4.8.4. Планиране на реакцията

Целите на планирането на реакцията са да се ограничат рисковете представляващи заплаха (негативните рискове) и да се максимизират рисковете даващи възможности (положителни рискове). Това е процес, който следва качествения анализ и ако е приложен количествения анализ. Включва и идентификацията на конкретна личност (собственик на риска), който е отговорен за третиране на риска.

Планираната реакция трябва да е адекватна на важността на риска, ценово ефективна и реалистична в контекста на проекта.

Техники за планиране на реакцията

Познати са различни стратегии за реакция на риска. За всеки риск трябва да се избере ефективната стратегия или съвкупност от стратегии. По-долу са представени най-често използваните стратегии за третиране на негативни рискове и заплахи.

- Избягване

Състои се в неизпълнение на дейност, която може да носи риск. Такъв пример е да не се лети с самолет на авиокомпания за избягване на риска от отвличане. Избягването може би изглежда отговор на всички рискове, но това означава загуба на потенциалните ползи, които тази дейност би донесла, ако се приеме риска. Така, в горния пример, би ни се наложило да пътуваме много по-дълго с друг транспорт, избягвайки риска.

Част от избягването на риска е предпазване от опасности и се отнася до настъпили спешни събития. Първата и най-ефективна стъпка е елиминирането на опасността, но ако отнема твърде дълго време, твърде е скъпо или по друг начин непрактично, следващата стъпка е ограничаването на риска и неговото въздействие.

- Намаляване/ограничаване

Намаляването на риска (или ограничаване или оптимизиране) се състои в предприемане на действия, които водят до намаляване обема на загубите от щетата или намаляване вероятността за нейното настъпване. В някои случаи инструментите за намаляване на риска може да доведат до други рискове или да са толкова ресурсоемки, че да не оправдават тяхното използване. В примера със самолета решението да се пътува с автомобил би довело до поява на риск от задръстване, например, а решението за пътуване със собствен самолет по очевидни причини не е широко приемливо.

Разбирайки, че рискът може да е положителен или отрицателен, оптимизирането на риска означава намирането на баланс между негативите, които риска носи, в сравнение с ползите, които произтичат от изпълнението на дейността, както и между степента на намаляване на риска и необходимите усилия за това.

Модерните методологии за разработка на софтуер като RUP намаляват риска чрез разработване и инкрементално представяне на прототипи. Старите методологии страдаха от факта, че доставят софтуера на финалната фаза и всички възникнали на по-ранен етап проблеми означават скъпа преработка и често обричат проекта на провал.

- Споделяне

Краткото описание на споделянето е „споделяне с друга страна на тежестта от загубата или пропуснатата полза от риска, както и усилията, необходими за прилагане на мерките за намаляването му".

- Трансфер

Трансфер предимно на финансовите рискове към трето лице, най-вече застраховател или доставчик. Тази реакция е припозната най-вече от методологията Prince2.

- Приемане

Представлява приемане на загубите или пропуснатите ползи от риска, когато събитието настъпи. Самозастраховането (заделяне на средства за компенсация на евентуални бъдещи загуби) попада в тази категория. Приемането на риска е съществена стратегия за малки рискове, където цената от подсигуряване срещу риска с течение на времето ще надмине общия сбор на очакваните загуби.

Всеки риск, който не е избегнат или прехвърлен към трета страна по подразбиране е приет. Това включва рискове, които са толкова големи или катастрофални, че не могат да бъдат подсигурени или цената на осигуровката е невъзможна. Форсмажорните обстоятелства (война, природно бедствие и др.) са примери за такъв риск.

Друга причина за приемане на риска е вероятността за настъпване на събитие, причиняващо твърде голяма загуба, е твърде малка или необходимите ресурси за осигуряването са такива, че да пречат твърде много на целите на организацията.

- Резервираност (Fallback)

Това е реакция, развита добре в методологията Prince2. Състои се в предварително оставяне на резерви (от време, ресурси, действия), които да се използват за противодействие на риска в случай на проявление.

В резултат на планиране на реакцията могат да се създадат следните документи:

- Промени в Регистъра на рисковете;
- Решения за сключване на договори, относими към рисковете;
- Промени в плана за управление на проекта – график, бюджет и др.;
- Промени в техническата документация.

4.8.5. Наблюдение и контрол

Планираните реакции на рисковете, включени в Регистъра на рисковете се изпълняват през целия жизнен цикъл на проекта, но трябва да се извършва и постоянно наблюдение за нови, променящи се или вече остарели рискове.

Използват се следните техники за наблюдение и контрол:

- Преоценка на риска – много често в резултат на наблюдението се идентифицират нови рискове, преоценяват се текущи рискове или се затварят остарели и невалидни вече;
- Одити на рисковете – изследва се и се документира ефективността на реакция на рисковете относно тяхното третиране и основните първопричини за тях, както и се оценява процесът по управление на рисковете;
- Анализ на отклонения и тенденции – сравняват се постигнатите резултати с планираните и се прави преглед на тенденции в изпълнението на проекта;

- Анализ на резервите – сравняване на остатъка на заделените за непредвидени обстоятелства резерви и остатъчните стойности на рисковете, за да се прецени адекватността на тези резерви;
- Оперативки – управлението на риска е толкова по-лесно, колкото по често се прилага. Честите дискусии относно рисковете увеличават вероятността хората да идентифицират рискове и възможности;

В резултат на наблюдението и контрола могат да се създадат следните документи:

- Промени в Регистъра на рисковете;
- Промени в Плана за управление на проекта;
- Искания за промяна (change requests);
- Промени в документацията на проекта.

В заключение е важно да се уточни, че процеса на управление на риска е итеративен процес (и затова най-добре кореспондира с методологията RUP) – изложените дейности по управление на риска се изпълняват циклично през целия жизнен цикъл на проекта. Първоначално идентифицираните, класифицираните, приоритизирани и с планирана реакция рискове подлежат на дейността „Наблюдение и контрол", през която могат да се идентифицират и нови рискове за които отново следва да изпълнят итеративно дейностите по класифициране, приоритизация и планиране на реакцията, а за част от вече идентифицираните рискове може да се наложи нова приоритизация, предвид на настъпилите нови обстоятелства.

4.8.6. Прилагане на Методологията за управление на риска на проекта

След като изложихме теоретичната рамка на Методологията за управление на риска в проекта в тази точка ще представим нейното практическо прилагане в проекта.

Практическото прилагане на методологията за управление на риска в проекта се базира на подхода на RUP за описване на процеса по изграждане на информационни системи в две измерения:

- ✓ **статично измерение** – описва дейностите по управление на риска по същество и детайлизира ролите и отговорностите участниците в екипа в процеса по управление на риска.
- ✓ **динамично (времево) измерение** – представя изпълнението на описаните в предложената методология дейности по управление на риска през целия жизнения цикъл на проекта (по фази и итерации).

Тъй като тези две измерения са неразделна част от една методология, чиято цел е да доведе IT проекта до успешно изпълнение, то нашият подход за прилагане на предлаганата Методология за управление на риска се базира на интегрираното и цялостно прилагане на тези две измерения. Това е в унисон и със споменатия вече силно изразен итеративен характер на процеса по управление на риска.

4.8.6.1.Планиране на управлението на риска

Считаме изпълнението на тази дейност и по-конкретно разработването на **План за управление на риска** за основополагащ и критичен фактор за успешното управление

на риска в проекта. Затова предлагаме **Плана за управление на риска** да бъде добавен като **допълнителен документ в Документацията по управление на проекта**.

4.8.6.2.Статично измерение на дейността „Планиране на управлението на риска“

Тази дейност по същество включва **разработването и актуализирането на Плана за управление на риска,** в съответствие със структурата, показана в предложената Методология за управление на риска:

- **Методология** – ще бъде изложена предложената Методология за управление на риска в проекта;
- **Бюджет** – предвид на спецификата на обществените поръчки не се предвижда обособено финансиране за управление на риска и тези дейности ще се финансират в рамките на общия бюджет на проекта;
- **График** – ще обобщава динамичното измерение за всички дейности по управление на риска в един общ график, който ще определя кога и колко често ще се извършват дейности по управление на риска, разпределени във времето по фазите и итерациите на проекта;
- **Роли и отговорности** – ще дефинира ясно и детайлно ролите и отговорностите на участниците в екипа за изпълнение на проекта в процеса по управление на риска, който ще бъдат изложени в статичното измерение на всяка една от дейностите по управление на риска;
- **Критерии за категоризиране/класифициране на рисковете** – отчитайки спецификите на проекта и добрите практики в тази област, предлагаме рисковете по проекта да се категоризират/класифицират по следните два критерия:
  - **по основните дейности на проекта** – общи рискове и рискове по двете основни дейности;
  - **по източниците на рисковете** – добрата практика е по този критерии рисковете да се категоризират в 6 направления: потребител/възложител, обхват и изисквания, технологии, планиране и контрол, екип за изпълнение и организационна среда;
- **Дефиниране на метрики** – по отношение на Рисковата експозиция следва да се определи скала за степента на критичност за целите на реакцията:

Таблица 6 – Рискова експозиция и степен на критичност

Рискова експозиция	Степен на критичност
< 0,1	много ниска
0,1 - 0,3	ниска
0,3 – 0,5	умерена
0,5 – 0,8	висока
0,8 >	много висока

4.8.6.3.Динамично измерение на дейността „Планиране на управлението на риска“

Планът за управление на риска ще бъде разработен в началото на изпълнението на проекта, като ще бъде прилаган през целия жизнен цикъл на проекта и при необходимост ще бъде актуализиран в края на всеки един от етапите, дефинирани в 5.4. от Техническата спецификация.

4.8.6.4.Идентифициране на рисковете

Тази дейност е също изключително критична за процеса на управление на риска, тъй като има за цел да идентифицира обекта на това управление - несигурните бъдещи събития или условия, наречени още рискове, които, ако възникнат биха имали ефект върху целите на проекта.

✓ **Статично измерение на дейността „Идентифициране на рисковете“**

Идентификацията на рисковете е итеративен процес, в резултат на който се създава **Регистъра на рисковете**, включващ:

- **Списък на идентифицираните рискове** – описани са в колкото се може повече подробности;
- **Списък на потенциалните реакции** – когато могат да бъдат идентифицирани още с откриването на риска или добавени впоследствие при изпълнение на дейността „Планиране на реакцията“.

Предвид на важността и критичността на тази дейност за ефективното управление на риска **предлагаме работна версия на Регистъра на рисковете**, посочени от Възложителя в Техническата спецификация и предложим първоначално виждане за **потенциални реакции** за всички рискове.

Таблица 7 - Работна версия на Регистъра на рисковете

№	Идентифицирани рискове	Потенциални реакции
1.	**Рискове идентифицирани от Възложителя**	
1.1.	Промяна в нормативната уредба, водеща до промяна на ключови компоненти на решението – предмет на разработка на настоящата обществена поръчка	Своевременно осигуряване на информация за предстоящи промени в нормативната уредба, за да може резултатите да бъдат съобразени с тях. Гъвкавост на разработките с възможност за параметризация и вариативност.
1.2.	Недобра комуникация между екипите на Възложителя и Изпълнителя по време на аналитичните етапи на проекта	Мерки за противодействие както следва: • Ръководителят на екипа, подпомаган от Тестовия инженер. Да създадат организацията за изпълнение на всеки етап от проекта, която задължително включва възлагане, следене, координация и съгласуване на изпълнението на дейностите през етапа и осъществяване на непрекъсната

		комуникация с Възложителя; • Регулярност на срещите на управленското ниво на проекта от страна на Изпълнителя и Възложителя, която включва: • Седмични срещи за бърз преглед на прогреса по изпълнение на проекта и синхронизация на дейностите между всички членове на екипа за изпълнение на проекта. Месечни срещи за детайлен преглед на прогреса по изпълнение на проекта, обсъждане на ресурсното обезпечаване на проекта, анализ на възникналите проблеми и задействани рискове, както и вземане на необходимите решения и мерки за разрешаване на проблемите и противодействие на рисковете.
1.3.	Ненавременно изпълнение на всяко от задълженията от страна на Изпълнителя	За противодействие на този риск сме предложили план график за изпълнение на дейностите по проекта, чието стриктно спазване ще противодейства успешно на този риск.
1.4.	Неправилно и неефективно разпределяне на ресурсите и отговорностите при изпълнението на договора	За избягване на този риск Изпълнителя и Възложителя трябва непрекъснато да следят нивото на ресурсна обезпеченост на изпълнението на проекта и при нужда да включва допълнителни ресурси.
1.5.	Забавяне при изпълнение на проектните дейности, опасност от неспазване на срока за изпълнение на настоящата поръчка	Този риск е **реален**, предвид на съотношението на обема работа към предлаганото време за изпълнение на поръчката. Най- силните инструменти за противодействие на този риск са: • задълбоченият опит на експертите на Изпълнителя, натрупан при разработката и внедряването на уеб базирани информационни системи; • прилагането на предложената от нас ефективна Организация за изпълнение на проекта. • висока мобилизация на ресурсите от страна както на Изпълнителя, така и на Възложителя.
1.6.	Грешки при разработване на функционалностите на системата	За противодействие на този риск, е дефинирано и ще се прилагат **ефективни механизми за управление и контрол на качеството.** Тясно придържане към спецификацията на системата и ранна валидация от страна на Възложителя също ще допринесат за минимизиране на този риск.

1.7.	Недостатъчна яснота по правната рамка и/или променяща се правна рамка по време на изпълнение на проекта	Провеждане на работни сесии, анализ на съществуваща документация във връзка с нормативната уредба, навременно оценяване на въздействието върху проекта при евентуални промени на съществуващата правна рамка.
1.8.	Липса на задълбоченост при изследването и описанието на бизнес процесите и данните	Инструментът за противодействие на този риск е задълбоченият анализ и опит на експертите на Изпълнителя, натрупан при разработката и внедряването на информационни системи.
1.9.	Неинформиране на Възложителя за всички потенциални проблеми, които биха могли да възникнат в хода на изпълнение на дейностите	Противодействието на този риск ще бъде обезпечено чрез анализиране на дейностите по реализация на проекта, идентифициране на потенциалните проблеми и навременното им обсъждане с Възложителя, както и регулярно допълване на списъка с идентифицирани рискове и от двете страни и изготвяне на стратегия за реакция на новоидентифицираните рискове и тяхната превенция. Регулярни междинни отчети за извършената работа.
1.10.	Риск за администриране на системата след изтичане на периода на гаранционна поддръжка	За противодействие на този риск, през етап „Обучение“ се провеждат обучения на 2 ма системните администратори. **Крайният резултат** от този етап ще включва **обучени** системни **администратори** за администриране на системата, което е **критична предпоставка** за безпроблемното администриране след изтичане на гаранционната поддръжка.

✓ **<u>Динамично измерение на дейността „Идентифициране на рисковете“</u>**
Тази дейност е повтарящ се (итеративен) похват.

Рискове от Техническата спецификация, допълнително идентифицираните от Изпълнителя в тръжната фаза и евентуално идентифицираните при подписване на договора за изпълнение рискове ще формират **първата версия Регистъра на рисковете**.

Итеративното изпълнение на тази дейност през целия жизнен цикъл на проекта може да породи **актуализация на Регистъра на рисковете** в края на всеки един от етапите на проекта, определени в т.6. от Техническото задание.

4.8.6.5.Анализ и Планиране на реакцията

✓ **Статично измерение на дейностите „Анализ“ и „Планиране на реакцията“**
Както беше изложено в представянето на Методологията за управление на риска в проекта, **качествения анализ** дава оценка за вероятността за възникване и влиянието на рисковете, а **количествения анализ** дава оценка на ефекта от тези рискови събития. Това е процес на **приоритизация** на вече идентифицираните рискове от предходната дейност, за целите на бъдещ анализ и действия за противодействие.

Планирането на реакцията е дейност, неразривно свързана с анализа и обичайно се извършва едновременно с него. Крайната цел е за всеки идентифициран и

приоритизиран риск да се планира реакция, която да е адекватна на важността на риска, ценово ефективна и реалистична в контекста на проекта.

Прилагането на предлаганата Методология за управление на риска по отношение на дейностите „Анализ“ и „Планиране на реакцията“ ще включва итеративното използване на техниките за качествен и количествен анализ и планиране на реакцията с цел определяне на номинални стойности на следните показатели за всеки от идентифицираните рискове, които се регистрират в **таблица „Приоритизация на рисковете и планирани реакции“**, неразделна част **Регистъра на рисковете**:

- Степен на значимост (Влияние)
- Вероятност от настъпване
- Рисковата експозиция
- Индикатор
- Планирани реакции

На база извършените от нас предварителен Анализ (качествен и количествен) и Планиране на реакцията достигнахме до следната първоначалната работна версия на таблицата „Приоритизация на рисковете и планирани реакции“:

Таблица 8 Приоритизация на рисковете и планирани реакции

№ на риск	Степен на значимост (Влияние)	Вероятност от настъпване	Рискова експозиция	Планирани реакции
1.1.	0,8	0,10	0,08	Мерки за противодействие както следва: ✓ Ръководителят на екипа, подпомаган от Тестовия инженер. Да създадат организацията за изпълнение на всеки етап от проекта, която задължително включва възлагане, следене, координация и съгласуване на изпълнението на дейностите през етапа и осъществяване на непрекъсната комуникация с Възложителя; ✓ Регулярност на срещите на управленското ниво на проекта от страна на Изпълнителя и Възложителя, която включва: • Седмични срещи за бърз преглед на прогреса по изпълнение на проекта и синхронизация на дейностите между всички членове на екипа за изпълнение на проекта; Месечни срещи за детайлен преглед на

				прогреса по изпълнение на проекта, обсъждане на ресурсното обезпечаване на проекта, анализ на възникналите проблеми и задействани рискове, както и вземане на необходимите решения и мерки за разрешаване на проблемите и противодействие на рисковете.
1.2.	0,9	0,10	0,09	За противодействие на този риск сме предложили план график за изпълнение на дейностите по проекта, чието стриктно спазване ще противодейства успешно на този риск.
1.3.	0,6	0,10	0,06	За избягване на този риск Изпълнителя и Възложителя трябва непрекъснато да следят нивото на ресурсна обезпеченост на изпълнението на проекта и при нужда да включва допълнителни ресурси.
1.4.	0,9	0,10	0,09	Този риск е **реален**, предвид на съотношението на обема работа към предлаганото време за изпълнение на поръчката – 210 дни от датата на подписване на договора между Възложителя и Изпълнителя. Най- силните инструменти за противодействие на този риск са: • задълбоченият опит на експертите на „Перфект Плюс“ ЕООД, натрупан при разработката и внедряването на уеб базирани информационни системи; • прилагането на предложената от нас ефективна Организация за изпълнение на проекта.
1.5.	0,6	0,10	0,06	**висока мобилизация на ресурсите от страна както на Изпълнителя, така и на Възложителя**. За противодействие на този риск, е дефинирано и ще се прилагат **ефективни механизми за управление и контрол на качеството.** Тясно придържане към спецификацията на системата и ранна валидация от страна на Възложителя също ще допринесат за минимизиране на този риск.
1.6.	0,7	0,10	0,07	Своевременно осигуряване на информация за предстоящи промени в правната рамка, за да може резултатите да бъдат съобразени с тях. Гъвкавост на разработките с възможност за параметризация и вариативност.
1.7.	0,7	0,10	0,07	Инструментът за противодействие на този риск е задълбоченият анализ и опит на експертите

				на Изпълнителя, натрупан при разработката и внедряването на информационни системи.
1.8.	0,6	0,10	0,06	Противодействието на този риск ще бъде обезпечено чрез: Анализиране на дейностите по реализация на проекта, идентифициране на потенциалните проблеми и навременното им обсъждане с Възложителя, както и регулярно допълване на списъка с идентифицирани рискове и от двете страни и изготвяне на стратегия за реакция на новоидентифицираните рискове и тяхната превенция. Регулярни междинни отчети за извършената работа.
1.9.	0,6	0,10	0,06	За противодействие на този риск, през етап „Обучение“ се провеждат обучения на 2 ма системните администратори. **Крайният резултат** от този етап ще включва **обучени** системни **администратори** за администриране на системата, което е **критична предпоставка** за безпроблемното администриране след изтичане на гаранционната поддръжка.
1.10.	0,6	0,2	а0,12	За противодействие на този риск, във фазата на проектиране ще се извърши анализ на съответствието между наличните в съществуващата система данни и модел на данни на проектираното решение. При несъответствие между двата модела на данни, ще бъдат предвидени допълнителни инструменти за допълване на данните, така че те да могат да бъдат заредени в крайната реализация. Посочените инструменти могат да бъдат например: интерфейсни форми за допълване на информацията или специфициран в рамките на проектирането импортен формат за зареждане на данни, който валидира консистентността на данните (xml, xls или csvn).

По отношение на Рисковата експозиция е определена следната скала за степен на критичност за целите на реакцията:

Таблица 9 - Скала за степен на критичност

Рискова експозиция	Степен на критичност
< 0,1	много ниска
0,1 - 0,3	ниска
0,3 – 0,5	умерена
0,5 – 0,8	висока

	0,8 >	много висока

✓ **Динамично измерение на дейностите „Анализ“ и „Планиране на реакцията“**

Тези дейности са също повтарящ се (итеративен) похват, както и целия процес по управление на риска в проекта.

На база анализа и планирането на реакцията извършени от нас в тръжната фаза и на изпълнението на тези дейности през етапа на проекта „Проектиране“ ще се формира първата версия на **таблицата „Приоритизация на рисковете и планирани реакции“ като неразделна част от Регистъра на рисковете**.

Итеративното изпълнение на тези дейности през целия жизнен цикъл на проекта може да породи **актуализация на таблицата „Приоритизация на рисковете и планирани реакции“** в края на всеки от етапите на проекта, определени в т.6. от Техническата спецификация.

4.8.6.6.Наблюдение и контрол

✓ **Статично измерение на дейността „Наблюдение и контрол“**

Планираните реакции на рисковете, включени в **Регистъра на рисковете** се изпълняват през целия жизнен цикъл на проекта. Ефектът от прилагането на реакциите обаче може да се промени ако не се отчете динамиката на проекта и настъпилите нови обстоятелства и промени в средата като цяло. Това именно обосновава нуждата от дейността Наблюдение и контрол, която при необходимост запалва итеративното прилагане на фазите Анализ и Планиране на реакцията. Това гарантира, че във всеки един момент управлението на риска в проекта се базира на коректна приоритизация на рисковете и адекватни реакции за тези рискове.

✓ **Динамично измерение на дейността „Наблюдение и контрол“**

Тази дейност има най-силно изразения итеративен характер и се изпълнява през целия жизнен цикъл на проекта. Наблюдаване за нови, променящи се или вече остарели рискове ще поражда актуализация на Регистъра на рисковете и итеративно прилагане на останалите дейности по управление на риска – Анализ (качествен и количествен) и Планиране на реакцията.

5. ЕТАПИ НА РЕАЛИЗАЦИЯ НА ДЕЙНОСТИТЕ ПО ПРОЕКТА

5.1. Анализ на данните и изискванията

Функционален обхват на проекта

- Разработка и внедряване на нови публични електронни административни услуги;
- Разработка и внедряване на нови вътрешно-административни услуги.

Независимо от източника на финансиране са приложими и предварителните условия за допустимост (Приложение № 1 от Пътната карта за електронно управление 2016-2020) за финансиране на проекти по ОП „Добро управление“, в т.ч.:

- Предвидените за разработка и внедряване услуги трябва да бъдат регистрирани предварително в Регистъра на услугите към Административния регистър (съгласно чл. 61 от Закона за администрацията) и да бъдат въведени и валидирани данни за броя на транзакциите по предоставяне на тези услуги в

Модула „Самооценка на административното обслужване" в Интегрираната информационна система на държавната администрация (ИИСДА). Услугите, които ще бъдат надградени, и новоразработените услуги трябва да отговарят на изискванията за електронни услуги с минимално Ниво 4, където е приложимо (т.е. услугата изисква заплащане на такса), или Ниво 3, в случаите, в които за предоставяне на услугата не се изисква заплащане на такса. Дефинициите за нивата на електронизация на административните услуги са регламентирани в Наредбата за административния регистър към Закона за администрацията;

- В процеса на бизнес анализ да бъдат изследвана съвместимостта на бизнес процесите на Възложителя с вече одобрени оптимизирани референтни модели за предоставяне на услуги и нормативни изисквания на Базисен модел за Комплексно административно обслужване в държавната администрация. При наличие на разработени модели за предоставяне на услуги по „Епизоди от живота" и „Събития от бизнеса", които включват услуги, предоставяни от Възложителя, да бъдат съобразени нуждите от модификации в референтните модели, за да се постигне подобряване на времето и намаляване на административната тежест при комплексно обслужване, спрямо предоставянето на отделните услуги поединично;
- В случай че се касае за административни услуги, те трябва да бъдат разграничени на базата на разлики в бизнес процесите и да не бъдат генерализирани и/или обобщавани на базата на типа на действие (например ако Системата издава няколко различни вида удостоверения, с които се удостоверяват различни обстоятелства, административните услуги трябва да бъдат регистрирани отделно);
- Удостоверителните административни услуги трябва да бъдат регистрирани и като вътрешни административни услуги и да бъде реализирана възможност за предоставянето на тези услуги като електронни вътрешно- административни услуги за нуждите на комплексното административно обслужване чрез служебен онлайн интерфейс.

5.1.1. Специфични изисквания към етапите на бизнес анализа и разработка

В началото на изпълнението на етапа Изпълнителят ще изготви детайлен график за изпълнение на поръчката, който подлежи на съгласуване с Възложителя.

Изпълнителят ще направи детайлно проучване на изискванията към функционалностите на системата. Детайлното проучване на системните и софтуерни изисквания ще обхващат всички компоненти в обхвата на поръчката, свързани с изграждането на софтуерното решение и внедряването.

Детайлното проучване и изготвянето на техническата спецификация ще включва изпълнението на следните задачи и изисквания:

- Изпълнителят ще следва Методологията за усъвършенстване на работните процеси за предоставяне на административни услуги и Наръчника за прилагане на методологията, приета с Решение № 578 на Министерския съвет от 30 септември 2013 г.;

- Ще бъде предвидена фаза на проучване, по време на която ще се дефинират потребителските нужди, да се проведат предварителни тестове с потребители и да се изработи план, по който да се адресират идентифицираните нужди;
- Ще бъдат предвидени периодични продуктови тествания по време на разработката и внедряването на Системата, с извадка (фокус-група) от бъдещите потребители на електронната услуга (служители в администрацията, граждани, доставчици на обществени услуги), чрез които да се изпита и оцени използваемостта на услугите и потребителските интерфейси, както и за да бъдат отстранени затруднения и несъответствия със заданието;
- Ще се спазват нормативните изисквания за еднократно събиране и повторна употреба на данни в държавната администрация (съгласно АПК и ЗЕУ) и в разработените бизнес процеси да не се изискват данни за заявителя и/или за получателя на услугата, които могат да се извлекат автоматично в процеса на електронна идентификация чрез Центъра за електронна идентификация или на база на ЕГН и от Квалифициран електронен подпис /КЕП/. При необходимост изпълнителят ще предложи на Възложителя адекватни промени в нормативната уредба, които да хармонизират съответните секторни нормативни изисквания с общите разпоредби на Административнопроцесуалния кодекс, Закона за електронно управление, Закона за електронния документ и електронния подпис и приложимите подзаконови актове, ако действащата нормативна уредба изисква:
    - изрично попълване на типов хартиен формуляр, върху който потребителите трябва да се подпишат собственоръчно и/или който да приложат като изискуем документ при заявяването на електронна административна услуга;
    - изрично деклариране или обявяване на обстоятелства или данни, които се администрират и/или удостоверяват от други държавни органи и могат да бъдат получени по служебен път, включително и автоматизирано през съответни интеграционни интерфейси;
    - други нормативни изисквания, които водят до неоптимални или ненужно бюрократични процеси, които биха могли да бъдат оптимизирани при заявяване и предоставяне на електронни административни услуги;
- Ще се разработят информативни текстове за всяка електронна административна услуга, които включват като минимум:
    - Условия за предоставяне на услугата;
    - Срокове за предоставяне на услугата;
    - Такси за заявяване и съответно предоставяне на услугата;
    - Начини за получаване на услугата;
    - Резултат от предоставяне на услугата;
    - Отказ от предоставяне на услугата;
- Информативните текстове за всяка електронна административна услуга ще бъдат достъпни за потребителите още като първа стъпка от заявяването на услуга;
- Тарифирането на услугите (ако е приложимо) ще бъде реализирано така, че Системата да съхранява всички версии на тарифите за услуги (от дата до дата) и да прилага съответната тарифа, в зависимост от момента, в който е заявена дадена услуга;

- Ще бъде оптимизиран потребителският път от влизане на сайта до заявяване и получаване на услуга и пътят от регистрация на нов потребител до заявяване и получаване на услуга.

5.1.2. Лица извършващи дейности с отпадъци

В информационната система, ще се дефинират следните лица, и при всяко действие с отпадък да се избира от падащо меню съответното лице, което извършва действието:

- причинители на отпадъци - лица които са образували отпадъка – физически лица/юридическо лице;
- притежатели на отпадъци - лице които са причинители или имат фактическа власт върху отпадъка;
- търговци на отпадъци - лица които закупуват и продават отпадъци;
- брокери на отпадъци - лица които организират третирането на отпадъци от името на други лица;
- предприятия за превоз и събиране на отпадъци, включително предварително сортиране, опаковане, съхраняване с цел превозването им до съоръжение за третиране на отпадъци и транспортиране;
- учреждения или предприятия, които извършват дейности по третиране на отпадъци – обезвреждане или оползотворяване.

За всяко от гореизброените лица, ще се регистрират в настоящата система, действия с битовите отпадъци.

При всяко действие с отпадък, в системата ще се отрази:

- кодът на отпадъка, съгласно Наредба № 2 от 23.07.2014 г. за класификация на отпадъците;
- количеството от всеки вид отпадък;
- вида на опаковката за всеки вид отпадък – съгласно UN, ADR или друга съответстваща класификация - при жп, морски или въздушен превоз;
- данни за лицето извършващо действие с отпадък;
- ролята на лицето;
- крайната точка на действието, включително оператора, държавата и обстоятелството, дали тя е член на ЕС или ЕАСТ или е член само на ОИСР;

В приложената таблица са представени спецификите и разликите в бизнес процесите в зависимост от качеството, в което действа заявител на ЕАУ, които ще бъдат отразени при реализацията на Системата:

Таблица 10 - Специфики и разлики в бизнес процесите в зависимост от качеството

Вид ползвател	Особености	Специфични процеси
Длъжностно лице, изготвящо справки или служител на юридическо лице извършващо дейности с отпадъци	Заявяване на справки по даден критерий, които системата осигурява автоматично, като подрежда наличната информация по избрания параметър, например за даден вид битов отпадък.	Справката трябва да се генерира на български и английски език. Всички полета за въвеждане на данни, както и падащите менюта за избор на приложимата опция, трябва да бъдат разработени като двуезични.
Законен представител на юридическо лице или упълномощен от него потребител, който въвежда/променя данни	За да обслужи нужди на юридическо лице, системата изисква оторизация с възможност да издава собствен сертификат за оторизация, преди да даде достъп за въвеждане на нови данни.	Услугата може да бъде предоставена, след като са изпълнени нуждите за идентификация - електронна идентификация по смисъла на ЗЕИ.
Длъжностно лице, което въвежда/променя данни	Системата осигурява специални права и възможности на ПУДООС, ИАОС и МОСВ и общините/центрове по събиране на опасни битови отпадъци, да добавят информация при определени правни основания – например изменение или оттегляне на разрешение за извършване на дейност, наложена санкция, просрочие от страна на даден оператор, приключване на изискуемо действие без негово участие, промяна на наименование и др.	Действието може да се извърши само след изискване за декларирането на правното основание, чрез изрична декларация, подписана с КЕП, и прилагане на копие от документалното основание за извършване на намеса в информационната система.

Правата за достъп ще бъдат определени с оглед следните изисквания:

- институционалните потребители – длъжностни лица, да виждат цялата въведена информация и да извършват справки;
- юридическите лица да виждат само данните които са въвели и да могат да променят само данните които са въвели, както и да въвеждат основание за промяната, при което да се гарантира запис на старите данни (тоест да има следа какво се е променило) и промяната от ЮЛ да е във вид на заявка, която да се одобрява от административно лице от страна на възложител, преди да се

извърши промяната (т.е. юридическитите лица- потребители, да могат да променят въведени от тях данни, като всяка корекции бъде отразявана в дневник, който никой да не може да коригира, за да има проследимост);

- администраторът да има пълни права, но да не може да изменя въведени данни.

За всяка категория ползватели, ще се отваря различен екран съобразно правата за достъп.

5.1.3. Изисквания за оптимизиране на процесите по подаване на декларации - регистрация на обстоятелства, изискуеми в съответствие с нормативната уредба и вътрешните правила

- Системата ще поддържа номенклатура с редактируеми двуезични шаблони на вписваните обстоятелства по предходната под-точка 5.1.2, които да бъдат достъпни за актуализация за администраторите на Системата; Трябва да се поддържа история на версиите на шаблоните и да няма възможност за перманентно премахване/изтриване на шаблони, а само смяна на статуса им и публикуване на нова версия;
- Ако даден оперативен процес изисква подаване на декларация от страна на заявител на услуга, при достигане на съответната стъпка от процеса Системата ще:
  - да попълва автоматично всички персонални данни на заявителя в електронна форма, генерирана на база на съответния шаблон на декларация;
  - да дава възможност на потребителя за избор на съответните обстоятелства, които може да декларира (ако шаблонът на декларацията предвижда възможност за деклариране на опционален набор от предефинирани обстоятелства);
  - да изисква потвърждение на обстоятелствата от страна на потребителя;

5.1.4. Изисквания към регистрите и предоставянето на административните услуги

- Всяка удостоверителна административна услуга в обхвата на системата ще бъде достъпна като вътрешно-административна електронна услуга чрез уеб-услуга, като комуникацията се подписва с електронен печат на институцията и с електронен времеви печат по смисъла на Регламент (ЕС) 910/2014;
- Всяка услуга, за която се допуска представителна власт, ще бъде интегрирана с Регистъра на овластяванията по смисъла на Закона за електронната идентификация;
- Системата няма да съхранява данни, на които възложителят не е първичен администратор, в случай че данните могат да бъдат извличани в реално време от регистър на съответния първичен администратор.

5.2.Изготвяне на системен проект

Изпълнителят ще изготви системен проект, който подлежи на одобрение от Възложителя. В системния проект ще бъдат описани всички изисквания за реализирането на системата. Изготвянето на системния проект включва следните основни задачи:

- Определяне на концепция на информационната система на базата на техническото задание;
- 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.

Изпълнението на задачите изисква дефиниране на 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, е необходимо да 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 е длъжен да ги отрази в системния проект в срок не по-късно от 10 работни дни.

Подробно описание може да бъде намерено в т. 9.4.

5.3.Разработване на софтуерното решение

Етапът на разработка включва изпълнението на следните задачи:

- Разработка на прототип, който трябва да бъде одобрен от Възложителя и въз основа на който трябва да се разработи цялата система;
- 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.

Методиката за разработка на софтуерното приложение е описана в т. 8.1.4. от настоящото предложение.

5.4. Тестване

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

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

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 8.1.6. „Методология за тестване".

5.5.Внедряване

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

Подробно описание на методиката за внедряване се намира в точка 8.1.5. от настоящия документ.

5.6.Обучение

Изпълнителят ще организира и да проведе обучения за следните групи и ползватели на софтуерното решение, в рамките на Задача 2.1 и Задача 3.4. от Техническото задание:

- Потребителска група 1 – потребители от 22 общини - Шумен, Разград, Левски, Съединение и Созопол и 17 по-малки общини – Велики Преслав, Смядово, Каспичан, Хитрино, Лозница, Самуил, Исперих, Завет, Цар Калоян, Пордим, Никопол, Белене, Марица, Калояново, Хисаря, Приморско и Царево – Задача 3.4;
- Потребителска група 2 - потребители в 5 (пет) пилотни общински центрове/площадки за събиране на опасни битови отпадъци, на територията на Шумен, Разград, Левски, Съединение и Созопол - Задача 2.1.
- Потребителска група 3 - длъжностни лица в ПУДООС – Задача 3.4.
- За провеждането на обученията Изпълнителят ще осигури за своя сметка:
- Необходимия хардуер;
- Необходимия софтуер;
- Учебни материали;
- Лектори.

Обученията ще включват не само теоретична подготовка под формата на семинари, но и практическа част, която ще позволи на обучаемите лица да се запознаят нагледно със Систематаи начина, по който тя функционира. За целта ще се използва внедрения софтуер в експлоатационна среда (но преди да бъде пуснат в реална експлоатация).

Изпълнителя ще изготви и съгласува с Възложителя План и програма за обучение, спрямо която след одобрение ще бъдат организирани обученията на потребителите.

Подробно описание на методиката за обучение може да бъде намерено в т. 8.1.8 от настоящия документ.

5.7.Гаранционна поддръжка

Предлагаме 24-месечен гаранционен срок и ще изготвим план за поддръжката функционирането на системата до 2021 г. включително.

Ще бъде осигурена гаранционна поддръжка за период от 24 месеца 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, заложени 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 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. ДЕТАЙЛЕН ПЛАН-ГРАФИК ЗА ИЗПЪЛНЕНИЕ НА ПРОЕКТА

Предлагаме срокове за изпълнение на услугата по дейности съгласно т. 3.5 от Техническата спецификация, както следва:

Дейност	Срок [месеци]
Дейност 1: Изработване на софтуерна платформа на информационната система Задача 1.1. Изработване на техническите характеристики на софтуерната платформа на системата Задача: 1.2. Изработване на софтуерната платформа Задача: 1.3. Консултиране на разработката	до 6
Дейност 2: Провеждане на пилотното тестване, коригиране и финализиране на софтуерната платформа на информационната система Задача 2.1. Обучение на място на ползвателите Задача 2.2 Тестване на системата в действие Задача 2.3. Корекции и финализиране на софтуерната платформа	до 1
Дейност 3. Подготовка за внедряване на информационната система Задача 3.1. Инсталиране на финализираната софтуерната платформа Задача 3.2. Изготвяне на Ръководство за ползване на информационната система Задача 3.3. Формиране на екип за консултиране във връзка с внедряването на системата Задача 3.4. Обучение на различните потребители за запознаване с информационната система и работа с нея	до 1
Дейност 4. Внедряване на системата Задача 4.1. Завършване на продукта Задача 4.2. Осигуряване на достъп до софтуерната платформа на системата	до 2
Задача 4.3. Гаранционна поддръжка за 24 месеца и отстраняване на грешки във функционирането на софтуера	24

Детайлният график на изпълнението е приложен в следната диаграма:

7. ОБЩИ И СПЕЦИФИЧНИ ИЗИСКВАНИЯ КЪМ РЕАЛИЗАЦИЯТА НА СОФТУЕРНОТО РЕШЕНИЕ

7.1.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.

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

- ***Информационна система 1 – Националната информационна система за отпадъци (НИСО);***
- ***Информационна система 2*** –интегрираната информационна система на държавната администрация (ИИСДА), в частност Регистъра на услугите, в който се вписват допустимите заявители и получатели на административни услуги - например: проверка на достъпа до съответните обстоятелства; посочване на идентификатор на конкретна административна услуга, за която е нужно извличането на съответните обстоятелства от регистрите;
- Интеграциите с външни информационни системи и регистри трябва да се реализира чрез стандартен интеграционен слой.

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

Интеграция с други системи

Интеграцията ще се базира на отворени стандарти, както за решението така и за компонентите и механизмите за интеграция на системите.

Ще бъдат използвани стандартни транспортни протоколи като TCP/IP, SSL, HTTP и HTTPS. Интеграцията ще гарантира консистентност на данните.Тя няма да зависи от езика за програмиране на системите. Като минимум ще предоставя API за интеграция на C/C++, Java и .Net приложения.

Когато за целите на интеграцията е удачно да се използват съобщения, архитектурата ще отговаря, без да се ограничава на следните изисквания:

- Да поддържа синхронен и асинхронен обмен на съобщенията.
- Да поддържа приоритизация на съобщенията според приоритетите на интегрираните системи.
- Да поддържа опашка от съобщения и да съхранява съобщенията, ако някоя система е временно недостъпна.

Общи изисквания

Като общо изискване, съгласно чл. 10, ал. 1 от Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги

/НООИСРЕАУ/, (приета с ПМС No 3 от 9.01.2017 г., обн., ДВ, бр. 5 от 17.01.2017 г., в сила от 01.03.2017г.), Информационната система трябва да се идентифицира пред регистрите чрез цифров сертификат, вписан в ИИСДА, двустранно по протокол TLS (Transport Layer Security – Сигурност на транспортния слой), версия 1.2 или по-висока, дефиниран в Препоръка RFC 5246, приета от IETF (The Internet Engineering Task Force – Целева група за Интернет инженеринг) през август 2008 г. При вписването, заличаването или извличането на данни от регистър от длъжностни лица лицата, които извършват вписването, заличаването или извличането, се идентифицират по реда на ЗЕИ. Идентификация не се изисква за извличане на данни от публични регистри.

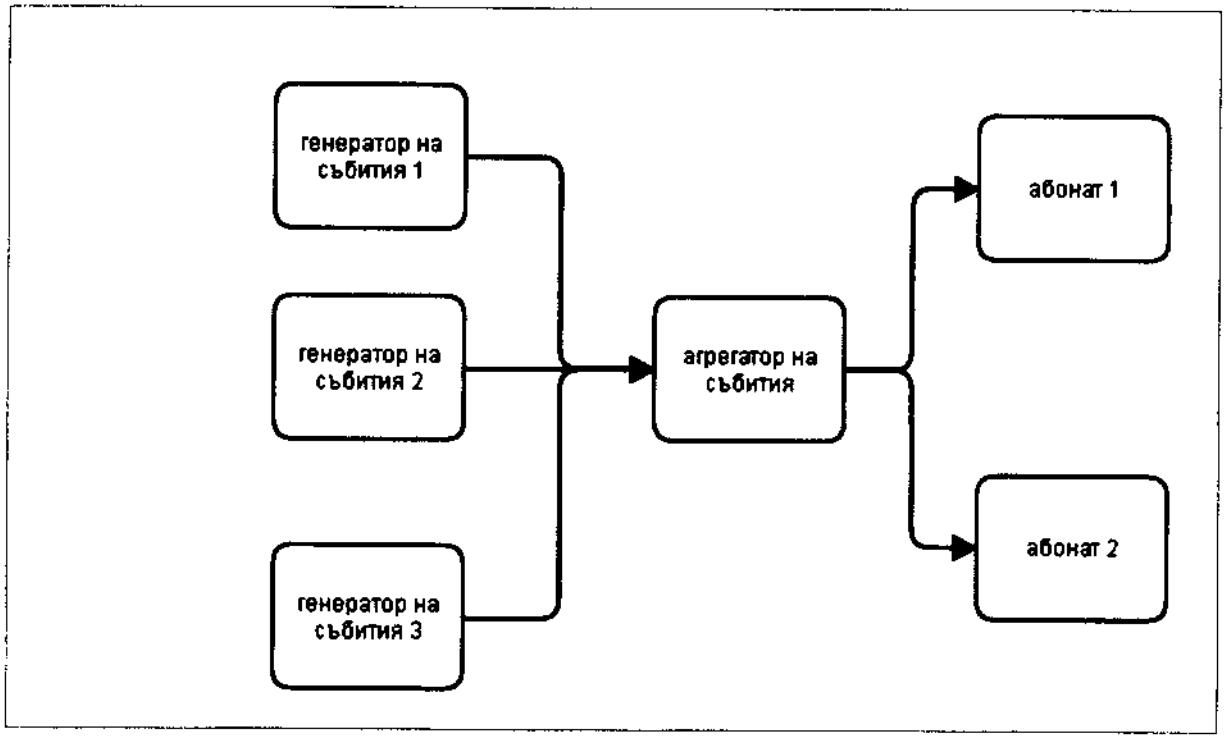
7.2.Интеграционен слой

- 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. Ще бъде предвидена 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 машинно поискване и предаване на история на изпълнените транзакции по машинен обмен на данни, предоставените електронни услуги и начислени такси, към информационни системи на други публични институции и доставчици на обществени услуги, с оглед предоставяне на комплексно административно обслужване /КАО/, съгласно действащите изисквания за оперативна съвместимост и информационна сигурност;
- Ще бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано изпращане на документи и нотификации чрез електронна препоръчана поща към подсистемата за сигурно връчване, част от националната система за електронна идентификация, съгласно действащите изисквания за оперативна съвместимост;
- 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;
- Ще бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано изпращане на ценни електронни документи към централизираната система за е-Архивиране, ако е приложимо и съответната система или регистър оперират с такива документи, съгласно действащите изисквания за оперативна съвместимост;
- За всяка операция по вписване, заличаване или извличане на обстоятелства се съхранява информация за момента на извършване и за лицето, съответно информационната система, извършила операцията, освен ако данните не са публични съгласно закон или други специфични изисквания.
- Идентификация ще се осъществява с всяка информационна система, с която регистърът или базата данни извършва комуникация, включително регистъра на регистрите, чрез електронно удостоверение във формат X.509, издадено за съответния регистър, съгл. чл. 6, ал. 1 от НОИИСРЕАУ.

- Достъпът до регистрите може да се извършва директно или чрез централен компонент, който гарантира спазването на изискванията на тази глава и отговаря на изисквания, определени от председателя на Държавна агенция "Електронно управление". Централният компонент, включително правата за достъп до ресурси чрез него, се определя от председателя на Държавна агенция "Електронно управление" (интеграция на базовите регистри на първичните администратори на данни със средата за междурегистров обмен, интеграция с RegiX и регистрите, които се поддържат от RegiX).

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"

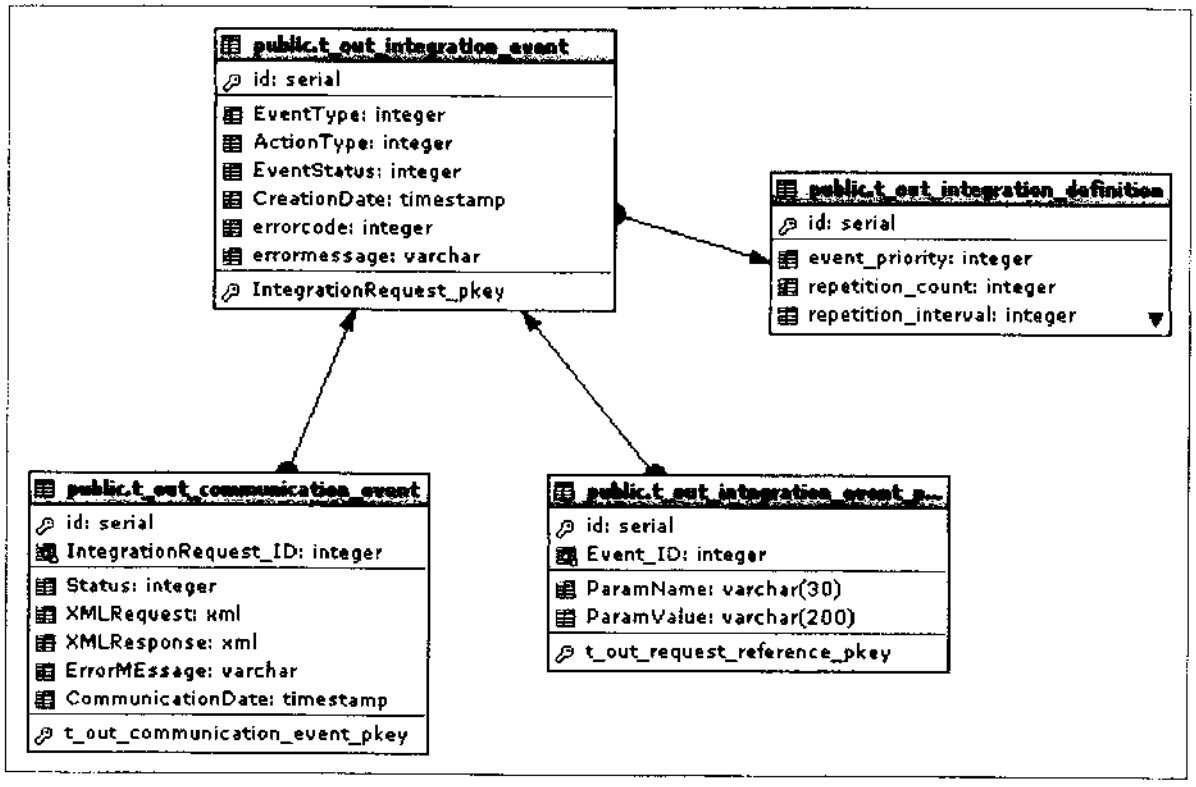
Архитектурата на модулът за интеграция с външни системи е базирана на модела "Агрегатор на събития". Моделът "Агрегатор на събития" се опитва да преодолее ограничаването на традиционния подход за управление на събития, като предостави централно място за публикуване и абониране за събития, които не са 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 модулът 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.

Модулът 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.

7.3.Технически изисквания към интерфейсите

Системата ще осигурява стандартизирани интерфейси към вътрешни и външни информационни системи. Изпълнителят ще създаде общ механизъм за обмен на данни, който позволява в бъдеще системните администратори да дефинират допълнителни структури от данни и информационни единици за обмен с други системи, без съществени софтуерни промени в съществуващите системи. Тези интерфейси ще бъдат двупосочни (към и от системата) и ще са XML-базирани, реализирани посредством web service, за което ще се изготви съответната техническа спецификация.

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 публични и 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, които всеки интерфейс обслужва.
- Ще се реализира интегриране на модул за разпределен кохерентен кеш (Distributed Caching) на „горещите данни", които Системата получава и/или които се обменят през служебните онлайн интерфейси, като логиката на Системата трябва гарантира кохерентност (Cache Coherency) между кешираните данни и данните, съхранявани в базите данни;
- 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.
- За извършване на интеграционни тестове с цел по-лесно и устойчиво интегриране на съществуващите и бъдещи информационни системи, ще бъде създадена и поддържана тестова среда. Тестовата среда ще бъде достъпна както за разработчиците извършващи интеграционни тестове, като и за изпълняващите дейности за други администрации или за бизнеса. Тестовете ще се извършват съобразно описаната в т. 8.1.7. **Error! Reference source not found.**.
- Идентификация ще се осъществява с всяка информационна система, с която регистърът или базата данни извършва комуникация, включително регистъра на регистрите.
- Достъпът до регистрите може да се извършва директно или чрез централен компонент, който гарантира спазването на изискванията на тази глава и отговаря на изисквания, определени от председателя на Държавна агенция "Електронно управление". Централният компонент, включително правата за достъп до ресурси чрез него, се определя от председателя на Държавна агенция "Електронно управление" (интеграция на базовите регистри на първичните администратори на данни със средата за междурегистров обмен, интеграция с RegiX и регистрите, които се поддържат от RegiX).
- В съответствие с чл.34, ал.6 от НОИИСРЕАУ системата ще предоставя програмни интерфейси за достъп до своите преписки и документи, както и за получаване на

входящи номера и регистриране на преписки, които да не подлежат на изтриване и модификация и интегритетът им следва да е защитен чрез криптографски методи.

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.

7.4.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 1януари 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.

- Правата за въвеждане на данни ще се активират само след влизане в системата с EU-login;
- Ще бъде реализирана интеграция с националната схема за електронна идентификация съгласно изискванията на Закона за електронната идентификация и действащите нормативни правила за оперативна съвместимост. За целта подсистемата за автентикация и оторизация на потребителите ще поддържа интеграция с външен доставчик на идентичност - в случая с центъра за електронна идентификация към Държавна агенция „Електронно управление". Реализацията на интеграцията трябва да бъде осъществена по стандартни протоколи SAML 2.0 и/или OpenID Connect;
- Системата ще поддържа и стандартен подход за регистрация на потребители с потребителско име и парола - за потребители, които нямат издадени удостоверения за електронна идентичност, и за потребители, които желаят да продължат да използват електронни административни услуги с квалифициран електронен подпис /КЕП/;

- 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 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 токън 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.
- При реализиране на вход в Системата с удостоверение за електронна идентичност, по националната схема за електронна идентификация, Системата ще използва потребителския профил, създаден в системата за електронна идентификация, чрез интерфейси и по протоколи съгласно подзаконовата нормативна уредба към Закона за електронната идентификация. В случай че даден потребител има регистриран потребителски профил в Системата, който е създаден преди въвеждането на националната схема за електронна идентификация, Системата трябва да предлага на потребителя възможност за "сливане" на профилите и асоцииране на локалния профил с този от националната система за електронна идентификация. Допустимо е Системата да поддържа и допълнителни данни и метаданни за потребителите, но само такива, които не са включени като реквизити в централизирания профил на потребителя в системата за електронна идентификация.
- Системата ще се съобразява с предпочитанията на потребителите, дефинирани в потребителските им профили в системата за електронна идентификация, по отношение на предпочитаните комуникационни канали и канали за получаване на нотификации.

7.5.Отворени данни

7.5.1. Автоматизиран достъп

За разработването на онлайн интерфейс за свободен публичен автоматизиран ще бъде създаден модул за описание на отворените данни – който ще поддържа и визуализира каталог и описание на предоставяните набори данни.

Сигурността на данните се гарантира от съответните потребителски права за достъп. Потребителите нямат права за въвеждане/ модифициране на данните, а само за четене.

Достъпът до хранилището за данни се осъществява единствено посредством специално проектиран и реализиран потребителски интерфейс, като потребителите нямат възможност за непосредствен достъп до данните.

Ще бъде създаден интерфейс за отворени данни с посочените функционалности и данните съгласно всички изисквания на Директива 2013/37/ЕС за повторна употреба на информацията в обществения сектор и на Закона за достъп до обществена информация. Интерфейса ще осигури автоматизиран достъп като „отворени данни", в машинночетим, отворен формат до определени документи, информация и данни в Системата.

Ще бъде разработен и внедрен онлайн интерфейс за предоставяне на пространствени данни, в машинночетим, отворен формат и интеграция с Националния портал за достъп до пространствени данни, съгласно всички изисквания на Директива 2007/2/ЕО и Закона за достъп до пространствени данни. Ще се поддържат всички набори от данни, които са изискуеми по Директива 2007/2/ЕО и за които Възложителят се явява първичен администратор на данните.

7.5.2. Интеграция с портала за отворени данни http://opendata.government.bg

Порталът за отворени данни opendata.governmrnt.bg представлява единна, централна, публична уеб-базирана информационна система, която предоставя средства за публикуване и управление на информация за повторно използване в отворен, машинно-четим формат заедно със съответните метаданни. Платформата е изградена по начин, който позволява цялостното извличане на публикуваната информация или на части от нея.

Средствата за публикуване в портала ще бъдат проучени и описани в детайлната техническа спецификация на етапа анализ на изискванията. Това описание ще послужи за реализация на модулите за зареждане и извличане на данни от базата данни на портала.

Детайлната техническа спецификация ще помогне за реализация на автоматизирано изпращане на ресурси към базата данни на портала.

В рамките на дейността ще бъде направена регистрация в портала от името на Възложителя.

В резултат на изпълнение на дейността ще се извърши подготовка за автоматизирано изпращане на ресурси към Opendata.government.bg като изпращането ще започне след решение на Възложителя.

7.5.3. Моделиране на информационния обмен на данни с външни източници

Ще бъдат моделирани процесите и интерфейсите за организиране на достъпа до данни от външните източници, информация от които се използва при изпълнение на функциите по предоставяне на данни в отворен, машинночетим формат. Тези процеси и интерфейси ще бъдат моделирани в зависимост от наличността и готовността на

външните системи, както и от техническите възможности да достъп до необходимата информация, които съответните външни системи предоставят.

За всеки процес/интерфейс ще се моделират следните обекти и връзките помежду им:

- Участници в процеса и сценарии за изпълнение;
- Метод/интерфейс за обмен на данни;
- Структура на обменяните данни (информационни обекти);
- Необходими условия и данни за обмен и др.

7.6.Формиране на изгледи

Потребителите на Системата ще получават разрези 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.

7.7.Администриране на системата

Системата ще се изгради със следните функционални характеристики:

- ✓ Системно администриране ще се извършва от оторизирани ИТ специалисти – системни администратори.
- ✓ Администраторите на Системата ще имат достъп до всички информационни ресурси на системата;
- ✓ Системата ще позволява отдалечено администриране на потребители и системни ресурси чрез наградена СУС.
- ✓ Системното администриране ще включва цялостен мониторинг и управление на всички информационни ресурси на новосъздаденото софтуерно решение.
- ✓ Системата ще осигурява администриране на потребителите и правата за достъп.

7.8.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.

- Приложените технологии за разработка на системата ще бъдат изцяло с отворен код и ще се съхраняват в публично хранилище Субвършън (Subversion - SVN). Хранилището за код на SVN може да бъде конфигурирано за предоставяне на публичен достъп до програмния код и документацията. SVN управлява ключовата информация за разработката на системата, процесите на поддръжка и инсталиране и база за потенциално преизползваеми артефакти.
- 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)
  - Apache License 2.0
  - New BSD license
  - MIT License
  - Mozilla Public License 2.0

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 па комерсиална поддръжка и са подкрепени от организации с идеална цел или комерсиални организации, вкл.:

- Уеб сървър Kestrel:
- Бази данни Postgres (ако Възложителя избере във фазата на анализ да се използва безплатна база данни, а не базата данни, на която е базирана съществуващата реализация – Microsoft SQL Server);
- Платформа за разработка :Net 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.

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. 4.6. от настоящото предложение.

7.9.Системна и приложна архитектура

Предлаганото решение ще има технологична архитектура осигуряваща отлична работоспособност и отказоустойчивост на системата, както и недискриминационно инсталиране и оперирање в продуктивен режим, върху виртуална инфраструктура, съответно върху Държавния хибриден частен облак.

Изпълнителят ще предвиди използване на мрежата на държавната администрация като комуникационна среда и като основен доставчик на защитен Интернет капацитет (Clean Pipe).

Изпълнителя ще документира детайлно изискванията на системата по отношение на използвани комуникационни протоколи, TCP портове и пр., за да се осигури максимална защита от хакерски атаки и външни проникванията чрез прилагане на подходящи политики за мрежова и информационна сигурност от Възложителя в инфраструктурата на Държавния хибриден частен облак и EECM.

Предлаганата архитектура на системата ще бъде базирана на трислойна архитектура, която се е доказала като най-доброто техническо решение за технологична база на системи с многопотребителски конкурентен достъп.

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 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 наложили 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 (Accept 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 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 па 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 оперираие в продуктивен режим, върху виртуална инфраструктура, съответно върху Държавния хибриден частен облак (ДХЧО).
- 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;
- 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 проникванията чрез прилагане на подходящи политики за мрежова и информационна сигурност от Възложителя в инфраструктурата на Държавния хибриден частен облак и ЕЕСМ;
- 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.
- Системата ще бъде разработена така, че да позволява използването ѝ от много различни институции (т.нар. multitenancy), като за използване от нова институция няма да се изисква нова инсталация.
- 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.
- Предвижда се архитектурата на системата да гарантира достъп 24/7/365, като позволява едновременна работа на не по-малко от 200 потребителя, както и да позволява мащабируемост на системата и базата данни, само чрез разширяване на възможностите на хардуера.

Детайлно описание на подхода за реализация е налично в 8.2. от настоящото предложение.

7.10. 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.

Базовите софтуерни платформи за разработка на проекта са с отворен код, 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.

7.11. Подход за избор на отворени имплементации и продукти

Проектът ще преизползва максимално налични публично достъпни инструменти, библиотеки и платформи с отворен код, като за реализацията на Системата ще се използват, винаги когато е възможно, 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.

7.12. Подход за работа с външните софтуерни ресурси

При използването на свободни имплементации на софтуерни библиотеки се предвижда да се организира копие (fork) на съответното хранилище в общото хранилище за проекти с отворен код, финансирани с публични средства в България - https://github.com/governmentbg. Използващите свободните библиотеки компоненти задават за "upstream repo" хранилищата в областта governmentbg, като задължително ще се реферира използваната версия/commit identificator.

Когато се налага промяна в изходния код на използван софтуерен компонент, промените ще се извършват във fork хранилището на governmentbg в съответствие с изискванията на основния проект. Изпълнителят ще извърши необходимите действия за включване на направените промени в основния проект чрез "pull requests" и извършване на необходимите изисквани от разработчиците на основния проект промени до приемането им. Тези дейности ще бъдат извършвани по време на целия проект.

При установяване на наличие на нови версии на използваните проекти ще се извършва анализ на влиянието върху настоящата система. В случаите, при които се оптимизира използвана функционалност, отстраняват се пропуски в сигурността, стабилността или бързодействието, новата версия ще се извлича и използва след успешното изпълнение на интеграционните тестове.

7.13. 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.

7.14. 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. 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).

Изходният 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. Управление на версиите.

В случай че върху част от компонентите, нужни за компилация, има авторски права, те могат да бъдат или в отделно хранилище с подходящия за това лиценз или за тях трябва да 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;
- 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.

7.15. Бързодействие и мащабируемост

7.15.1. 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.

7.15.2. 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.

7.15.3. Кохерентно кеширане на данни и заявки

- Отделните информационни системи, подсистеми и интерфейси ще бъдат проектирани и ще използват системи за разпределен кохерентен кеш в случаите, в

които това би довело до подобряване на производителността и мащабируемостта, чрез спестяване на заявки към СУБД или файловите системи на сървърите.

Изпълнителят ще опише детайлно подхода и използваните механизми и технологии за реализация на разпределения кохерентен кеш. както и системните компоненти, които ще използват разпределения кеш в системния проект.

- Разпределеният кохерентен кеш ще поддържа възможност за компресия на подходящите за това данни - например тези от текстов тип; компресирането на данни може да бъде реализирано и на приложно ниво;
- Използваният алгоритъм за създаване па ключове за съхранение/намиране на данни в кеша няма да допуска колизии и ще използва оптимално процесорните ресурси за генериране на хешове:
- Изпълнителят ще подбере подходящи софтуерни решения с отворен код за реализираме на буфериране и кеширане на данните к оперативната памет на сървърите. В зависимост от конкретните приложни случаи (Use Cases) е допустимо да се използват и внедрят различни технологии, които покриват по-добре конкретните нужди - например решения като Memcached или Redis в комбинация с Redis GeoAPI могат да осигурят порядъци по-висока мащабируемост и производителност за често достъпвани оперативни данни, номенклатурни данни или документи.

Като минимум разпределен кохерентен кеш трябва ще бъде предвиден при:

- Извличане на информация от номенклатури и атомични данни за статус и актуално състояние на партиди от регистри в информационните системи;
- Извличане на информация от предефинирани периодични справки;
- Информация от лога на транзакциите при достъп с електронно-ИД до дадена услуга;
- Информация за извършените плащания;
- Други, които са идентифицирани на етап бизнес и системен анализ.
- От кеша ще бъдат изключени прикачени файлове и големи по обем резултати от справки.

7.15.4. Използване на HTTP/2

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, трябва да 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.

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:

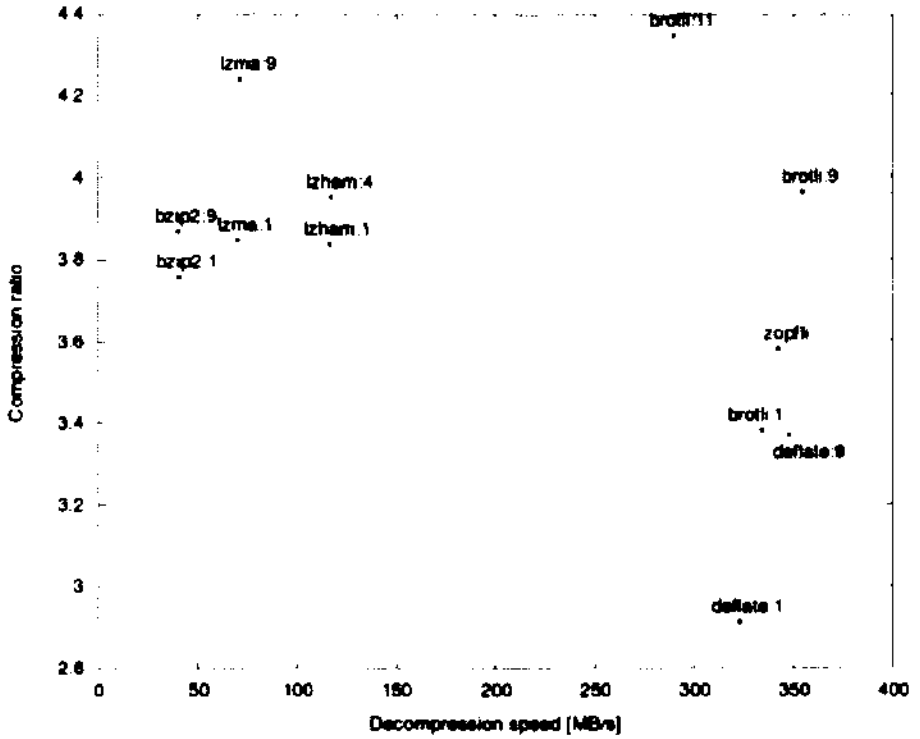
- Намаляване на packet header overhead (bandwidth savings);
- Намаляване на загубата на пакети;
- По-добро време за интерактивно реагиране;
- Намаляване на разходите за инфраструктура, повече потребители на channel bandwidth означава по-малко разходи за разполагане на инфраструктурата.

Тези предимства водят до подобрено 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 Engeneering 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, приоритизиращ 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 възмжността 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.

7.16. Подписване на документи

При реализация на електронно подписване с всички видове електронен подпис ще се съблюдава спазването на следните изисквания:

- Трябва да се подписва сигурен хеш-ключ, генериран на базата на образа/съдържанието, а не да се подписва цялото съдържание.
- Минимално допустимият алгоритъм за хеширане, който трябва да се използва при електронно подписване, е SHA-256. В случаите, в които не се подписва уеб съдържание (например документи, файлове и др.), е необходимо да се реализира поточно хеширане, като се избягва зареждането на цялото съдържание в оперативната памет.
- Системата трябва да поддържа подписване на електронни изявления и електронни документи и с електронни подписи, издадени от Доставчици на доверителни услуги в ЕС, които отговарят на изискванията за унифициран профил на електронните подписи, съгласно подзаконовите правила към Регламент ЕС 910/2014, които влизат в сила и са задължителни от 1 януари 2017 г.;

- Трябва да бъдат анализирани техническите възможности за реализиране на подписване на електронни изявления и документи без използване на Java аплет и без да се изисква от потребителите да инсталират Java Runtime, като по този начин се осигури максимална съвместимост на процеса на подписване с всички съвременни браузъри. Такава реализация може да бъде осъществена чрез:
- използване на стандартни компоненти с отворен код, отговарящи на горните условия, които са разработени по други проекти на държавната администрация и са достъпни в хранилището, поддържано от Държавна агенция „Електронно управление" – при наличие на такива компоненти в хранилището те трябва да се преизползват и само да бъдат интегрирани в Системата;
- използване на плъгин-модули с отворен код, достъпни за най-разпространените браузъри (Browser Plug-ins), които са адаптирани и поддържат унифицираните профили на електронните подписи, издавани от ДДУ в ЕС, и съответните драйвери за крайни устройства за четене на сигурни носители или по стандартизиран в националната нормативна уредба протокол за подписване извън браузъра;
- чрез интеграция с услуги за отдалечено подписване, предлагани от доставчици на доверителни услуги в ЕС.
- Качество и сигурност на програмните продукти и приложенията
- Да бъде предвидено спазването на добри практики на софтуерната разработка – покритие на изходния код с тестове – над 60%, документиране на изходния код, използване на среда за непрекъсната интеграция (Continuous Integration), 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, трябва да отговарят на актуалните уебстандарти за визуализиране на съдържание.

7.17. Информационна сигурност и интегритет на данните

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.