

- Определяне на концепция на информационната система на базата на техническата спецификация;
- Дефиниране на детайлни изисквания и бизнес процеси, които трябва да се реализират в системата;
- Дизайн на информационната система, хардуерната и комуникационната инфраструктура;
- Изготвяне на план за техническа реализация;
- Определяне на потребителския интерфейс.

При изпълнението на задачите ще се дефинират модели на бизнес процеси, модели на стандартни справки и анализи, модели на печатни бланки, политика за сигурност и защита на данните, основни изграждащи блокове, транзакции, технология на взаимодействие, мониторинг на системата, спецификация на номенклатурите, роли в системата и други. При документирането на изискванията, с цел постигане на яснота и стандартизация на документите, ще се използва стандартен език за описание на бизнес процеси – BPMN.

Системният проект подлежи на одобрение от Възложителя. В случай на забележки, корекции или допълнения от страна на Възложителя Изпълнителят ще ги отрази в системния проект в срок не по-късно от 10 работни дни.

Подробно описание на подхода за изпълнение на дейностите по проектиране може да бъде намерено в т. 7.1. „Предложение за извършване на дейностите по анализ и проектиране“

5.3. Разработване на софтуерното решение

Етапът на разработка включва изпълнението на следните задачи:

- Разработка на модулите на информационната система съгласно изискванията на настоящото техническо задание и системния проект;
- Провеждане на вътрешни тестове на Системата (в среда на разработчика);
- Изготвяне на детайлни сценарии за провеждане на приемателните тестове за етапи „Тестване“ и „Внедряване“ на проекта.

Подходът (Методологията) за разработка на софтуерното приложение е описан в т.7.2 „Предложение за извършване на дейностите по разработка на системата“

5.4. Тестване

По време на софтуерната разработка и след нейното приключване изпълнителят ще извърши обстойно тестване на Системата.

Изпълнителят ще предвиди време за отстраняване на възникнали проблеми при тестването или несъответствия в разработения софтуер.

Чл.36 а, ал. 3 от ЗОП

Изпълнителят ще проведе тестване на софтуерното решение в създадената тестова среда, с цел да се удостовери, че разработените програмни продукти са работоспособни и отговарят на изискванията на Възложителя. Това се постига чрез осъществяване на следните подцели на тестването:

- ✓ Откриване на всички грешки в кода, които екипът трябва отстранява;
- ✓ Откриване на грешки при дизайна;
- ✓ Откриване на повреди от неочаквано потребителско поведение;
- ✓ Тестване на всички елементи на решението.

Подробно описание на методологията за тестване и предварителен план за тестване може да бъде намерен в точка 7.2.3. „Методология за тестване“.

5.5. Внедряване

Изпълнителят ще внедри софтуерното решение в информационната и комуникационна среда на НСИ. Това включва инсталиране, конфигуриране и настройка на програмните компоненти на системата в условията на експлоатационната среда на НСИ.

Подробно описание на методиката за внедряване се намира в точка 8.2.2. от настоящия документ.

5.6. Обучение

Изпълнителят ще организира и да проведе бучения за всички видове потребители и ползватели, съответно:

- в Националния статистически институт

За провеждане на обученията, Изпълнителя ще осигури за своя сметка:

- Необходимия хардуер;
- Необходимия софтуер;
- Зала/Зали за провеждане на обученията;
- Учебни материали;
- Лектори.

Изпълнителя ще изготви и съгласува с Възложителя План и програма за обучение, спрямо която след одобрение ще бъдат организирани обученията на потребителите. Преди провеждане на обученията, Изпълнителят ще изготви и предаде на Възложителя следните документи, които ще бъдат използвани и като обучителни материали:

- Ръководство на администратора;
- Ръководство на потребителя, илюстрирано с графики/скрийншотове на системата;
- Описание на базата данни;
- Описание на софтуерните модули.

Чл.36 а, ал. 3 от ЗОП

Подробно описание на методиката за обучение може да бъде намерено в т. 8.2.11 от настоящия документ.

5.7. Гаранционна поддръжка

Изпълнителят ще извърши за своя сметка гаранционна поддръжка с 24-месечен гаранционен срок, след приемане в експлоатация на системата.

При необходимост, по време на гаранционния период ще бъдат осъществявани дейности по осигуряване на експлоатационната годност на софтуера и ефективното му използване от Възложителя, в случай че настъпят явни отклонения от нормалните експлоатационни характеристики, заложи в системния проект.

Изпълнителят ще предоставя услугите по гаранционна поддръжка, като предоставя за своя сметка единна точка за достъп за приемане на телефонни и e-mail съобщения.

Приоритетите на проблемите се определят от Възложителя в зависимост от влиянието им върху работата на администрацията. Редът на отстраняване на проблемите се определя в зависимост от техния приоритет.

Минималният обхват на поддръжката ще включва:

- Извършване на диагностика на докладван проблем с цел осигуряване на правилното функциониране на системите и модулите;
- Отстраняване на дефектите, открити в софтуерните модули, които са модифицирани или разработени в обхвата на проекта;
- Консултации за разрешаване на проблеми по предложената от Изпълнителя конфигурация на средата (операционна система, база данни, middleware, хардуер и мрежи), използвана от приложението, включително промени в конфигурацията на софтуерната инфраструктура на мястото на инсталация;
- Възстановяването на системата и данните при евентуален срив на системата, както и коригирането им в следствие на грешки в системата;
- Експертни консултации по телефон и електронна поща за системните администратори на Възложителя за идентифициране на дефекти или грешки в софтуера;
- Актуализация и предаване на нова версия на документацията на системата при установени явни несъответствия с фактически реализираните функционалности, както и в случаите, в които са извършени действия по отстраняване на дефекти и грешки, в рамките на гаранционната поддръжка.

6. СЪОТВЕТСТВИЕ С ОБЩИТЕ И СПЕЦИФИЧНИ ИЗИСКВАНИЯ КЪМ РЕАЛИЗАЦИЯТА НА СОФТУЕРНОТО РЕШЕНИЕ

6.1. Общи изисквания

Информационната система “Образование” ще бъде изградена като ясно обособени и логически свързани части на функционалните компоненти “Зареждане на данни”, “Редактиране на данни”, “Обработка на данни” и “Изходи и справки” на бизнес процеса на статистическите изследвания;

Информационната система ще бъде изградена като отворена система, даваща възможност за разширяване на обхвата и промяна в информационното съдържание на обектите, данни за които се поддържат и обработват от системата, при промяна на законови, нормативни и други правови актове – след допълнително разработване;

Информационната система “Образование” ще бъде изградена на базата на многослойна компонентна архитектура, за да се обезпечи гъвкавост и повторно използване на софтуерни компоненти;

Информационната система “Образование” ще бъде централизирана система с децентрализиран достъп. Системата ще бъде базирана на централна база данни в Националния статистически институт – София, като достъпът до информацията е през Интернет.

Публичността на информационната система ще бъде в рамките на изискванията на Закона за статистиката за конфиденциалност на индивидуалната информация за наблюдаваните единици;

Информационната система ще осигурява ефективна защита на информационния достъп. Достъпът до системата ще бъде възможен само след предварително регистриране на потребителя и определяне на неговите права.

6.2. Функционални изисквания

6.2.1. Зареждане на данни

6.2.1.1. Зареждане на първични данни от МОН

Функционалността ще позволява на администратор от ЦУ да зареди в БД на системата данни, предоставени от МОН във вид на текстови файл с данни. Файловете с данни следват предварително зададена структура (тип полета, възможни стойности, номенклатури). Системата ще извършва синтактична проверка на данните (брой полета и данни-типове на полетата) и ги зареди в съответните регистри.

6.2.1.2. Ръчно въвеждане и актуализиране на данни

Функционалността ще позволява ръчно въвеждане/ редактиране/ изтриване на данни към вече заредените от файловете на МОН, чрез интерфейса на системата.

Ръчна промяна или добавяне на записи се налага само в редки и специални случаи, когато получените данни не са достатъчно прецизни или е налице недообхват (например, допълване на записи за духовните висши училища). Поради тази причина, за извършване на ръчна промяна на данни в системата ще се изисква служителят да притежава специални права на достъп.

Чл.36
а, ал.
3 от
ЗОП

Чл.36 а, ал. 3 от ЗОП

6.2.1.3. Повторно зареждане на данни

При открити сериозни неточности, несъответствия (например при брой полета и данни-типове на полетата) или липсващи стойности, системата ще позволява повторно зареждане на данните, чрез „припокриване“ – изтриване на първоначално заредените и зареждане отново.

6.2.2. Редактиране на данни

6.2.2.1. Логически контрол

Функционалността позволява, да се извърши логически контрол и да обработи запис от заредените данни. Логическият контрол се извършва по заложен в системата алгоритми, които са дефинирани от НСИ и е специфичен за отделните типове записи.

При успешно преминаване през контролите, системата регистрира записа в съответния регистър и маркира първичният запис като успешно обработен. При неуспешно преминаване през логическият контрол, системата маркира записа като проблемен и регистрира в БД текстово описание на проблема.

Основни логически контроли са:

- проверка за пълнота на полетата;
- проверка за възможни стойности в отделните полета;
- проверка за уникалност на записите (наличие на дублирани записи);
- проверки между свързани полета или записи, като тези контроли ще бъдат дефинирани допълнително при разработването на системата.

6.2.2.2. Генериране на справка-контролен журнал за проблемни записи

Функционалността ще позволява да бъде генерирана справка за записите от МОН, при логическия контрол, на които са констатирани проблеми. Справката се генерира върху записите от указана година, тип и/или регион и извежда списък на проблемните съобщения и текстови описания на проблемите. Справката може да се генерира по всяко време след като вече е извършен логически контрол и обработка на записите.

6.2.2.3. Редактиране на проблемни записи

Функционалността ще позволява, да бъдат коригирани ръчно първичните данни на проблемни записи, да се анулира неуспешно обработен запис или да се въведе (регистрира) ръчно нов запис. Системата ще позволява коригиране/анулиране само на записи, които не са преминали успешно логическите контроли и не са регистрирани съответни в съответните регистри на наблюдение. Необходимите действия се извършват директно в БД на системата.

6.2.3. Създаване на крайни регистри (модули)

Системата дефинира и зарежда релационна БД с обработени микроданни в следните крайни регистри, свързани с различните видове данни:

- Предучилищно образование – образователни институции;
- Предучилищно образование – записани деца;

Чл.36 а, ал. 3 от ЗОП

- Предучилищно образование – персонал;
- Училищно образование – образователни институции;
- Училищно образование – записани ученици;
- Училищно образование – персонал;
- Училищно образование – завършили образование и обучение ученици;
- Висше образование – образователни институции;
- Висше образование – записани студенти;
- Висше образование – персонал;
- Висше образование – дипломирани студенти;
- Докторанти – образователни институции;
- Докторанти – записани (зачислени) докторанти;
- Докторанти – дипломирани докторанти;
- НАЦИД – Академично признати дипломи за висше образование.

Между отделните регистри ще съществува релейна връзка.

6.2.4. Обработка на макроданни

Системата ще разполага с функционалност за дефиниране и обработване на агрегирани данни, изчислени на база на информацията, съхранявана в отделните регистри на наблюдение, които са в обхвата на настоящата система.

Тази функционалност ще бъде реализирана от системата чрез интегриране на готов OLAP-продукт, притежаващ възможности за:

1) Изграждане и поддържане на аналитична база данни:

- Дефиниране на многомерна база данни;
- Дефиниране на дименсии в многомерна БД;
- Дефиниране на кубове с агрегирани данни.
- Извличане на данни от релационни и нерелационни източници на данни;
- Агрегиране на извлечените данни;
- Зареждане на агрегирани данни в многомерна БД;
- Съхраняване на многомерна БД като таблици в релационна СУБД;

2) Наличие на средство за аналитични обработки на данни (OLAP):

- Създаване на OLAP-модели;
- Наличие на графичен интерфейс за работа с OLAP-структурите;
- Притежава система за архивиране и възстановяване на данни и експортиране в ASCII файл;
- Извършване на многомерен анализ върху многомерни БД;

Чл.36 а, ал. 3 от ЗОП

- Притежава набор от визуални и аналитични средства, осигуряващи възможност за избор, представяне, манипулиране, визуализация и анализ на данните;

- Притежава средство за генериране на отчети;

- Притежава административно средство за управление на потребители, групи от потребители и връзки към базата данни.

6.2.5. Поддържане, актуализиране и ползване на статистически класификации

ИС "Образование" ще използва набор от статистически класификации със запазена история на промените. Системата ще поддържа собствена релационна БД с копия на необходимите ѝ статистически класификации във формат, който е максимално подходящ за извършваните транзакционни обработки на първичните данни на наблюденията.

6.2.5.1. Администриране на статистически класификации

Функционалността ще позволява на администратор от ЦУ да извърши дейности по администриране на статистическите класификации - дефиниране на статистическа класификация, зареждане на стойности на елементи, добавяне / промяна / обединяване на елементи и др.

6.2.5.2. Актуализиране на наблюдавани обекти при промени в статистически класификации

Функционалността ще включва действията по актуализиране на данни за обекти на наблюдение, поддържани от ИС "Образование", при евентуална промяна на статистическа класификация. Такова актуализиране се извършва за обектите, за които системата трябва да поддържа актуални към настоящия момент версии на данните.

Актуализирането на обектите се извършва синхронно с актуализирането на поддържаните от системата копия на статистически класификации. При настъпили промени в класификация системата при необходимост актуализира данните на засегнатите обекти и регистрира записи в историята на промените им, за да позволи извършване на справки за тези обекти към минал момент от времето.

6.2.6. Администриране и поддържане на системата

Служебни дейности, свързани с администриране и поддържане на системата:

- Администриране на релационната и многомерната БД;
- Администриране на потребители;
- Архивиране и възстановяване на БД (backup / recovery);
- Експортиране и зареждане на данни структури в БД (export / import).

6.2.7. Интеграция с външни информационни системи

Изпълнителят ще реализира интерфейс за обмен на данни под формата на електронна услуга, който да бъде единна точка за обмен на данни между Системата и други системи.

Чл.36
а, ал.
3 от
ЗОП

Чл.36 а, ал. 3 от ЗОП

Ще бъде поддържана интеграция в реално време с информационни системи на други администрации:

Системата ще осигурява връзка с външни за НСИ системи и ще поддържа интеграция в реално време съгласно споразумението за сътрудничество и обмен на данни между НСИ и МОН, където МОН предоставя на НСИ индивидуални (включително лични данни) от следните информационни системи и регистри

- Национална електронна информационна система за предучилищното и училищното образование (НЕИСПУО);
- 2. Регистрите по чл. 10, ал. 2, т. 3, букви „а“, „б“, „в“ и „г“ от Закона за висшето образование, а именно: Регистър на акредитираните висши училища, Регистър на академичния състав на висшите училища, Регистър на всички действащи и прекъснали студенти и докторанти и Регистър на завършилите студенти и докторанти;
- 3. Регистър на „Защитени дисертационни трудове и лица на академични длъжности“;
- 4. Регистър на признатите дипломи за висше образование, придобито в чуждестранни висши училища;
- 5. Регистър на професионалните колежи.

За интеграцията с външни системи и регистри ще бъде реализиран стандартен интеграционен слой.

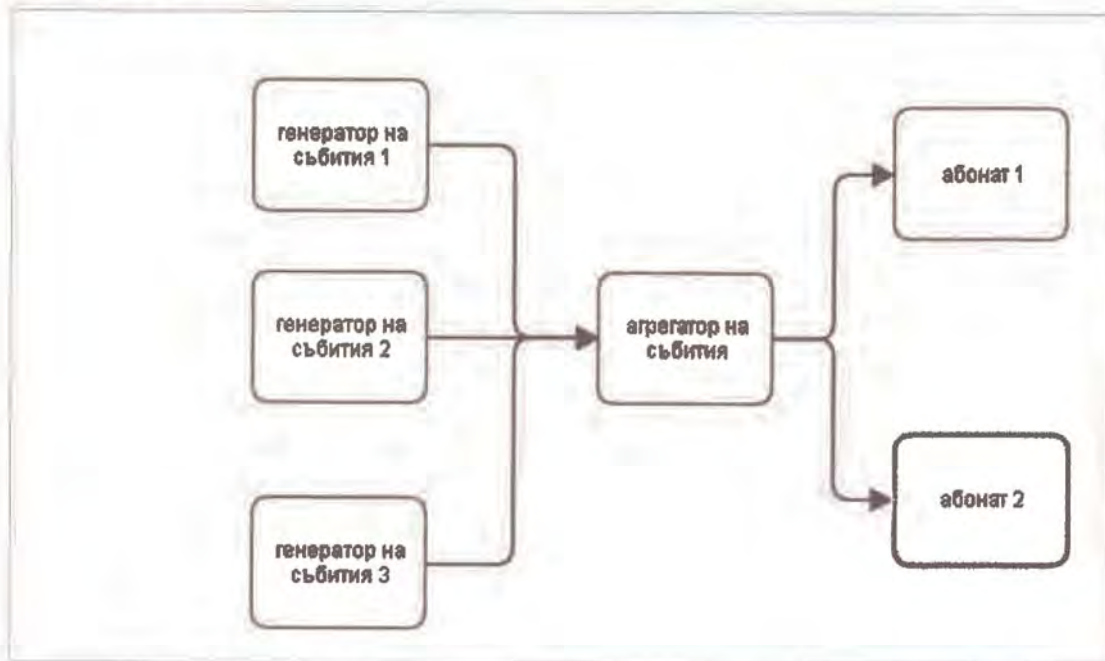
Обмена на данните ще се извършва автоматично на ниво БД НСИ-БД МОН използвайки механизмите на използваните СУБД. Достъпа на данните ще се извършва по защитен комуникационен канал (VPN) , като се приложат добрите практики за защита на предаваната информация за да се гарантира сигурността и интегритета (цялостност) на данните.

6.2.8. Интеграционен слой

- Ще бъде разработен и внедрен служебен онлайн интерфейс за машинен обмен на данни и предоставяне на вътрешно-административни електронни услуги към информационни системи и регистри на други администрации, публични институции и доставчици на обществени услуги, съгласно действащите изисквания за оперативна съвместимост. Предвидена е интеграция с първични регистри чрез стандартен междинен слой или чрез националната схема за електронна идентификация – конкретната реализация трябва да бъде одобрена от Възложителя след приключване на етапа на бизнес-анализ;
- Ще бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано изпращане на транзакционна история към системата за електронна идентификация, съгласно действащите изисквания за оперативна съвместимост;

В процеса на обработка на данни в системата се стига до изпълняване на условия, при които следва да се извърши трансфер на данни към външни системи. В последващото описание разглеждаме тази съвкупност от условия като "интеграционни събития", а обменът на данни с външна система – като "интеграционен трансфер"

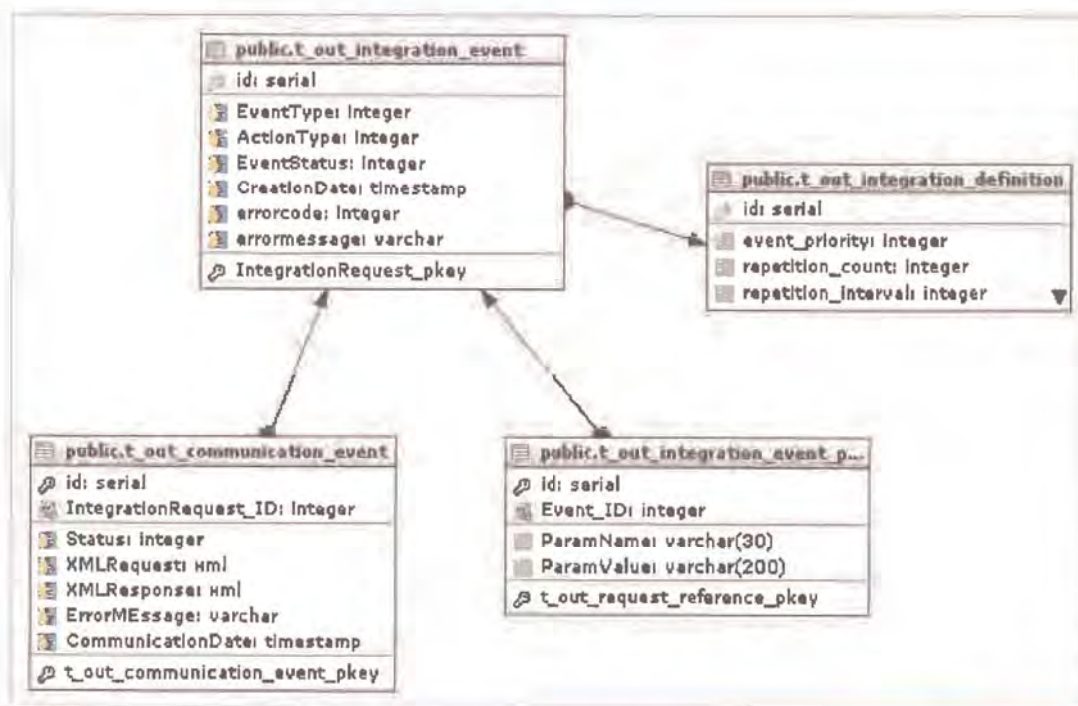
Архитектурата на модулът за интеграция с външни системи е базирана на модела "Агрегатор на събития". Моделът "Агрегатор на събития" се опитва да преодолее ограничаването на традиционния подход за управление на събития, като предостави централно място за публикуване и абониране за събития, които не са нищо друго освен събитие за събития. Агрегаторът за събития се грижи за регистрирането, отписването и извикването на събития, които свободно свързват генераторите на събития и абонатите. На диаграмата по-долу е показана принципна схема на типичен агрегатор на събития в приложение или система.



Фигура 13 Принципна схема на агрегатор на събития в система

Услугата EventAggregator е преди всичко контейнер за събития, които позволяват отделяне на връзките между генераторите и абонатите, така че те да могат да се развиват самостоятелно. Това отделяне е полезно при модулни приложения, защото могат да се добавят нови модули, които отговарят на събитията, дефинирани от ядрото или от други модули.

В контекста на интеграцията на системата с външни системи моделът за агрегиране на събитията ще се реализира по следния начин: генерирането на събития ще е достъпно в Системата посредством специализирано API, даващо възможност за създаване и съхраняване на събития в момента на възникването им, като моделът на данните позволява да се въведат неограничен брой параметри-референции, отразяващи контекста на събитието.



Фигура 14 Модел на данни на общия интеграционен компонент.

На ниво СУБД генерираните събития се съхраняват в таблица **t_out_integration_event**, като в таблица **t_out_integration_event_parameters** се съхраняват параметри-референции във формат ключ/стойност. Параметрите позволяват на модулът за интеграция да възстанови контекста на данните при възникването на събитието – в най-общия случай като параметри се използват уникални идентификатори на информационните обекти в базата данни.

Отделните специфични интеграции към всяка външна система се реализират като програмен код (клас), имплементиращ стандартен интерфейс по отношение на агрегатора на събития, и съдържащ специфична част за осъществяване на конкретната интеграция. Специфичната част най-често представлява web/wcf клиент или REST API комуникатор, като конкретната имплементация е независима и архитектурата позволява добавянето на бъдещи интеграции.

Диспечер на задачите обработва постъпилите събития, като в зависимост от техния тип и допълнителните метаданни от таблица **t_out_integration_definition** приоритизира събитията, определя типа абонат (интегратор) и извикват стандартния дефиниран в интерфейса метод за извършване на интеграцията – генериране на дейта трансфер обекти, извикване на външни уеб услуги със съответната автентификация и отразяване на резултата от комуникацията с външната система.

Самият процес на комуникация, генерираните XML или JSON пакети и възникналите грешки се отразяват в таблица **t_out_communication_event**.

Диспечерът на задачите по интеграцията е имплементиран под формата на системна услуга на операционната система.

Към модулет за интеграция ще се реализира и набор от споделен между отделните интеграции програмен код с общо предназначение – библиотеки, помощни класове и като цяло инфраструктура за работа с уеб услуги, автентикация със и управление на сертификати, криптиране и тунелиране.

Модулет за интеграция ще предоставя потребителски интерфейс на системните администратори за преглед на текущия статус на комуникациите, изпълнените събития и възникналите грешки, както и справки за изминали периоди.

Основните предимства на избрания подход са следните:

- реализацията на интеграцията е отделена от бизнес логиката за съхраняване и управление на основните данни на Системата
- процесът на обмен на данни с външните системи може да се извършва в асинхронен режим. В случай на загуба на свързаност с външните системи интеграционните събития се запазват и трансферът на данните се осъществява при възстановяване на свързаността.
- налице е пълна хронологична проследяемост на трансфера на данните и възникналите грешки
- при евентуално бъдещо добавяне на нови външни системи голямата част от програмният код остава непроменена и изтествана (API за генериране на събития и диспечера за задачите) което намалява значително разходите за подобни дейности.

6.2.9. Технически изисквания към интерфейсите

Приложните програмни интерфейси ще отговарят на следните архитектурни, функционални и технологични изисквания:

- Служебните онлайн интерфейси ще бъдат реализирани като уеб-услуги (web-services), осигуряващи достатъчна мащабируемост и производителност за обслужване на синхронни заявки (sync pull) в реално време, с максимално време за отговор на заявки под 1 секунда за 95% от заявките, които не включват запитвания до регистри и външни системи.
- Изпълнителят ще обоснове прогнозирано натоварване на системата и ще предложи критерии за оценка на максимално допустимото време за отговор на машинна заявка. Критерият за оценка ще се основава на анализ на прогнозираното натоварване и на наличния хардуер, който ще се използва. Изпълнителят ще представи обосновано предложение за минималното време за отговор на заявка на базата на посочените по-горе критерии и да осигури нужните условия за спазването му, като същото ще се съблюдава във фазата на разработка;
- Всички служебни онлайн интерфейси ще поддържат режим “push” или “pull”, в асинхронен и синхронен вариант. На етап бизнес-анализ ще бъде определено практическото прилагане на всяка от комбинациите, съобразена с реални казуси (use

Чл.36 а, ал. 3 от ЗОП

cases), които всеки интерфейс обслужва.

- Ще бъде предвидено създаването и поддържането на тестова среда, достъпна за използване и извършване на интеграционни тестове от разработчици на информационни системи, включително такива, изпълняващи дейности за други администрации или за бизнеса, с цел по-лесно и устойчиво интегриране на съществуващите и бъдещи информационни системи.

Потребителският интерфейс на системата ще използва опростена навигационна структура, базирана на едно меню за достъп до функционалностите на системата, филтрирано според потребителския профил на потребителя и със структура базирана на MenuProvider клас, позволяващ лесно управление и преконфигуриране на системното меню от административния панел.

6.2.10. Електронна идентификация на потребителите

Електронната идентификация на всички потребители ще бъде реализирана в съответствие с изискванията на Регламент ЕС 910/2014 и Закона за електронната идентификация, както и съгласно Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги (Приета с ПМС № 3 от 9.01.2017 г., обн., ДВ, бр. 5 от 17.01.2017 г., в сила от 1.03.2017г.), като при това следва да се спазят и изискванията на Наредбата, чл.6 - Идентификация на регистрите и базите данни, Наредбата, чл.7 – Достъп до регистрите и базите данни, Наредбата, чл.8 – Условия за достъп, Наредбата, чл.9 – Удостоверителни административни услуги и Наредбата, чл.10 – Идентифициране на информационните системи.

Забележка:

Задължението за вход по реда на Закона за електронната идентификация в системи за електронен документооборот по чл. 34, ал. 2 от наредбата влиза в сила от Януари 2019 г. В срок до 1 август 2018 г. за идентификация на физически лица, освен по реда на Закона за електронната идентификация и други методи, определени със закон, може да се прилага и прочитане на личен идентификатор от квалифициран електронен подпис.

- Процесът по регистрация на потребители ще бъде максимално опростен и бърз, но ще включва следните специфични стъпки:
 - Визуализиране на информация относно стъпките по регистрация и информация във връзка с процеса за потвърждаване на регистрацията и активиране на потребителския профил. Съвети към потребителите за проверка на настройките на имейл клиентите, свързани с блокиране на спам, и съвети за включване на домейна на Възложителя в "бял списък";
 - Избор на потребителско име с контекстна валидация на полетата (in-line validation), включително и за избраното потребителско име;
 - Избор на парола с контекстна валидация на полето (in-line validation) и

Чл.36
а, ал.
3 от
ЗОП

Чл.36 а, ал. 3 от ЗОП

визуализиране на сложността на паролата като "слаба", "нормална" и "силна";

- Реализиране на функционалност за потвърждение и активиране на регистрацията чрез изпращане на съобщение до регистрирания имейл адрес на потребителя с хипер-линк, с еднократно генериран токен с ограничена времева валидност за потвърждение на регистрацията. Възможност за последващо препращане на имейла за потвърждение, в случай че е бил блокиран от системата на потребителя.

6.2.11. Формиране на изгледи

Потребителите на Системата ще получават разреди на информацията чрез добавени възможности за филтриране, пренареждане и агрегиране на данните. Резултатите ще бъдат представяни чрез:

- Визуализиране на таблици;
- Графична визуализация на екран;
- Разпечатване на хартиен носител;
- Експорт на данни в един или в няколко от изброените формати – ODF, Excel, PDF, HTML, TXT, XML, CSV.

6.2.12. Администриране на Системата

Системата ще разполага с функционалност осигуряваща администриране на потребителите и правата за достъп.

Тази функционалност ще позволява на Администраторите на системата да извършват следните дейности по администриране на потребители на системата:

- Регистриране на нов потребител;
- Деактивиране на потребител;
- Активиране на потребител;
- Предоставяне/отнемане на права на достъп на потребител;
- Промяна на парола на потребител (може да се изпълнява и от съответния потребител).
- дефиниране на потребителски роли

6.3. Нефункционални изисквания към информационната система

Системата ще бъде разработена на база на съвременните ИТ стандарти, технологични средства и най-добри практики. Подходът при разработката ще позволява поэтапно разработване, бъдещо разширение и развитие. Системата ще осигурява гъвкав механизъм за обмен и интеграция на данни с външни информационни системи, чрез стандартизиран формат и механизъм за обмен на данни.

Системата ще отговаря на нефункционалните изисквания, описани както следва:

Изисквания към потребителския интерфейс

- Системата ще бъде интуитивна;
- Системата ще предостави интегриран потребителски интерфейс на български език;
- Системата ще предоставя достъп само до опции в менюта и право на достъп до функционалности, съответстващи на правата на съответния потребител;
- Системата ще предостави потребителски интерфейс, осигуряващ контекстно-зависима помощ. Контекстно-зависимата помощ ще бъде лесно достъпна за потребителя;
- Потребителският интерфейс ще бъде оптимизиран за ускорено въвеждане на данни;
- В графичния интерфейс ще се предвиди такова подреждане на полетата, че да се ограничи дължината на вертикалния скрол (scroll) и ще изключва появата на хоризонтален скрол (scroll);
- Системата ще осигурява лесна отмяна на действия;
- Системата ще изисква задължително потвърждаване при необратими действия;
- Системата ще да поддържа функции copy / paste на обектите;
- Системата ще предоставя възможност за извършване на процедури по IMPORT / EXPORT на данните от файлове, структурирани по зададени от НСИ критерии.

Експлоатационни изисквания

- Системата ще предоставя възможност на оторизираните потребители за бърз достъп до функционалностите;
- Потребителите на системата ще могат да я ползват с помощта на кратка инструкция;
- Системата ще има адекватна производителност, съобразена с очакваното натоварване;
- Системата ще бъде на разположение и в експлоатация във времето, когато се използва от потребителите. Няма да се допуска липса на услугата по време на очакваните периоди на пиково натоварване;
- Системата ще бъде способна да се възстановява ефективно след повреди, съгласно изискванията на стандарт БДС EN ISO/IEC 27001:2017 и закона за електронното управление;
- Системата ще предоставя функционалност за създаване на архивни копия на данните;
- Системата ще предоставя функционалност за възстановяване на данни от архивни копия;

Чл.36 а, ал. 3 от ЗОП

- Системата ще обезпечава процеса на поддръжка и актуализация на заложените системни модели при смяна на законовата и подзаконовата нормативна база в Република България и ЕС;
- Всички web интерфейси на системата ще са съвместими и ще работят с най-разпространените интернет браузъри;
- Съществуващи приложения и миграция на данни:
 - Системата и системните компоненти ще бъдат внедрени без прекъсвания в работата на НСИ;
- Системата ще бъде проектирана по начин, позволяващ интеграция с другите системи на НСИ без извършването на скъп реинженеринг.
- Системата ще гарантира целостта и непротиворечивостта на данните в БД чрез следните средства:
 - Дефиниране и прилагане на набор от правила за валидност на данните и операции (логически контроли);
 - Недопускане на директно добавяне/редактиране/изтриване на данни в Крайните регистри, заобикаляйки дефинираните правила за логически контрол на данните.
- Системата ще осигури цялостност на данните в конкурентен многопотребителски режим на работа. Системата няма да допуска паралелно извършване от различни потребители на промени върху едни и същи данни в БД.

6.3.1. Авторски права и изходен код

- Всички компютърни програми, които се разработват за реализиране на системата, ще отговарят на критериите и изискванията за софтуер с отворен код.
- Изключителното право на собственост принадлежи на Възложителя - всички авторски и сродни права върху произведения, обект на закрила на Закона за авторското право и сродните му права, включително, но не само, компютърните програми, техният изходен програмен код, структурата и дизайнът на интерфейсите и базите данни, чието разработване е включено в предмета на поръчката, възникват за Възложителя в пълен обем без ограничения в използването, изменението и разпространението им и представляват произведения, създадени по поръчка на Възложителя съгласно чл. 42, ал. 1 от Закона за авторското право и сродните му права.
- Приложимите и допустими лицензи за софтуер с отворен код са:
 - GPL (General Public License) 3.0
 - LGPL (Lesser General Public License)
 - AGPL (Affero General Public License)

Чл.36 а, ал. 3 от ЗОП

- Apache License 2.0
- New BSD license
- MIT License o Mozilla Public License 2.0
- EUPL (European Union Public License)

За създаване на софтуерното решение, Изпълнителят ще използва базови софтуерни платформи с отворен код, които имат разработена техническа документация за актуалната стабилна версия, възможност за предоставяне на комерсиална поддръжка и са подкрепени от организации с идеална цел или комерсиални организации, а именно Microsoft .NET Framework Core, Entity Framework Core.

- Изходният код (Source Code), разработван по проекта, както и цялата техническа документация ще бъдат публично достъпни онлайн като софтуер с отворен код от първия ден на разработка чрез използване на система за контрол на версиите и хранилището по чл. 7в, т.18 от ЗЕУ;

Проектът ще използва публично достъпни софтуерни библиотеки с отворен код за визуализация и подобряване на усещанията на потребителя.

При предоставяне на изходния код и документацията при условията на EUPL лиценз (Публичен лиценз на ЕС) ще се приложи пряко Решение за изпълнение (ЕС) 2017/863 от 18 май 2017 год. на ЕК за актуализиране на лиценз за софтуер с отворен код с цел допълнително улесняване на споделянето и повторната употреба на софтуер, разработен от публични администрации. Решението включва допълнение със „съвместими лицензи“ което осигурява оперативна съвместимост със списък на други „споделени сходни“ лицензи.

Ще се изследва възможността резултатният продукт (системата) да се изгради частично (библиотеки, пакети, модули) или изцяло на базата на съществуващи софтуерни решения, които са софтуер с отворен код. Когато е финансово оправдано, ще се предпочита този подход пред изграждането на собствено софтуерно решение в цялост, от нулата.

- Предвижда се използването на Система за контрол на версиите и цялата информация за главното копие на хранилището, прието за оригинален и централен източник на съдържанието, ще бъде достъпна публично, онлайн, в реално време. По-подробно описание може да бъде намерено в т.7.2.1.4 “ Процедура за управление на програмния код „ от настоящото предложение.

6.3.2. Системна и приложна архитектура

По отношение на системната архитектура приложението ще спазва следните изисквания посочени от Възложителя в техническата спецификация:

- Системата ще бъде реализирана като разпределена модулна информационна система. Той ще бъде реализиран със стандартни технологии и ще поддържа общоприети комуникационни стандарти, които ще гарантират съвместимост на системата с бъдещи разработки. Съществуващите модули и функционалности ще бъдат рефакторирани и/или надградени по начин, който да осигури изпълнението на настоящето изискване.
- Бизнес процесите и услугите ще бъдат проектирани колкото се може по-независимо с

Чл.36 а, ал. 3 от ЗОП

цел по-лесно надграждане, разширяване и обслужване. Системата ще е максимално параметризирана и ще позволява настройка и промяна на параметрите през служебен (администраторски) потребителски интерфейс.

- Ще бъде реализирана функционалност за текущ мониторинг, анализ и контрол на изпълнението на бизнес процесите в системата.
- При разработката, тестването и внедряването на системата, Изпълнителят ще прилага наложени се архитектурни (SOA, MVC или еквивалентни) модели и дизайн-шаблони, както и принципите на обектно ориентирания подход за разработка на софтуерни приложения.
- Системата ще бъде реализирана със софтуерна архитектура, ориентирана към услуги – Service Oriented Architecture (SOA).
- Взаимодействията между отделните модули в системата и интеграциите с външни информационни системи ще се реализират и опишат под формата на уеб-услуги (Web Services), които ще са достъпни за ползване от други системи в държавната администрация, а за определени услуги - и за гражданите и бизнеса;
- За всеки от отделните модули/функционалности на системата ще се реализират и опишат приложни програмни интерфейси – Application Programming Interfaces (API). Приложните програмни интерфейси бъдат достъпни и за интеграция на нови модули и други вътрешни или външни системи;
- Приложните програмни интерфейси и информационните обекти задължително ще поддържат атрибут за версия;
- Версията на програмните интерфейси, представени чрез уеб-услуги, ще поддържа версията по един или няколко от следните начини:
 - като част от URL-а;
 - като GET параметър;
 - като HTTP header (Асепт или друг).
- За отделните приложни интерфейси ще бъде разработен софтуерен комплект за интеграция (SDK) на поне две от популярните развойни платформи - .NET, Java, PHP.
- Системата ще осигурява възможности за разширяване, резервиране и балансиране на натоварването между множество инстанции на сървъри с еднаква роля;
- При разработването на системата ще се предвидят възможни промени, продиктувани от непрекъснато променящата се нормативна, бизнес и технологична среда. Системата ще бъде разработена като гъвкава и лесно адаптивна, като отчита законодателни, административни, структурни или организационни промени, водещи до промени в работните процеси.
- Изпълнителят ще осигури механизми за реализиране на бъдещи промени в системата

Чл.36 а, ал. 3 от ЗОП

без промяна на съществуващия програмен код. Когато това не е възможно, времето за промяна, компилиране и пускане в експлоатация ще е сведено до минимум. Бъдещото развитие на Системата ще се налага във връзка с промени в правната рамка, промени в модела на работа на потребителите, отстраняване на констатирани проблеми и др. Такива промени ще се извършват през целия период на експлоатация на регистъра, включително и по време на гаранционния период.

- Архитектурата на системата и всички софтуерни компоненти (системни и приложни) ще бъдат така подбрани и разработени, че да осигуряват работоспособност и отказоустойчивост на Системата, както и недискриминационно инсталиране (без различни условия за инсталиране върху физическа и виртуална среда) и опериране в продуктивен режим, върху виртуална инфраструктура, съответно върху Държавния хибриден частен облак (ДХЧО).
- Част или всички компоненти на Системата ще бъдат разположени върху Държавния хибриден частен облак като среда за функциониране на информационната система.
- Изпълнителят ще проектира, подготви, инсталира и конфигурира като минимум следните среди за системата: тестова, стейджинг, продуктивна.
- Системата ще бъде разгърната върху съответните среди (тестова за вътрешни нужди, тестова за външни нужди, стейджинг и продуктивна);
- Тестовата среда за външни нужди ще бъде създадена и поддържана като "Sandbox", така че да е достъпна за използване и извършване на интеграционни тестове от разработчици на информационни системи, включително такива, изпълняващи дейности за други администрации или бизнеса, с цел по-лесно и устойчиво интегриране на съществуващи и бъдещи информационни системи. Тестовата среда за външни нужди ще е напълно отделна от останалите среди и нейното използване няма да влияе по никакъв начин на нормалната работа на останалите среди или да създава каквито и да било рискове за информационната сигурност и защитата на личните данни;
- НСИ разполага със среда за виртуализация изградена с продукта VMware vCenter Server 6.5. и притежава лицензи за операционни системи Windows Server 2016 R2 x64 Standard, база данни Microsoft SQL Server 2016 x64 Standard или по високи. Изпълнителят ще използва посочените софтуерни продукти и лицензи при реализацията.
- Мрежата на държавната администрация (ЕЕСМ) ще бъде използвана като основна комуникационна среда и като основен доставчик на защитен Интернет капацитет (Clean Pipe) – изискванията на софтуерните компоненти по отношение на използвани комуникационни протоколи, TCP портове и пр. Трябва да бъдат детайлно документирани от Изпълнителя, за да се осигури максимална защита от хакерски атаки и външни прониквания чрез прилагане на подходящи политики за мрежова и

информационна сигурност от Възложителя в инфраструктурата на Държавния хибриден частен облак и EECM;

- При планиране и реализация на отделните компоненти на системната и приложната архитектура на Системата Изпълнителят ще прилага следните добри практики:
 - ще използва утвърдения MVC дизайн-шаблон;
 - ще спазва препоръките на международните стандарти на W3C относно визуализация и достъпност на информацията в Интернет;
 - ще спазва изискванията за интернационализация, като използва само UTF-8 кодиране на данните, съхранява текстовете от потребителския интерфейс извън програмния код и има разработени средства за превод и превключване на езиковите версии на интерфейса;
 - ще реализира обмен на данни с външни системи (където е приложимо) на базата на архитектура, ориентирана към услуги чрез REST протокол;
 - ще предоставя данни, за които е първоизточник, в отворен, стандартен машинно-четим формат, напр. xml, csv;
 - ще използва системи за пълнотекстово търсене;
 - ще разработи процедури за архивиране, възстановяване и възпроизвеждане на системните функции и данните в случай на неизправност, авария или бедствие.
- За реализиране на търсенето ще бъде използвана система за пълнотекстово търсене, а именно Solr/Lucene.
- Ще бъде създаден административен интерфейс, чрез който може да бъде извършвана конфигурацията на софтуера.
- За всеки обект в Системата се предвижда да има уникален идентификатор.
- Записите в регистрите няма да подлежат на изтриване или на промяна, а всяко изтриване или промяна ще представлява нов запис.

Детайлно описание на подхода за реализация е налично в 7.2. „Предложение за извършване на дейностите по разработката на системата“ от настоящото предложение.

6.3.3. Повторно използване (преизползване) на ресурси и готови разработки

Проектът ще преизползва максимално налични публично достъпни инструменти, библиотеки и платформи с отворен код, като за реализацията на Системата ще се използват максимално софтуерни библиотеки и продукти с отворен код.

Настоящият проект позволява при реализация на дадена техническа функционалност да бъдат използвани един или няколко от съществуващите множество отворени

алтернативни проекти, като с приоритет се ползват тези проекти, които са финансирани със средства на Европейския съюз, както и на такива, в които Изпълнителят има активни разработчици. В случаите, когато липсва подходяща open source алтернатива с необходимата функционалност, се допуска използване на closed source и на инструменти, библиотеки, продукти и системи с платен лиценз, но това става за сметка на Изпълнителя, който трябва да осигури поддръжка от комерсиална организация, развиваща основните отворени продукти, които ще бъдат използвани като минимум за операционните системи и софтуерните продукти за управление на базите данни.

Отворените проекти ще отговарят на следните критерии:

- За разработката им да се използва система за управление на версиите на кода и да е наличен механизъм за съобщаване на несъответствия и приемане на допълнения;
- Да имат разработена техническа документация за актуалната стабилна версия;
- Да имат повече от един активен програмист, работещ по развитието им;
- Да имат възможност за предоставяне на комерсиална поддръжка;
- Да нямат намаляваща от година на година активност;
- По възможност проектите да са подкрепени от организации с идеална цел, държавни или комерсиални организации;
- По възможност проектите да имат разработени unit tests с code coverage над 50%, а проектът да използва Continuous Integration (CI) подходи – build bots, unit tests run, регулярно използване на статични/динамични анализатори на кода и др.

Изпълнителят не идентифицира свободните компоненти и средства, които възнамерява да използва.

6.3.4. Изграждане и поддръжка на множество среди

Изпълнителят ще изгради и ще поддържа минимум следните логически разделени среди:

Development - Чрез Development средата се осигурява работата по разработката, усъвършенстването и развитието на Системата. В тази среда са налични и допълнителните софтуерни системи и инсталации, необходими за управление на разработката – continuous integration средства, системи за автоматизирано тестване и др.

Staging - Чрез Staging средата се извършват тестове преди разгръщане на нова версия от Development средата върху Production средата. В нея се извършват всички интеграционни тестове, както и тестовете за натоварване.

Sandbox Testing - чрез Sandbox средата всички, които трябва да се интегрират към Системата, могат да тестват интеграцията си, без да застрашават работата на продукционната среда.

Production - Това е средата, която е публично достъпна за реална експлоатация и интеграция със съответните външни системи и услуги.

Управлението на средите ще става чрез автоматизирана система за провизиране и разгръщане на системните компоненти. При необходимост от страна на Възложителя Изпълнителят ще съдейства за изграждането на нови системни среди.

стр.

Чл.36 а, ал. 3 от ЗОП

6.3.5. Процес на разработка, тестване и разгръщане

Процесите, свързани с развитието на Системата, ще гарантират висока прозрачност и възможност за обществен контрол над всички разработки по проекта. Изграждането на доверие в гражданите и в бизнеса налага радикално по-висока публичност и прозрачност чрез отворена разработка и публикуването на системите компоненти под отворен лиценз от самото начало на разработката.

Всички софтуерни приложения, системи, подсистеми, библиотеки и компоненти, които са необходими за реализацията на Системата, ще бъдат разработвани като софтуер с отворен код и ще бъдат достъпни в публично хранилище, поддържани от ДАЕУ съгласно чл. 7в, т. 18 от ЗЕУ и чл. 58 от Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги. Към настоящия момент ще се използва общото хранилище за проекти с отворен код, финансирани с публични средства в България (към момента <https://github.com/governmentbg>).

Исходният код (Source Code) разработван по проекта, ще бъде публично достъпен онлайн като Софтуер с отворен код от първия ден на разработка, чрез използване на система за контрол на версиите.

Разработките по проекта ще бъдат изцяло с отворен код от първия ден на разработка, като се използва публично хранилище и система за контрол на версиите. Освен кодът, цялата документация и отчетни материали ще бъдат качвани в хранилището.

Описано подробно в т.4.6.

В случай че върху част от компонентите, нужни за компилация, има авторски права, те ще бъдат или в отделно хранилище с подходящия за това лиценз или за тях ще бъде предоставен заместващ „mock up“ компонент, така че да не се нарушава компилацията на проекта.

За всеки един разработван компонент Изпълнителят ще покрие следните изисквания за гарантиране на качеството на извършваната разработка и на крайния продукт:

- Документиране на Системата в изходния код, минимум на ниво процедура/функция/клас;
- Покритие на минимум 50% от изходния код с функционални тестове
- Използване на continuous integration практики;
- Използване на dependency management.

Във всеки един компонент на Системата, който се build-ва и подготвя за инсталация (deployment), се предвижда да присъстват следните реквизити:

- Дата и час на build;
- Място/среда на build;
- Потребител извършил/стартирал build процеса;

- Идентификатор на ревизията от кодовото хранилище на компонента, срещу която се извършва build-ът.

Ще се анализират възможностите за включване на граждани в процесите по разработка, тестване и идентифициране на пропуски на софтуера. Във фазата на анализ участникът ще предложи механизъм и процедури за реализирането на такива процеси.

6.3.6. Бързодействие и мащабируемост

6.3.6.1. Контрол на натоварването и защита от DoS/DDoS атаки

- На приложно ниво Системата ще поддържа "Rate Limiting" и/или "Throttling" на заявки от един и същ клиентски адрес, както към страниците с уеб-съдържание, така и по отношение на заявките към приложните програмни интерфейси, които са достъпни публично или служебно като уеб-услуги (Web Services) и служебни интерфейси.
- Лимитите за отделни страници, уеб-услуги и ресурси, които се достъпват с отделен URL/URI ще могат да се конфигурират от администраторите на Системата.
- Ще позволява конфигуриране на различни лимити за конкретни автентикирани потребители и ще предоставя възможност за генериране на справки и статистики за броя заявки по ресурси и услуги.

6.3.6.2. Бързодействие

Архитектурата на системата е ориентирана към осигуряване на максимална производителност и бързодействие. В съответствие с изискванията и очакванията на потребителите, системата ще осигури адекватно време за реакция при работа.

Времето за реакция се измерва за атомарни по отношение на работата на потребителя операции, за които той изчаква отговор от системата.

При визуализация на уеб-страници системите ще осигуряват висока производителност и минимално време за отговор на заявки - средното време за заявка ще бъде по-малко от 1 секунда, с максимум 1 секунда стандартно отклонение за 95% от заявките, без да се включва мрежовото времезакъснение (Network Latency) при транспорт на пакети между клиента и сървъра.

Системата ще прекъсва потребителската сесия при неактивност за време повече от определена стойност, която ще бъде зададена като управляем параметър от модула за конфигуриране на параметрите на системата.

За да се гарантира бързодействието на системата се предвижда създаването на тестове за натоварване.

6.3.6.3. Използване на HTTP/2

Чл.36 а, ал. 3 от ЗОП

С оглед намаляване на служебния трафик, времената за отговор и натоварването на сървърите ще се използва HTTP/2 протокол при предоставяне на публични потребителски интерфейси с включени като минимум следните възможности:

- Включена header compression;
- Използване на brotli алгоритъм за компресия;
- Включен HTTP pipelining;
- HTTP/2 Server push, приоритизиращ специфични компоненти, изграждащи страниците (CSS, JavaScript файлове и др.);
- Публичните потребителски интерфейси трябва да поддържат адаптивен избор на TLS cipher suites според вида на процесорната архитектура на клиентското устройство - AES-GCM за x86 работни станции и преносими компютри (с налични AES-NI CPU разширения), и ChaCha20/Poly1305 за мобилни устройства (основно базирани на ARM процесори);
- Ако клиентският браузър/клиент не поддържа HTTP/2, ще бъде предвиден fallback механизъм към HTTP/1.1. Тази възможност ще може лесно да се реконфигурира в бъдеще и да отпадне, когато браузърите/клиентите, неподдържащи HTTP/2, станат незначителен процент.

HTTP/2 е новата версия на основния протокол за пренос на данни в Уеб - HTTP. HTTP/2 е с повишена производителност, понижено потребление на трафик и нова, оптимизирана организация на комуникацията клиент-сървър. С оглед намаляване на служебния трафик, времената за отговор и натоварването на сървърите, Изпълнителят ще използва HTTP/2 протокол при предоставяне на публични потребителски интерфейси.

Едно от основните подобрения в HTTP/2 е мултиплексирането на комуникацията клиент-сървър. Предаваните данни се подреждат в пакети (фреймове), които се придвижват в двете посоки в паралелни потоци (стриймове). Това от своя страна позволява на комуникацията да се проведе в една единствена TCP връзка, която може да има множество потоци, с множество пакети. За разлика от HTTP/1.1 където, за да се постигне по-добра производителност, уеб браузърът отваря по няколко TCP връзки със сървъра.

Другите значителни подобрения са компресиране на хедърите, бинарното естество на протокола и самоинициативното подаване на данни от уеб сървъра. В резултат на тези подобрения, зареждането на уеб сайтовете през HTTP/2 е ускорено в пъти, което го прави предпочитан в реализираните от Изпълнителя проекти.

Предвижда се включването минимум на следните възможности:

- Включена header compression;

Компресирането на header-а подобрява ефективността на мрежовото предаване, качеството и скоростта с:

- Намаляване на packet header overhead (bandwidth savings);
- Намаляване на загубата на пакети;

Чл.36 а, ал. 3 от ЗОП

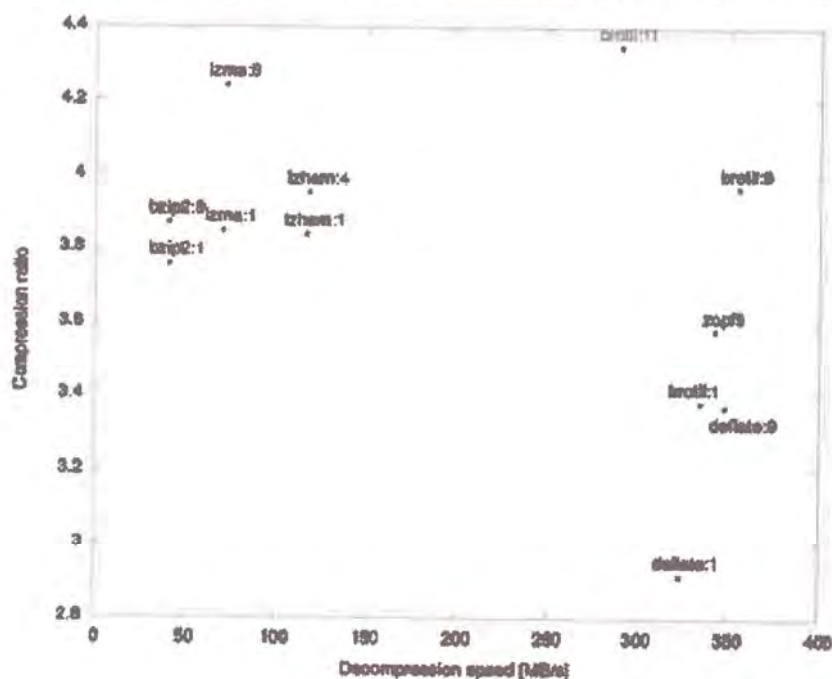
- По-добро време за интерактивно реагиране;
- Намаляване на разходите за инфраструктура, повече потребители на channel bandwidth означава по-малко разходи за разполагане на инфраструктурата.

Тези предимства водят до подобро качество на QoS в мрежата и възможност операторите да подобрят своите ARPU. За потребителите, това води до по-добра QoS в мрежата и повече услуги и съдържание на връзките.

- **Използване на Brotli алгоритъм за компресия**

Brotli принадлежи към компресиращите алгоритми с общо ползване и се използва основно за минимизиране обема на данни при мрежовите връзки. Спецификите му са подадени към IETF (Internet Engineering Task Force) и сега Brotli е претендент за включване в Интернет стандартите. Новият алгоритъм се използва за компресия на шрифтовете Web Open Font Format 2.0. Оригиналният Brotli е написан на C++ и се разпространява с Apache 2.0. лиценз.

Brotli постига ниво на компресия от нивото на най-добрите съвременни методи за компресия, но изпреварва всички останали по скоростите на кодиране и декодиране.



- **Включен HTTP pipelining**

HTTP pipelining е техника, при която множество HTTP заявки се изпращат на една TCP връзка, без да се чакат съответните отговори.

Техниката беше заменена от мултиплексиране чрез HTTP / 2 [2], което се поддържа от повечето съвременни браузъри.

Внедряването на pipelining в уеб сървърите е относително проста задача - мрежовите буфери не трябва да се изчистват между заявките. По тази причина повечето съвременни уеб сървъри се справят с pipelining безпроблемно.

Внедряване в уеб браузъри - от всички основни браузъри, само в Орега имаше напълно работеща имплементация, която беше разрешена по подразбиране. Във всички други браузъри HTTP pipelining е деактивиран или не е имплементиран изобщо.

Например - Internet Explorer 11 не поддържа pipelining, Mozilla поддържа. Той обаче е деактивиран по подразбиране, за да се избегнат проблеми със сървъри с лошо управление. Когато включването в мрежата е активирано, браузърите на Mozilla използват някои евристики, особено за да изключат pipelining за по-стари IIS сървъри. Поддръжката на H1 Pipeline бе премахната от Mozilla Firefox във Версия 54. Google Chrome преди поддържаше pipelining, но към момента е деактивиран поради бъгове и проблеми с лошо поведение на сървърите.

- HTTP/2 Server push, приоритизира специфични компоненти, изграждащи страниците

HTTP / 2 Server Push позволява на HTTP / 2-съвместим сървър да изпраща ресурси към HTTP / 2 съвместим клиент, преди клиентът да ги поиска. Това е, в по-голямата си част, техника за ефективност, която може да бъде полезна при предварително зареждане на ресурси.

С HTTP / 2 Push, сървърът може да поеме инициативата, като има правила, които задействат съдържанието, което трябва да бъде изпратено, дори преди да бъде поискано, което намалява възможността за загуба на bandwidth, ако изпратените до клиента подадени ресурси останат неизползвани.

- Публичните потребителски интерфейси ще поддържат адаптивен избор на TLS cipher suites според вида на процесорната архитектура на клиентското устройство - AES-GCM за x86 работни станции и преносими компютри (с налични AES-NI CPU разширения), и ChaCha20/Poly1305 за мобилни устройства (основно базирани на ARM процесори);
- Ако клиентският браузър/клиент не поддържа HTTP/2, ще бъде предвиден fall-back механизъм към HTTP/1.1. Тази възможност трябва да може лесно да се реконфигурира в бъдеще и да отпадне, когато браузърите/клиентите, неподдържащи HTTP/2, станат незначителен процент.

6.3.6.4. Качество и сигурност на програмните продукти и приложенията

Ще се спазват добрите практики на софтуерната разработка – над 60% документирание на изходния код, използване на среда за непрекъсната интеграция, възможност за компилиране и пакетиране на продукта с една команда, възможност за инсталиране на нова версия на сървъра с една команда, система за управление на зависимостите (Dependency Management);

Публичните модули, които ще предоставят информация и електронни услуги в Интернет, ще отговарят на актуалните уеб стандарти за визуализиране на съдържание.

6.3.6.5. Информационна сигурност и интегритет на данните

Чл.36 а, ал. 3 от ЗОП

Системата ще притежава високо ниво на сигурност и защита на данните при експлоатация и ще гарантира надеждно съхраняване и архивиране на информацията.

Тя ще позволява дефиниране на профили за достъп до информацията за потребителите. Всеки профил ще контролира достъпа до функции от системата и в същото време достъпа до определена част от данните в базата.

Системата ще реализира следния комплект от мерки и решения за сигурност и защита на данните:

- Осигуряване на цялостност на данните при многопотребителски режим на работа;
- Разрешаване на достъп до системата само след успешно идентифициране на потребителя. Идентифицирането ще се извърши чрез проверка на уникално потребителско име и парола, различни от тези на операционната система, на системата за управление на релационна база данни и на интегрирания OLAP-продукт. Паролите ще бъдат съхранявани в шифриран вид и ще съдържат не по-малко от 6 символа. Потребителите ще могат да променят паролите си самостоятелно;
- Регистриране на всички неуспешни опити за достъп до системата;
- Реализиране на механизъм за дефиниране на групи от потребители и за предоставяне и контролиране на права за достъп на ниво потребителски групи (роли);
- Реализиране на механизъм за предоставяне и контролиране на права за достъп до ресурсите на системата на ниво отделен служител в зависимост от конкретните задължения и отговорности на служителя;
- Регистриране на служебна информация за всички действия на потребители, касаещи регистриране, промяна и/или изтриване на данни;
- Съхраняване на история на промените в микроданните;

Системата няма да предявява специални изисквания за антивирусна защита извън приетите в НСИ решения.

Системата ще работи върху надеждно защитен уеб сървър, достъпът до който се осъществява по защитен протокол (HTTPS).

Системата ще осигурява следните нива на защита на достъпа до ресурсите:

- Няма да се допуска съхранението на пароли на администратори, на вътрешни и външни потребители и на акаунти за достъп на системи (ако такива се използват) в явен вид. Всички пароли трябва да бъдат защитени с подходящи сигурни алгоритми (напр. BCrypt, PBKDF2, scrypt (RFC 7914) за съхранение на пароли и където е възможно, да се използва и прозрачно криптиране на данните в СУБД със сертификати (transparent data-at-rest encryption);
- Ще бъде предвидена система за ежедневно създаване на резервни копия на данните, които да се съхраняват извън инфраструктурата на системата по ред, определен с наредбата по чл. 43, ал. 2 от НОИИСРЕАУ;
- Няма да бъде допуснато използването на Self-Signed сертификати за публични услуги;

Чл.36 а, ал. 3 от ЗОП