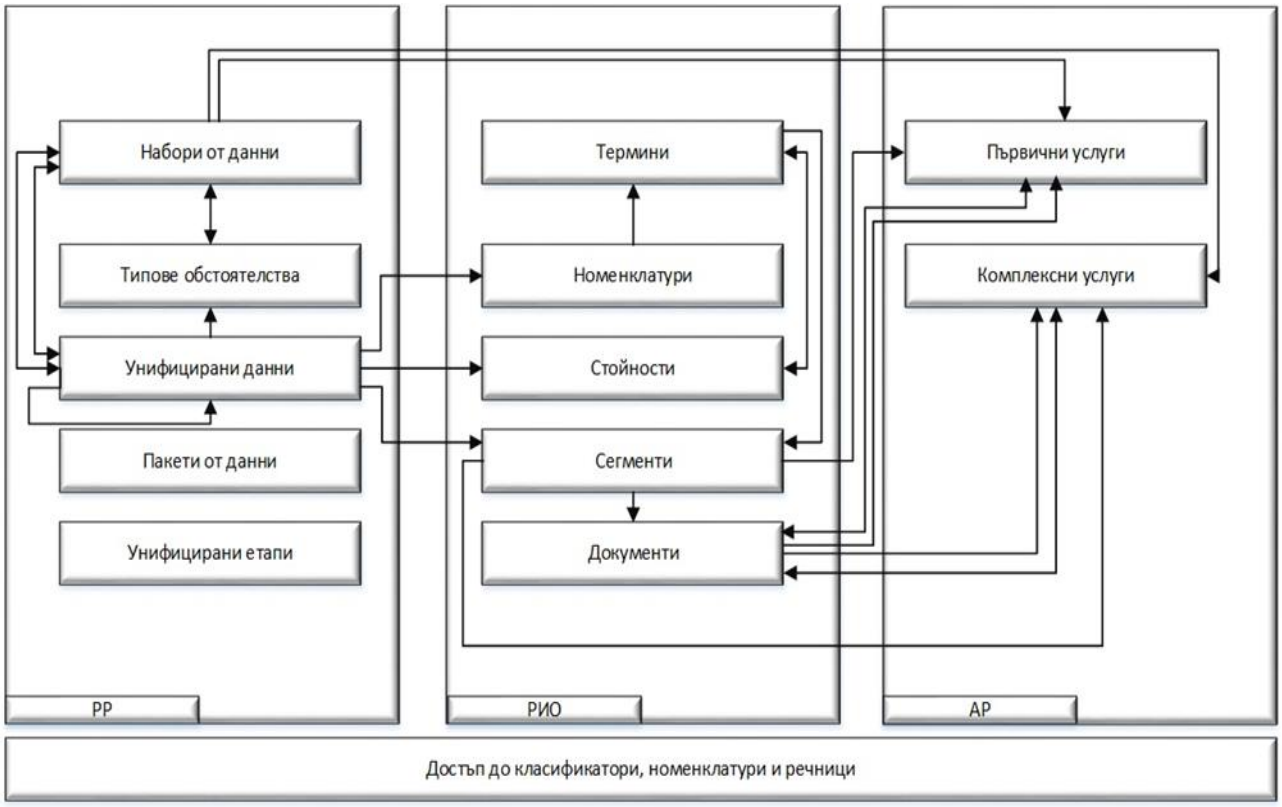


Схема на структурата и връзките между РР, РИО и АР

Основните регистри за оперативна съвместимост са:

- **Регистър на регистрите** – в него се вписват всички регистри и бази данни на ПАД, в които се съдържат първични данни, както и описание на структурата им. Компонентите на структурата трябва да са вписани предварително в РИО.

- **Регистър на информационните обекти** – чрез него се поддържат формализираните технологични описания на информационните обекти, събирани, създавани, съхранявани и обработвани от АО в рамките на тяхната компетентност. Тези определения на нормативно регулираните данни позволяват машинна обработка на тези данни, както и поддържане на препратки между унифицирани и формализирани определения на данни, което позволява недвусмислена интерпретация, както за машинна, така и за ръчна обработка.

Информационните обекти са: термин; номенклатура; стойност; сегмент; документ.

Формализираното описание на всеки информационен обект (ИО) е в XML схема (XSD).

Всички информационни системи на АО следва да се разработват съгласно обектите, вписани в регистъра.

- **Административен регистър** – в него се вписват всички услуги, предоставяни от лицата по чл. 1 от ЗЕУ за целите на административното обслужване.

- **Регистър на стандартите** – в него се вписват техническите стандарти, които трябва да се прилагат от АО за предоставяне на ЕАУ и за осигуряване на ОС, информационна сигурност и автоматизиран обмен на данни и документи между АО. Всички информационни системи на АО следва да се разработват съгласно стандарти, описани в Регистъра на стандартите.

- **Списък на удостоверените системи** – включва следните подсистеми: „Регистър на участниците“, „Регистър на обектния идентификатор“, „Регистър на ресурсите“, „Регистър

на информационните ресурси“, „Адресен регистър“, „Централизиран регистър за гражданска регистрация“ и др.

5.3. Номенклатури, класификатори и речници за семантична ОС

Администрацията работи с унифицирани данни, чиято структура се вписва в раздел пакети от данни от Регистъра на регистрите. В раздела се вписват условията и начинът за достъп до данните, включително период, през който са валидни, и история на промените.

Номенклатурите, класификаторите и речниците се поддържат от своите собственици – АО или организация, на които с нормативен или поднормативен акт е вменено задължение за поддържането им.

Дефинирана е структура, задължителна за всеки един пакет от данни. Така се гарантира еднозначност на интерпретацията на вписаните понятия, история на промените и спазване на изискванията на ЗЕУ.

6. Спецификации и Регистър на стандартите

Стандартите и спецификациите са основополагащи за оперативната съвместимост.

За нуждите на ЕУ се използват общоприети международни и европейски стандарти. При това стандартизацията обхваща по-широка област от тази на т.нар. „формални хармонизирани стандарти“, утвърждавани от официалните междуправителствени стандартизационни органи (като ISO, ITU на глобално ниво или CEN, CENELEC, ETSI – на европейско ниво). Тя включва неформални и хибридни стандартизационни процеси – продукцията на секторни консорциуми, като OASIS, IETF, W3Consortium, UN/CEFACT, OMG и др.

Управлението на стандартите за ЕУ се осъществява чрез Регистъра на стандартите, съдържащ техническите стандарти и спецификации, които трябва да се прилагат от АО за предоставяне на е-услуги, разработване на ИС, както и за осигуряване на оперативна съвместимост и мрежова и информационна сигурност. Регистърът е инструмент за практическо създаване и поддържане на стандартизация.

В Регистъра на стандартите са вписани обстоятелствата за стандарти от следните типове стандарти за:

- комуникация и процедури за обмен;
- уеб услуги;
- интеграция на данни;
- управление на документи, данни и съдържание;
- управление на съдържанието и дефиниции на метаданни;
- потребителски интерфейси;
- работни станции;
- вътрешна организация на дейността и работни процеси;
- управление на електронната идентичност;
- информационна сигурност.

В регистъра могат да се вписват и други обстоятелства, утвърдени от председателя на ДАЕУ.

Регистърът се поддържа от ДАЕУ и съдържа следните раздели:

- задължителни стандарти;
- препоръчителни стандарти;
- стандарти под наблюдение;
- спецификации на интерфейси и протоколи.

7. Нови технологии в електронното управление

7.1. Политика, базирана на данните

Политиката, базирана на данните, е **резултат от продължителни усилия** на АО. Нейната реализация е последователен процес, като всяка следваща стъпка надгражда над успехите от предходната:

- **използване на наличните данни** в рамките на самата организация и обработката им със сравнително директни аналитични методи: визуализация, описателни статистики, линейни статистически модели (корелация, регресия, дисперсия и др.);
- **свързване на базите данни от даден сектор** и изграждане на единен склад (хранилище) за данни, за поддръжка на визуализационни и аналитични функционалности;
- **разширяване на аналитичните функционалности** с използване на линейни и нелинейни методи за анализ (клъстерни анализи, анализ на времеви редове, класификационни методи, методи за машинно самообучение);
- **интеграция** с други бази данни и първични регистри за по-усложнено моделиране, симулации и визуализации;
- **изграждане на интелигентни системи за управление** – използване на изкуствен интелект за подпомагане на взимането на решения, за автоматична обработка на заявки, за извеждане на рискови фактори и компоненти, за управление на рисковете, за оптимизация на ресурсите, за предупреждение в реално време и др.

Важно е процесът на дигитална (цифрова) трансформация да бъде съпътстван от **оценка на ползите спрямо разходите**.

7.2. Използване на разпределени технологии в електронното управление

Блокчейн технологиите с т.нар. разпределен дневник (distributed ledger) вече се доказват като ефективно средство за гарантиране истинността на информацията и създаване на ефективни процеси, базирани на тази информация. Те са съвместими с конвенционалния хардуер и намаляват драстично изискванията към инфраструктурата.

Блокчейн технологиите позволяват пълна проследимост на операциите. Невъзможно е информация да бъде записана или обновена, без това да остави ясна следа кой, кога, откъде и как е направил тази промяна. Информация, записана в блокчейн, не може да се изтрие, нито да се модифицира. Ако това се случи, примерно при злонамерена атака, самата система недвусмислено ще установи, че има промяна, къде е промяната и ще откаже изпълнението на каквито и да е операции с цел защита от последваща деградация.

В случаите, когато регистър се поддържа от множество териториални звена или няколко администрации, всяка от които разполага с хардуерна инфраструктура, би следвало да се разгледа възможността за използване на блокчейн. Преминаването към блокчейн следва да бъде добре аргументирано и вземайки предвид готовността на изпълнителите в бранша да доставят качествени решения, базирани на тази технология.

7.3. Мобилно електронно управление

Масовото използване на мобилни електронно-съобщителни услуги налага електронното управление да акцентира върху ползвателите на тези услуги. Приложенията, предназначени за крайни потребители, следва да се разработват с възможности за използване както на стационарни компютри, така и на мобилни устройства. В някои случаи е полезно да се разработват решения, предназначени за ползване изключително на мобилни устройства.

7.4. Интернет на нещата

В индустрията и ежедневието активно навлизат „интелигентни“ или „умни“ (smart) устройства. Работи се усилено по теми като „умен град“ (smart city), интелигентен транспорт и интелигентни/автономни превозни средства. Постепенно тези технологии стават част от

електронното управление – реакция при инциденти с интелигентни устройства, вземане на управленски решения от машини (софтуер), засягащи други машини (автономни устройства), хора и други.

Интелигентните устройства генерират големи обеми от данни, които се предават по съществуващите комуникационни канали, съхраняват се в големи масиви от данни и са подходящи за обработка с технологии като изкуствен интелект, машинно обучение, обработка на данни с цел извличане на нова информация и познание и др.

7.5. Официални интернет страници на АО

Интернет страниците на АО служат за подобряване, насърчаване и реализиране на взаимодействието между АО и гражданите и бизнеса за целите на държавното управление, подобряване на информираността на обществото и насърчаване на обществената подкрепа, разбиране, съучастие и легитимност на осъществяваните публични политики.

АО проектират своите интернет страници, така че да обхващат всички техни потенциални потребители, като вземат под внимание възможните видове взаимодействие, особеностите на различни видове устройства, ниво на техническо познание, личностни и колективни интереси.

Структурата и съдържанието на интернет страниците трябва да бъдат достъпни за хора с увреждания, включително зрителни, слухови, познавателни, езикови, неврологични и други.

Интернет страниците на централните, териториалните и общинските администрации имат следните основни функции:

- информационна – представя услуги, политики и програми, новини; отговаря на често задавани въпроси и др.;
- административна – предоставя административни услуги по електронен път; подпомага предоставянето на административни услуги чрез пряко взаимодействие на потребителя с организацията („на гише“ или друго);
- представителна – формира и отразява организационната идентичност; отразява структурата, екипа и организационната логика на администрацията, както и единството в прилаганите от публичните организации политики на откритост, прозрачност и достъпност;
- комуникационна – предоставя информация и инструменти за дву- и многопосочна връзка с администрацията, насърчава общуването и разбирането между организацията и нейните публики, изгражда доверие, генерира подкрепа и участие.

Официалната институционална интернет страница на АО следва да има линк към институционалните страници в социалните мрежи.

V. Съкращения

CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Electrotechnique
CERT	Computer Emergecy Response Team
DB	Data Base
DMZ	DeMilitarized Zone
DNS	Domain Name System
DWDM	Dense Wavelengh Division Multiplex
eIDAS	Electronic IDentification, Authentication and trust Services
EIRA	Europian Interoperability Reference Architecture
ETSI	European Telecommunications Standards Institute
IaaS	Infrasrtructure as a Service
ID	Identifier
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standartization
MPLS	MultiProtocol Label Switching
NTP	Network Time Protocol
OASIS	Organization for the Advancement of Structured Information Standards
OMG	Object Management Group
PaaS	Platform as a Service
PBAC	Policy Based Access Control
SaaS	Software as a Service
SAN	Storage Area Network
SDH	Synchronous Digital Hierarchy
SFP	Small Form-factor Pluggable
SMS	Short Message Service
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
vApp's	Virtual Applications
VLAN	Virtual Local Area Network
VM's	Virtual machines
VPN	Virtual Private Network
XML	eXtensible Markup Language
XSD	XML Schema Definition
АМС	Администрация на Министерския съвет
АО	Административен орган
БДС	Български държавен стандарт
БК	Бюджетен контрол
БЛД	Български лични документи
ВЕАУ-ЕП	Вътрешни електронни административни услуги – електронна поща
ВЕС	Ведомствен експертен съвет
ГИМ	Главен информационен мениджър
ДАЕУ	Държавна агенция „Електронно управление“

ДОПК	Данъчно-осигурителен процесуален кодекс
ДП ЕСО	Държавно предприятие „Единен системен оператор“
ДХЧО	Държавен хибриден частен облак
ЕАУ	Електронни административни услуги
ЕЕСМ	Единна електронна съобщителна мрежа
еИД	Електронна идентичност
ЕИК	Единен идентификационен код
ЕИСУЧРДА	Единна интегрирана система за управление на човешките ресурси в държавната администрация
ЕПДЕАУ	Единен портал за достъп до електронни административни услуги
ЕРИКС	Екипи за реагиране при инциденти с компютърна сигурност
ЕРОС	Европейска рамка за оперативна съвместимост
ЕС	Европейски съюз
ЕСИФ	Европейски структурни и инвестиционни фондове
ЕУ	Електронно управление
ЗЕДЕУУ	Закон за електронния документ и електронните удостоверителни услуги
ЗЕИ	Закон за електронната идентификация
ЗЕУ	Закон за електронното управление
ЗИВ	Защитен интернет възел
ИИСДА	Интегрирана информационна система на държавната администрация
ИКТ	Информационни и комуникационни технологии
ИРЕУ	Информационни ресурси за електронно управление
ИС	Информационна система
ИСУН	Информационна система за управление и наблюдение на средствата от ЕС в България
ИТ	Информационни технологии
КЕП	Квалифициран електронен подпис
КИИ	Комуникационно-информационна инфраструктура
МВР	Министерство на вътрешните работи
МИС	Мрежова и информационна сигурност
МС	Министерски съвет
НАП	Национална агенция за приходите
НЗОК	Национална здравноосигурителна каса
НОИ	Национален осигурителен институт
НОИИСРЕАУ	Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги
НОИМИС	Наредба за общите изисквания за мрежова и информационна сигурност
НСОРБ	Национално сдружение на общините в Република България
ОКЛ	Оптична кабелна линия
ОПДУ	Оперативна програма „Добро управление“
ОС	Оперативна съвместимост
ПАД	Първичен администратор на данни
ПИК	Персонален идентификационен код
ПИН	Персонален идентификационен номер

ПМС	Постановление на Министерския съвет
ПРБ	Първостепенен разпоредител с бюджет
РИО	Регистър на информационните обекти
РОС	Регистър за оперативна съвместимост
РР	Регистър на регистрите
РС	Регистър на стандартите
СГИМ	Съвет на главните информационни мениджъри
СМИС	Система за мрежова и информационна сигурност
СОСП	Съобщителни обекти със специално предназначение
СУБД	Система за управление на база от данни
СЧ	Страни членки
ТД	Техническо досие
ТЗ	Техническо задание
ТП	Технически проект
УКД	Уникален код за достъп
УО	Управляващ орган
УРИ	Уникален регистров идентификатор
ЦСЕИ	Централизирана система за електронна идентификация