Приложение № 1 към чл. 38, ал. 3

Изпълнителна агенция „Морска администрация“

ТЕХНИЧЕСКО ЗАДАНИЕ

за

Актуализация и надграждане на национална информационна система SafeSeaNet

СЪДЪРЖАНИЕ

1. РЕЧНИК НА ТЕРМИНИ, ДЕФИНИЦИИ И СЪКРАЩЕНИЯ

1.1. Използвани акроними

Акроним	Описание
АИС	Автоматизирана информационна система
АМС	Администрация на Министерския съвет
АОП	Агенция по обществени поръчки
АПК	Административнопроцесуален кодекс
БУЛСТАТ	Регистър Булстат
ДАЕУ	Държавна агенция "Електронно управление"
ЗДОИ	Закон за достъп до обществена информация
ЗЕДЕП	Закон за електронния документ и електронния подпис
ЗЕУ	Закон за електронното управление
ИТ	Информационни технологии
КАО	Комплексно административно обслужване
ТР	Търговски регистър
ДХЧО	Държавен хибриден частен облак
ЦАИС	Централизирана автоматизирана информационна система
SDK	Software development kit
API	Application programming interface/Приложно програмен интерфейс

1.2. Технологични дефиниции

Термин	Описание
Виртуална комуникационна инфраструктура	Инфраструктура, която на база съществуваща физическа свързаност, предоставена от ДАЕУ, предоставя възможност за изграждане на отделни и защитени виртуални мрежи за всяка една от структурите в сектора, при гарантиране на

	сигурен и защитен обмен на информация в тях.
Държавен хибриден частен облак	Централизирана на ниво държава информационна инфраструктура (сървъри, средства за съхранение на информация, комуникационно оборудване, съпътстващо оборудване, разпределени в няколко локации, в помещения отговарящи на критериите за изграждане на защитени центрове за данни), която предоставя физически и виртуални ресурси за ползване и администриране от секторите и структурите, които имат достъп до тях, в зависимост от нуждите им, при гарантиране на високо ниво на сигурност, надеждност, изолация на отделните ползватели и невъзможност от намеса в работоспособността на информационните им системи или неоторизиран достъп до информационните им ресурси. Изолацията на ресурсите и мрежите на отделните секторни ползватели (е-Общини, е-Правосъдие, е-Здравеопазване, е-Полиция) се гарантира с подходящи мерки на логическо ниво (формиране на отделни клъстери, виртуални информационни центрове и мрежи) и на физическо ниво (клетки и шкафове с контрол на достъпа).
Софтуер с отворен код	Компютърна програма, която се разпространява при условия, които осигуряват безплатен достъп до програмния код и позволяват: Използването на програмата и производните на нея компютърни програми, без ограничения в целта; Промени в програмния код и адаптирането на компютърната програма за нуждите на нейните ползватели; Разпространението на производните компютърни програми при същите условия. Списък на стандартни лицензионни споразумения, които предоставят тези възможности, който може да бъде намерен в подзаконовата нормативна уредба към Закона за електронно управление или на: http://opensource.org/licenses.
Машинночетим формат	Формат на данни, който е структуриран по начин, по който, без да се преобразува в друг формат позволява софтуерни приложения да идентифицират, разпознават и извличат специфични данни, включително отделни факти и тяхната вътрешна структура.

Отворен формат	Означава формат на данни, който не налага употребата на специфична платформа или специфичен софтуер за повторната употреба на съдържанието и е предоставен на обществеността без ограничения, които биха възпрепятствали повторното използване на информация.
Метаданни	Данни, описващи структурата на информацията, предмет на повторно използване.
Официален отворен стандарт	Стандарт, който е установен в писмена форма и описва спецификациите за изискванията как да се осигури софтуерна оперативна съвместимост.
Система за контрол на версиите	Технология, с която се създава специално място, наречено “хранилище”, където е възможно да се следят и описват промените по дадено съдържание (текст, програмен код, двоични файлове). Една система за контрол на версиите трябва да може: • Да съхранява пълна история - кой, какво и кога е променил по съдържанието в хранилището, както и защо се прави промяната; • Да позволява преглеждане разликите между всеки две съхранени версии в хранилището; • Да позволява при необходимост съдържанието в хранилището да може да се върне към предишна съхранена версия; • Да позволява наличието на множество копия на хранилището и синхронизация между тях. Цялата информация, налична в системата за контрол на версиите за главното копие на хранилището, прието за оригинален и централен източник на съдържанието, трябва да може да бъде достъпна публично, онлайн, в реално време.
Първичен регистър	Регистър, който се поддържа от първичен администратор на данни - административен орган, който по силата на закон събира или създава данни за субекти (граждани или организации) или за обекти (движими и недвижими) за първи път и изменя или заличава тези данни. Например Търговският регистър е първичен регистър за юридическите лица със стопанска цел, Имотният регистър е първичен регистър за недвижима собственост.

2. ВЪВЕДЕНИЕ

2.1. Цел на документа

Целта на настоящия документ е да опише софтуерните изисквания към изпълнението на обществена поръчка с предмет: **Актуализиране и надграждане на национална информационна система SafeSeaNet**

В настоящото техническо задание са описани и изискванията към проектната организация, документацията и отчетността.

2.2. За възложителя – функции и структура

Изпълнителна агенция "Морска администрация” (ИАМА) е юридическо лице на бюджетна издръжка към Министерство на транспорта, второстепенен разпоредител с бюджетни средства, със седалище София и с регионални дирекции във Варна, Бургас, Русе и Лом.

Основната дейност на Агенцията е да:

- организира и координира дейности по безопасността на корабоплаването в морските пространства и във вътрешните водни пътища на Република България;
- осигурява реалната връзка между държавата и корабите, плаващи под българско знаме;
- упражнява контрол за:

  a) спазването на условията за безопасност на корабоплаването спрямо български и чужди кораби;

  b) спазването на условията на труд и живот на моряците;

  c) предоставянето на услуги по управление на трафика и информационно обслужване на корабоплаването в морските пространства, вътрешните водни пътища, каналите, пристанищата на Република България и другите, определени по съответния ред, райони;

  d) спазване на изискванията за качество на корабните горива.

- организира и координира търсене и спасяване на бедстващи хора, кораби и самолети; упражнява контрол и организира опазването на морската среда и на р. Дунав от замърсяване от кораби;

- организира и провежда изпити за придобиване на правоспособност от морските лица;
- издава свидетелства за правоспособност на морските лица;
- води регистри на корабите, морските лица, пристанищата и пристанищните оператори в Република България;
- следи за изпълнението на разпоредбите по обезпечаване сигурността на:

  a) корабите, плаващи под българско знаме;

  b) пристанищата в Република България;
- събира и предоставя на министъра на транспорта, информационните технологии и съобщенията информация за изпълнението на изискванията за експлоатационна годност на пристанищата и на обектите по чл. 111а, ал. 1 от Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България (ЗМПВВППРБ);
- прави предложение до министъра на транспорта, информационните технологии и съобщенията за преустановяване на дейността или за ограничаване временно или постоянно на експлоатацията на пристанища, които не отговарят на изискванията на закона или извършват пристанищни услуги в нарушение на чл. 116, ал. 5 ЗМПВВППРБ;
- контролира спазването на изискванията за техническа безопасност на пристанищните съоръжения, за охрана на труда и за безопасно осъществяване на товарно-разтоварни операции;
- определя нивата за сигурност на корабите, плаващи под българско знаме, и на пристанищата в Република България;

  контролира спазването на изискванията за свободен достъп в пристанищата за обществен транспорт;
- прави предложения до министъра на транспорта, информационните технологии и съобщенията за изменяне размера на пристанищните такси;
- подпомага министъра на транспорта, информационните технологии и съобщенията при осъществяване на контрола по изпълнението на концесионните договори, както и на договорите по § 74, ал. 3 от Закона за изменение и допълнение на ЗМПВВППРБ (ДВ, бр. 24 от 2004 г.);
- контролира изпълнението на договорите по чл. 117б, ал. 1 ЗМПВВППРБ;
- подпомага министъра на транспорта, информационните технологии и съобщенията при програмиране на дейности и осъществяване на контрол

на инвестициите при изграждането, реконструкцията и модернизацията на транспортните коридори в областта на водния транспорт (пристанища, морски магистрали, вътрешни водни пътища), финансирани със средства от държавния бюджет или със средства от заеми, гарантирани от държавата;

- подпомага министъра на транспорта, информационните технологии и съобщенията при съгласуването на подробни устройствени планове, с които се отреждат територия и акватория за извършване на строителство на пристанища по чл. 107 - 109 и на обекти по чл. 111а, ал. 1 ЗМПВВППРБ;
- подпомага министъра на транспорта, информационните технологии и съобщенията при съгласуването на документи за отреждане на земни и водни участъци за извършване на строителство по крайбрежието на Черно море и р. Дунав, във вътрешните води и в териториалното море, както и в зоните на действие на средствата за навигационно осигуряване;
- представя на министъра на транспорта, информационните технологии и съобщенията мотивирани становища по инвестиционните инициативи за изграждане на нови или разширение на съществуващи пристанища за обществен транспорт;
- одобрява плановете за приемане и обработване на отпадъци;
- съгласува плановете на пристанищните оператори за действия при бедствия, аварии и катастрофи;
- извършва други функции, възложени й със закон или с акт на Министерския съвет.

Агенцията проучва европейския опит и предлага на управителния съвет на Фонд

"Вътрешни водни пътища" мерки по регулирането на капацитета на флота по вътрешни

водни пътища и осъществява организационно-техническото осигуряване на дейността на

фонда.

Агенцията провежда изпит за професионална компетентност за лицензиране на

превозвачи за извършване превози на товари по вътрешни водни пътища.

Териториалната компетентност на агенцията се разпростира върху:

- вътрешните морски води;

- териториалното море;

- българския участък на р. Дунав;

- сухоземната крайбрежна ивица, имаща широчина 100 метра, отчитана от линията на най-големия отлив; там, където има селища или височина, отстояща на по-малко от 100 метра от линията на най-големия отлив, границите на крайбрежната ивица съвпадат с чертите на селището от страна на морето или с върха на височината;

- сухоземната крайбрежна ивица на разстояние 100 м, мерено от линията, където водната повърхност на р. Дунав пресича сушата на българския участък при най- ниски водни стоежи;

- територията на пристанищата, включително зоните по чл. 103, ал. 6 и обектите по чл. 111а, ал. 1 ЗМПВВППРБ, с изключение на военните пристанища.

Структурата на ИАМА е представена във Фигура 1:

Фигура 1. Структура на ИАМА

2.3. За проекта

Директива 2002/59/ЕО приета от Европейския парламент и Съвет на 27 Юни 2002 година цели създаването в рамките на Общността на информационна система за следене на морския трафик, с цел да увеличи безопасността на морския трафик, подобри реакцията на властите при инциденти, катастрофи или потенциално опасни ситуации в морето, включително операции за търсене и спасяване и да съдейства за по-добро предотвратяване и намиране на замърсяване от корабите. Тази директива изисква от държавите-членки на Европейския съюз и Европейската комисия да си сътрудничат в изграждането на компютъризирани системи за обмен на информация и създаването на необходимата за тази цел инфраструктура.

Прилагането на Директива 2002/59/ЕО, както и клаузите съдържащи се в законодателствата на Европейските страни изискват събирането и разпространяването на различни видове данни. Те засягат следене на корабния трафик, данни за опасни товари, резултати от инспекции на корабите и информация свързана с корабните и товарните отпадъци. SafeSeaNet притежава развита система за обмен на данни с по-добър стандарт и множество механизми за комуникация – от телефон и факс до електронни съобщения. SafeSeaNet допринася за по-ефективното прилагане на Европейското законодателство за безопасност на морския трафик.

В допълнение SafeSeaNet е разработена с цел да осигурява, ако е нужно, достъпа на голям брой потребители до услуги с цел подпомагане на прилагането на политиките на други страни за защита на околната среда, националната сигурност, имиграцията и др.

На 11 март 2009 година Европейският парламент прие трети пакет от Директиви и Регламенти отнасящи се до морското корабоплаване в това число и Директива 2009/17/ЕО на Европейския парламент и на Съвета за изменение на Директива 2002/59/ЕО относно създаване на система на Общността за контрол на движението на корабите и за информация

Директива 2009/17/ЕО допълва Директивата за контрол на трафика с нови изисквания:

- Задължения за информиране във връзка с превоза на опасни товари;
- Компютризиран обмен на данни между държавите-членки – чл.13, в) „посредством SafeSeaNet, при поискване, и ако е необходимо за целите на морската безопасност или сигурност, или за защита на морската среда, държавите-членки трябва да бъдат в състояние незабавно да изпратят на националните и местните компетентни органи на друга

държава-членка информация относно кораба и опасните или замърсяващи товари на борда.”;

- Обмен на информации за рисковите кораби;
- Мерки по отношение на морски инциденти и произшествия;
- Добавя се Член 22a, SafeSeaNet, с което системата се установява като референтна и стандарт за обмен на данни между държавите;

„1. Държавите-членки създават системи за управление на морска информация на национално или местно равнище за обработка на информацията, посочена в настоящата директива.

2. Системите, създадени съгласно параграф 1, трябва да позволяват оперативното използване на събраната информация и изпълняват по-специално условията, посочени в член 14.

3. За да осигурят ефективен обмен на информацията, посочена в настоящата директива, държавите-членки гарантират, че националните или местните системи, създадени за събиране, обработка и съхраняване на информация, могат да бъдат взаимно свързани със SafeSeaNet. Комисията гарантира, че SafeSeaNet работи двадесет и четири часа в денонощието.

4. Без да се засяга параграф 3, когато действат в рамките на вътреобщностни споразумения или в рамките на презгранични, междурегионални или транснационални проекти в рамките на Общността, държавите-членки гарантират, че информационните системи или мрежи съответстват на изискванията на настоящата директива и са съвместими и свързани със "SafeSeaNet""

- Сътрудничество между държавите-членки и Комисията;
- Обработване и управление на информация за морска безопасност;
- Поверителност на информацията;

2.4. Нормативна рамка

Проектът се осъществява в съответствие с изискванията, регламентирани със следните нормативни актове и стратегически документи:

- Директива 2002/59/ЕС относно създаване на система на Общността за контрол на движението на корабите и за информация;
- Директива 2009/17/ЕО за допълване на Директива 2002/59/ЕО относно създаване на система на Общността за контрол на движението на корабите и за информация;

- EMSA SafeSeaNet manual;
- SafeSeaNet XML Messaging Reference Guide;
- SafeSeaNet Network & Security Reference Guide;
- SafeSeaNet Interface Control Document.

3. Цели, обхват и очаквани резултати от изпълнение на проекта

3.1. Общи и специфични цели на проекта

Проектът е насочен към актуализиране и надграждане на националната информационна система SafeSeaNet, в съответствие с новите изисквания на законодателството, промените в структурата на данните, които се обменят и повишените изисквания към интерфейса в съвременните информационни системи.

Постигането на общата цел ще бъде реализирано чрез следните специфични цели, съответстващи на планираните по проекта дейности:

- Хармонизиране на националната информационна система с последните изисквания на европейската система SafeSeaNet
- Улесняване на работата по администрирането на системата
- Подобряване на работата с потребителският интерфейс
- Подобряване на надеждността на хардуера и системния софтуер

3.2. Обхват на проекта

Описаните в т. 3.1 цели се осъществяват с изпълнението на следните основни дейности, които формират обхвата на проекта:

- Дейност 1 Надграждане на информационната система SafeSeaNet
- Дейност 2 Доставка на хардуер и изграждане на работна среда
- Дейност 3 Тестване за приемане и обучение на потребителите
- Дейност 4 Пускане в експлоатация

3.3. Целеви групи

Целевите групи, към които е насочен проектът, обхващат:

- Изпълнителна агенция „Морска администрация“;
- Държавно предприятие „Пристанищна инфраструктура“;
- Ръководство на корабния трафик

3.4. Очаквани резултати

Очакваните резултати от изпълнението на настоящата поръчка са:

- Доставка, инсталиране и конфигуриране на необходимия хардуер и системен софтуер
- Актуализирана национална информационна система SafeSeaNet до последна версия 4 съгласно изискванията на EMSA.
- Актуализиране на интерфейса с Националния център за електронен документооборот в морския транспорт (НЦЕДМТ)
- Преминати успешно тестове за приемане на актуализираната версия на националната система SafeSeaNet в централната система SafeSeaNet
- Актуализирана потребителска и административна документация
- Обучени потребители

3.5. Период на изпълнение

Периодът на изпълнение е 9 (девет) месеца.

Участниците трябва да изготвят подробен график, в който следва да се конкретизират сроковете за изпълнение на всяка дейност и поддейност от настоящата поръчка. Графикът за изпълнение трябва да бъде съобразен с продължителността на дейността и не може да надвишава 10 месеца от дата на сключване на договора.

4. ТЕКУЩО СЪСТОЯНИЕ

Българската част от SafeSeaNet (SSN BG) е тясно интегрирана с автоматизираната идентификационна система (AIS). Получената информация за корабите от AIS (местоположение, скорост, курс и др.) автоматично се получава и изпраща към Европейския сървър. Заедно с това автоматично се изпращат запитвания към европейския сървър за всички кораби, които влизат в обсега на AIS, за наличието на декларирани опасни товари на борда.

SafeSeaNet България има изградени входно-изходни точки и към нея могат да се интегрират външни системи като Системата за управление на трафика, Националният център за електронен документооборот в морският транспорт (Maritime Single Window) и др.

Националната система SafeSeaNet на България е изградена и пусната в експлоатация през ноември 2009 г. Системата е разширена с нови функции, пуснати в действие през март 2011 г.

Към настоящия момент националната система SafeSeaNet генерира следните XML нотификации (MS2SSN) към централния SSN сървър (EIS):

- Ship Notification;
- Alert Notification;
- PortPlus Notification

Тези нотификации са автоматично генерирани на базата на входна информация въведена ръчно от оператор, получена от Националният център за електронен документооборот в морският транспорт (Maritime Single Window) или получена от системата за следене на кораби и системата за автоматично идентифициране (AIS).

Системата генерира следните запитвания (MS2SSN) към централния SSN сървър (EIS) и обработва съответно получените отговори (SSN2MS):

- ShipReq – ShipRes;
- AlertReq – AlertRes;
- ShipCall_Req – ShipCall_Res

Системата получава запитвания (SSN2MS) от централния SSN сървър (EIS) и генерира съответния отговор (MS2SSN):

- ShipReq – ShipRes;
- AlertReq – AlertRes;
- ShipCall_Req – ShipCall_Res

Всички обменяни съобщения отговарят напълно на стандарта дефиниран в „SafeSeaNet XML Messaging Reference Guide - Version 3.05 - 26/10/2016”. Системата е сертифицирана за работа с централния SSN индекс сървър (EIS) и са преминати успешно всички тестове описани в „SSN-Member States Commissioning Test Plan - v.1.95”.

5. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

5.1. Общи изисквания към изпълнението на обществената поръчка

Обществената поръчка се изпълнява в рамките на „Актуализация и надграждане на национална информационна система SafeSeaNet“, финансиран по бюджета на ИА „Морска администрация“. Изпълнителят следва да спазва всички нормативни изисквания по отношение на дейността на Изпълнителна агенция „Морска администрация“ и електронното управление в Република България.

5.2. Общи организационни принципи

Задължително изискване е да се спазят утвърдените хоризонтални и вертикални принципи на организация на изпълнението на предмета на обществената поръчка за гарантирано постигане на желаните резултати от проекта, така че да се покрие пълният набор от компетенции и ноу-хау, необходими за изпълнение на предмета на поръчката, а също така да се гарантира и достатъчно ниво на ангажираност с изпълнението и проблемите на проекта:

- Хоризонталният принцип предполага ангажиране на специалисти от различни звена, така че да се покрие пълният набор от компетенции и ноу-хау по предмета на проекта и същевременно екипът да усвои новите разработки на достатъчно ранен етап, така че да е в състояние пълноценно да ги използва и развива и след приключване на проекта;
- Вертикалният принцип включва участие на експерти и представители на различните управленски нива, така че управленският екип да покрива както експертните области, необходими за правилното и качествено изпълнение на проекта, така и управленски и организационни умения и възможности за осъществяване на политиката във връзка с изпълнението на проекта. Чрез участие на ръководители на звената – ползватели на резултата от проекта, ще се гарантира достатъчно ниво на ангажираност на институцията с проблемите на проекта.

5.3. Управление на проекта

Участниците трябва да предложат методология за управление на проекта, която смятат да приложат, като се изтъкнат ползите й за успешното изпълнение на проекта. Предложената методология трябва да съответства на най-добрите

световни практики и препоръки (например Project Management Body of Knowledge (PMBOK) Guide, PRINCE2, Agile/SCRUM/Kanban, RUP и др. еквивалентни).

Дейностите по управление на проекта трябва да включват като минимум управление на реализацията на всички дейности, посочени в настоящата обществена поръчка, и постигане на очакваните резултати, както и разпределението на предложените участници в екипа за управление на поръчката по роли, график и дейности при изпълнение на настоящата обществена поръчка.

Доброто управление на проекта трябва да осигури:

- координиране на усилията на експертите от страна на Изпълнителя и Възложителя и осигуряване на висока степен на взаимодействие между членовете на проектния екип;
- оптимално използване на ресурсите;
- текущ контрол по изпълнението на проектните дейности;
- разпространяване навреме на необходимата информация до всички участници в проекта;
- идентифициране на промени и осигуряване на техните анализ и координация;
- осигуряване на качеството и полагане на усилия за непрекъснато подобряване на работата за удовлетворяване на изискванията на участниците в проекта.
-

Методологията трябва да включва подробно описание на:

- фазите на проекта;
- организация на изпълнение:
    - структура на екипа на Изпълнителя;
    - начин на взаимодействие между членовете на екипа на Изпълнителя;
    - връзки за взаимодействие с екипа на Възложителя;
- проектна документация:
    - видове доклади;

- техническа и експлоатационна документация;
- време на предаване;
- съдържание на документите;
- управление на версиите;

- управление на качеството;
- график за изпълнение на проекта.

В графика участниците трябва да опишат дейностите и стъпките за тяхното изпълнение максимално детайлно, като покажат логическата връзка между тях. В графика трябва да са посочени датите за предаване на всеки от документите, изготвени в изпълнение на обществената поръчка.

5.4. Управление на риска

В техническото си предложение участниците трябва да опишат подхода за управление на риска, който ще прилагат при изпълнението на поръчката.

Участниците трябва да представят и списък с идентифицираните от Възложителя рискове с оценка на вероятност, въздействие и мерки за реакция.

През времето за изпълнение на проекта Изпълнителят трябва да следи рисковете, да оценява тяхното влияние, да анализира ситуацията и да идентифицира (евентуално) нови рискове.

В хода на изпълнение на поръчката Изпълнителят следва да поддържа актуален списък с рисковете и да докладва състоянието на рисковете най-малко с месечните отчети за напредъка.

При изготвянето на списъка с рискове Участниците следва да вземат предвид следните идентифицирани от Възложителя рискове:

- Промяна в нормативната уредба, водеща до промяна на ключови компоненти на решението – предмет на разработка на настоящата обществена поръчка;
- Недобра комуникация между екипите на Възложителя и Изпълнителя по време на аналитичните етапи на проекта;
- Ненавременно изпълнение на всяко от задълженията от страна на Изпълнителя;

- Неправилно и неефективно разпределяне на ресурсите и отговорностите при изпълнението на договора;
- Забавяне при изпълнение на проектните дейности, опасност от неспазване на срока за изпълнение на настоящата поръчка;
- Грешки при разработване на функционалностите на системата;
- Недостатъчна яснота по правната рамка и/или променяща се правна рамка по време на изпълнение на проекта;
- Липса на задълбоченост при изследването и описанието на бизнес процесите и данните;
- Неинформиране на Възложителя за всички потенциални проблеми, които биха могли да възникнат в хода на изпълнение на дейностите;
- Риск за администриране на системата след изтичане на периода на гаранционна поддръжка.

6. ЕТАПИ НА ИЗПЪЛНЕНИЕ НА ПРОЕКТА

В техническото си предложение участниците трябва да предложат подход за изпълнение на проекта, като включат минимум следните етапи:

6.1. Анализ на данните и изискванията

В началото на изпълнението на етапа Изпълнителят трябва да изготви детайлен график за изпълнение на поръчката, който да съгласува с Възложителя.

Изпълнителят трябва да направи детайлно проучване на изискванията към новите функционалности на системата. Изпълнителят трябва да подготви подробна Спецификация на софтуерните изисквания и Системна архитектура. Детайлното проучване на системните и софтуерни изисквания трябва да обхващат всички компоненти в обхвата на поръчката, свързани с информационната система и нейното внедряване.

Въз основа на анализа и изискванията, Изпълнителят трябва да проектира необходимите промени и доработки в модули и функционалности, както и тяхната конфигурация.

При документирането на изискванията и системната архитектура, е необходимо да се използва структурирано описание и стандартен език за моделиране - UML нотация.
Структурираните изисквания ще бъдат основа за създаване на тестови случаи за приемане на системата.

Етапа ще се смята за приключен след предаването от Изпълнителя на:

- Спецификация на софтуерните изисквания;
- Системна архитектура;

Всички документи разработени в Етап 1 следва да бъдат утвърдени от Възложителя и ще бъдат основа за реализиране на следващите етапи. В срок от 5 работни дни Възложителят ще утвърди документите или ще върне коментари по тях.

6.2. Изготвяне на системен проект

Изпълнителят трябва да изготви системен проект, който подлежи на одобрение от Възложителя. В системния проект трябва да са 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.

6.3. Разработване на софтуерното решение

Етапът на разработка включва изпълнението на следните задачи:

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

За изпълнение на дейностите по разработка на системата участниците в настоящата обществена поръчка трябва да опишат в своите технически предложения приложим подход (методология) за софтуерна разработка, която ще използват, както и инструментите за разработка и средата за провеждане на вътрешните тестове. Участниците трябва да опишат как предложеният от тях подход ще бъде адаптиран за успешната реализация на Системата.

6.4. Тестване

Изпълнителят трябва да проведе тестване на софтуерното решение в създадена за целта тестова среда, за да демонстрира, че изискванията са изпълнени. Изпълнителят трябва да предложи и опише методология за тестване, която ще използва в план за тестване с описание на обхвата на тестването, вид и спецификация на тестовете, управление на дефектите, регресионна политика, инструменти, логистично осигуряване и други параметри на процеса.

6.5. Внедряване

Изпълнителят трябва да внедри софтуерното решение в информационната и комуникационна среда на ИА „Морска администрация“.

Това включва инсталиране, конфигуриране и настройка на програмните компоненти на системата в условията на експлоатационната среда на ИА „Морска администрация“.

6.6. Обучение

Изпълнителят трябва да организира и да проведе обучения за следните групи и ползватели на софтуерното решение:

- Ръководители на корабния трафик
- Служители на спасителните центрове;
- Служители на аварийно спасителна служба
- Администратори на системата.

За провеждането на обученията Изпълнителят е длъжен да осигури за своя сметка:

- Учебни материали;
- Лектори.

6.7. Гаранционна поддръжка

Изпълнителят трябва да осигури за своя сметка гаранционна поддръжка за цялостното и пълно функциониране на системата за период от минимум 36 месеца след приемането и в експлоатация.

При необходимост, по време на гаранционния период трябва да 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 следва да 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 трябва да 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.

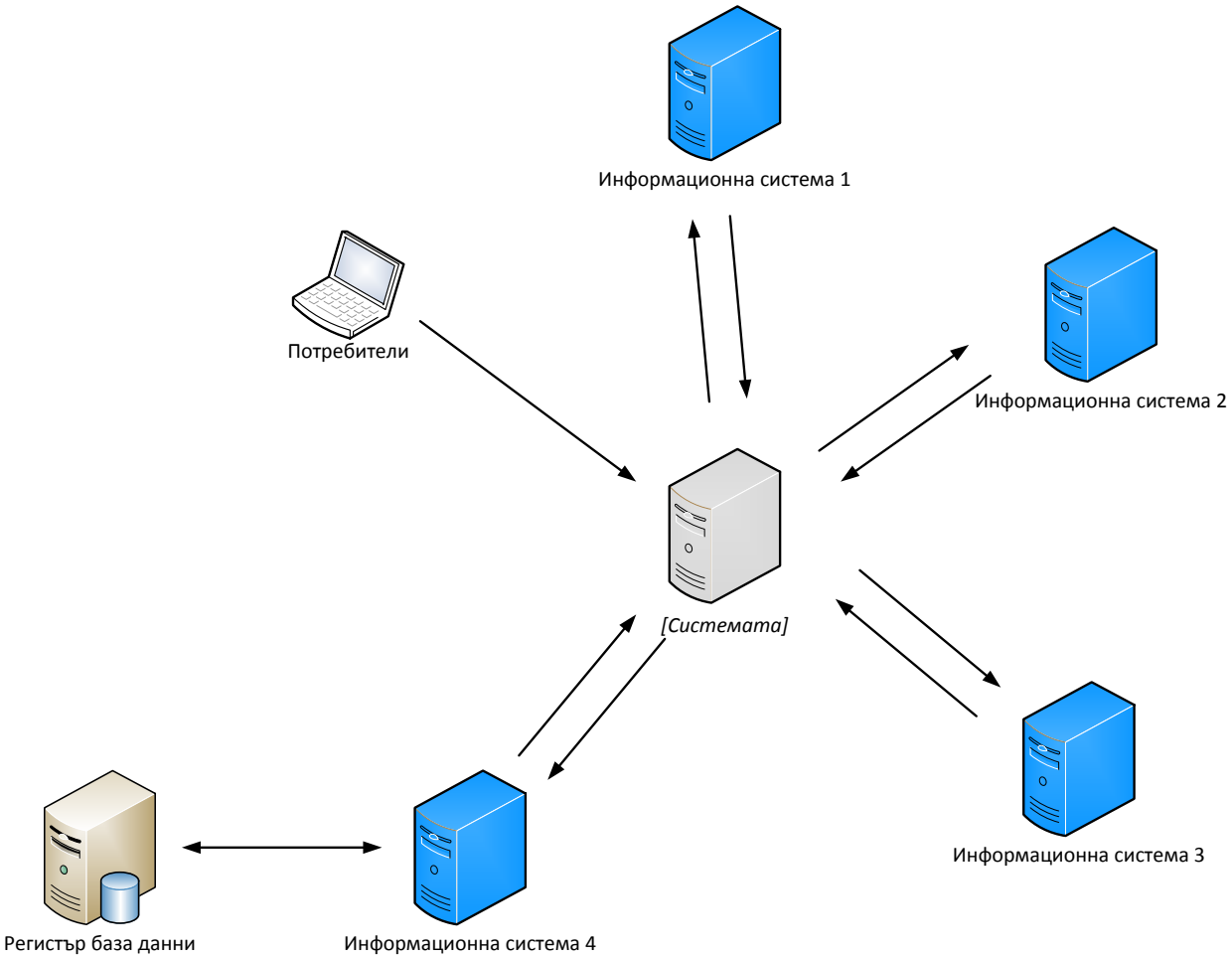
7. ОБЩИ ИЗИСКВАНИЯ ЗА ИНФОРМАЦИОННИ СИСТЕМИ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

7.1. Функционални изисквания към информационната система

7.1.1. Интеграция с външни информационни системи

За реализиране на основни бизнес процеси Системата трябва да поддържа интеграция в реално време с информационни системи на други администрации:

- Националния център за електронен документооборот в морският транспорт – НЦЕДМТ (Maritime Single Window)
- European SafeSeaNet server
- Интеграциите с външни информационни системи и регистри трябва да се реализира чрез стандартен интеграционен слой.



7.1.2. Интеграционен слой

7.1.3. Технически изисквания към интерфейсите

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

▪ Служебните онлайн интерфейси трябва да се предоставят като уеб-услуги (web-services) и да осигуряват 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 трябва да обоснове прогнозирано натоварване на Системата и да предложи критерии за оценка на максимално допустимото време за отговор на машинна заявка. Критерият за оценка следва да се основава на анализ на прогнозираното натоварване и на наличния хардуер, който ще се използва. Изпълнителят трябва да 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;

▪ Всички публични и служебни онлайн интерфейси трябва да бъдат реализирани с поддръжка на режими “push” и „pull”, в асинхронен и синхронен вариант – практическото прилагане на всяка от комбинациите трябва да бъде определено на етап бизнес-анализ и да бъдат съобразени реалните казуси (use cases), които всеки интерфейс обслужва;

▪ Да 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.

7.1.4. Електронна идентификация на потребителите

7.1.5. Отворени данни

▪ Трябва да се разработят процеси по предоставяне на данни в отворен, машинночетим формат заедно със съответните метаданни. Форматите и метаданните следва да съответстват на официалните отворени стандарти.

7.1.6. Формиране на изгледи

Потребителите на Системата трябва да получават разрези на информацията чрез филтриране, пренареждане и агрегиране на данните. Резултатът се представя 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.

7.1.7. Администриране на Системата

Системата трябва да осигурява администриране на потребителите и правата за достъп.

7.2. Нефункционални изисквания към информационната система

7.2.1. Авторски права и изходен код

- Всички компютърни програми, които се разработват за реализиране на Системата, трябва да отговарят на критериите и изискванията за софтуер с отворен код;
- Всички авторски и сродни права върху произведения, обект на закрила на Закона за авторското право и сродните му права, включително, но не само, компютърните програми, техният изходен програмен код, структурата и дизайнът на интерфейсите и базите данни, чието разработване е включено в предмета на поръчката, възникват за Възложителя в пълен обем без ограничения в използването, изменението и разпространението им и представляват произведения, създадени по поръчка на Възложителя съгласно чл. 42, ал. 1 от Закона за авторското право и сродните му права;
- Приложимите и допустими лицензи за софтуер с отворен код са:
  - GPL (General Public License) 3.0
  - LGPL (Lesser General Public License)
  - AGPL (Affero General Public License)
  - Apache License 2.0

- New BSD license
- MIT License
- Mozilla Public License 2.0

▪ Изходният код (Source Code), разработван по проекта, както и цялата техническа документация трябва да бъде 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;

▪ Да 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, да се предпочита този подход пред изграждането на собствено софтуерно решение в цялост, от нулата. Избраният подход трябва да бъде детайлно описан в техническото предложение на участниците;

▪ Да бъде предвидено използването на Система за контрол на версиите и цялата информация за главното копие на хранилището, прието за оригинален и централен източник на съдържанието, да бъде достъпна публично, онлайн, в реално време.

7.2.2. Системна и приложна архитектура

▪ Системата трябва да бъде реализирана като разпределена модулна информационна система. Системата трябва да бъде реализирана със стандартни технологии и да поддържа общоприети комуникационни стандарти, които ще гарантират съвместимост на Системата с бъдещи разработки. Съществуващите модули функционалности трябва да бъдат рефакторирани и/или надградени по начин, който да осигури изпълнението на настоящето изискване;

▪ Бизнес процесите и услугите трябва да бъдат проектирани колкото се може по-независимо с цел по-лесно надграждане, разширяване и обслужване. Системата трябва да е максимално параметризирана и да позволява настройка и промяна на параметрите през служебен (администраторски) потребителски интерфейс;

▪ Трябва да бъде реализирана функционалност за текущ мониторинг, анализ и контрол на изпълнението на бизнес процесите в Системата;

▪ При разработката, тестването и внедряването на Системата Изпълнителят трябва да 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 трябва да бъде реализирана със софтуерна архитектура, ориентирана към услуги - Service Oriented Architecture (SOA);

▪ Взаимодействията между отделните модули в Системата и интеграциите с външни информационни системи трябва да се реализират и опишат под формата на уеб-услуги (Web Services), които да 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 следва да се реализират и опишат приложни програмни интерфейси – Application Programming Interfaces (API). Приложните програмни интерфейси трябва да са достъпни и за интеграция на нови модули и други вътрешни или външни системи;

▪ Приложните програмни интерфейси и информационните обекти задължително да поддържат атрибут за версия;

▪ Версията на програмните интерфейси, представени чрез уеб-услуги, трябва да поддържа версията по един или няколко от следните начини:

- Като част от URL-а
- Като GET параметър
- Като HTTP header (Accept или друг)

▪ За всеки отделен приложен програмен интерфейс трябва да бъде разработен софтуерен комплект за интеграция (SDK) на поне две от популярните развойни платформи (.NET, Java, PHP);

▪ Системата трябва да осигурява възможности за разширяване, резервиране и балансиране на натоварването между множество инстанции на сървъри с еднаква роля;

▪ При разработването на Системата трябва да се предвидят възможни промени, продиктувани от непрекъснато променящата се нормативна, бизнес и технологична среда. Основно изискване се явява необходимостта информационната система да бъде разработена като гъвкава и лесно адаптивна, като отчита законодателни, административни, структурни или организационни промени, водещи до промени в работните процеси;

▪ Изпълнителят трябва да 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 трябва да е сведено до минимум. Бъдещото развитие на

Системата ще се налага във връзка с промени в правната рамка, промени в модела на работа на потребителите, промени във външни системи, интегрирани със Системата, отстраняване на констатирани проблеми, промени в модела на обслужване и др. Такива промени ще се извършват през целия период на експлоатация на Системата, включително и по време на гаранционния период;

▪ Архитектурата на Системата и всички софтуерни компоненти (системни и приложни) трябва да бъдат така подбрани и/или разработени, че да осигуряват работоспособност и отказоустойчивост на Системата, както и недискриминационно инсталиране (без различни условия за инсталиране върху физическа и виртуална среда) и опериране в продуктивен режим, върху виртуална инфраструктура, съответно върху Държавния хибриден частен облак (ДХЧО);

▪ Изпълнителят трябва да проектира, подготви, инсталира и конфигурира като минимум следните среди за Системата: тестова, стейджинг, продуктивна;

▪ Системата трябва да бъде разгърната върху съответните среди (тестова за вътрешни нужди, тестова за външни нужди, стейджинг и продуктивна);

▪ Тестовата среда за външни нужди трябва да 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 трябва да е напълно отделна от останалите среди и нейното използване не трябва 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 прониквания чрез прилагане на подходящи политики за мрежова и информационна сигурност от Възложителя в инфраструктурата на Държавния хибриден частен облак и ЕЕСМ;

▪ В Техническото си предложение участникът трябва да опише добрите практики, които ще прилага по отношение на всеки аспект от системната и приложната архитектура на Системата;

▪ За търсене трябва да се използват системи за пълнотекстово търсене (например Solr, Elastic Search). Не се допуска използването на индекси за пълнотекстово търсене в СУБД;

▪ Трябва да бъде създаден административен интерфейс, чрез който може да бъде извършвана конфигурацията на софтуера;

▪ Всеки обект в системата трябва да има уникален идентификатор;

▪ Записите в регистрите не трябва да подлежат на изтриване или на промяна, а всяко изтриване или промяна трябва да представлява нов запис.

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

Проектът следва максимално да преизползва налични публично достъпни инструменти, библиотеки и платформи с отворен код.

За реализацията на Системата следва да се използват в максимална степен софтуерни библиотеки и продукти с отворен код.

Подход за избор на отворени имплементации и продукти

За реализацията на дадена техническа функционалност обикновено съществуват множество отворени алтернативни проекти, които могат да се използват в настоящата Система. Участникът следва да представи базов списък със свободните компоненти и средства, които възнамерява да използва. Отворените проекти трябва да 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.

Препоръчително е преизползването на проекти, финансирани със средства на Европейския съюз, както и на такива, в които Участникът има активни разработчици. Използването на closed source и на инструменти, библиотеки, продукти и системи с платен лиценз става за сметка на Изпълнителя, като е допустимо в случаите, когато липсва подходяща свободна алтернатива с необходимата функционалност или тя не отговаря на горните условия.

Изпълнителят 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.

Подход за работа с външните софтуерни ресурси

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

Когато се налага промяна в изходния код на използван софтуерен компонент, промените трябва да се извършват във fork хранилището на governmentbg в съответствие с изискванията на основния проект. Изпълнителят трябва да 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 трябва да бъдат извършвани по време на целия проект.

При установяване на наличие на нови версии на използваните проекти 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 се извлича и използва след успешното изпълнение на интеграционните тестове.

7.2.4. Изграждане и поддръжка на множество среди

Изпълнителят трябва да изгради и да поддържа минимум следните логически разделени среди:

Среда	Описание
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 трябва да става чрез автоматизирана система за провизиране и разгръщане на системните компоненти. При необходимост от страна на Възложителя Изпълнителят трябва да съдейства за изграждането на нови системни среди.
Участникът може да предложи изграждането на допълнителни среди според спецификите на предложеното решение.

7.2.5. Процес на разработка, тестване и разгръщане

Процесите, свързани с развитието на Системата, трябва да 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. По този начин гражданите биха могли да съдействат в процесите по развитие и тестване на разработките през целия им жизнен цикъл.

Всички софтуерни приложения, системи, подсистеми, библиотеки и компоненти, които са необходими за реализацията на Системата, трябва да бъдат разработвани като софтуер с отворен код и да бъдат достъпни в публично хранилище. Към настоящия момент следва да се използва общото хранилище за проекти с отворен код, финансирани с публични средства в България (към момента https://github.com/governmentbg).

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.

Трябва да се анализират възможностите за включване на граждани в процесите по разработка, тестване и идентифициране на пропуски на софтуера.

Участникът трябва да предложи механизъм и процедури за реализирането на такива процеси.

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

- Документиране на Системата в изходния код, минимум на ниво процедура/функция/клас;
- Покритие на минимум 50% от изходния код с функционални тестове *[в случай на надграждане на съществуваща система – 50% от новата функционалност и 20% от съществуващата]*;
- Използване на continuous integration практики;
- Използване на dependency management.

Участникът трябва да опише детайлно подхода си за покриване на изискванията.

Във всеки един компонент на Системата, който се build-ва и подготвя за инсталация (deployment), е необходимо 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.

7.2.6. Бързодействие и мащабируемост

7.2.6.1 Контрол на натоварването и защита от DoS/DDoS атаки

▪ Системата трябва да поддържа на приложно ниво "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, достъпни публично или служебно като уеб-услуги (Web Services) и служебни интерфейси.

▪ Системата трябва да поддържа възможност за конфигуриране на различни лимити за конкретни автентикирани потребители (напр. системи на други администрации) и трябва да предоставя възможност за генериране на справки и статистики за броя заявки по ресурси и услуги.

7.2.6.2 Кохерентно кеширане на данни и заявки

7.2.6.3 Бързодействие

▪ При визуализация на уеб-страници системите трябва да осигуряват висока производителност и минимално време за отговор на заявки - средното време за заявка трябва да 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 *[В случай че функционалните изисквания предвиждат визуализация на справки или сложни електронни документи, изискването се адаптира, като се съобразява спецификата на функционалността].*

▪ Трябва да бъдат създадени тестове за натоварване.

7.2.6.4 Използване на HTTP/2

С оглед намаляване на служебния трафик, времената за отговор и натоварването на сървърите следва да 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.);

▪ 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.

7.2.6.5 Подписване на документи -

7.2.6.6 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.

7.2.7. Информационна сигурност и интегритет на данните

▪ Не се допуска съхранението на пароли на администратори, на вътрешни и външни потребители и на акаунти за достъп на системи (ако такива се използват) в явен вид. Всички пароли трябва да бъдат защитени с подходящи сигурни алгоритми (напр. BCrypt, PBKDF2, scrypt (RFC 7914) за съхранение на пароли и където е възможно, да се използва и прозрачно криптиране на данните в СУБД със сертификати (transparent data-at-rest encryption);

▪ Да бъде предвидена система за ежедневно създаване на резервни копия на данните, които да се съхраняват извън инфраструктурата на системата;

▪ Всички уебстраници (вътрешни и публично достъпни в Интернет) трябва да бъдат достъпни единствено и само през протокол HTTPS. Криптирането трябва да се базира на сигурен сертификат с валидирана идентичност (Verified Identity), позволяващ задължително прилагане на TLS 1.2, който е издаден от удостоверителен орган, разпознаван от най-често използваните браузъри (Microsoft Internet Explorer, Google Chorme, Mozilla Firefox). Ежегодното преиздаване и подновяване на сертификата трябва да бъде включено като разходи и дейности в гаранционната поддръжка за целия срок на поддръжката;

▪ Трябва да бъдат извършени тестове за сигурност на всички уебстраници, като минимум чрез автоматизираните средства на SSL Labs за изпитване на сървърна сигурност (https://www.ssllabs.com/ssltest/). За нуждите на автентикация с КЕП трябва да се предвиди имплементирането на обратен прокси сървър (Reverse Proxy) с балансиране на натоварването, който да препраща клиентските сертификати към вътрешните приложни сървъри с нестандартно поле (дефинирано в процеса на разработка на Системата) в HTTP Header-а. Схемата за проксиране на заявките трябва да бъде защитена от Spoofing;

▪ Като временна мярка за съвместимост настройките на уебсървърите и Reverse Proxy сървърите трябва да бъдат балансирани така, че Системата да позволява използване и на клиентски браузъри, поддържащи по-стария протокол TLS 1.1. Това изключение от общите изисквания за информационна

сигурност не се прилага за достъпа на служебни потребители от държавната администрация и доставчици на обществени услуги, които имат служебен достъп до ресурси на Системата;

▪ При разгръщането на всички уебуслуги (Web Services) трябва да се използва единствено протокол HTTPS със задължително прилагане на минимум TLS 1.2;

▪ Програмният код трябва да включва методи за автоматична санитизация на въвежданите данни и потребителски действия за защита от злонамерени атаки, като минимум SQL инжекции, XSS атаки и други познати методи за атаки, и да отговаря, където е необходимо, на Наредбата за оперативна съвместимост и информационна сигурност;

▪ При проектирането и разработката на компонентите на Системата и при подготовката и разгръщането на средите трябва да се спазват последните актуални препоръки на OWASP (Open Web Application Security Project);

▪ Трябва да бъде изграден модул за проследимост на действия и събития в Системата. За всяко действие (добавяне, изтриване, модификация, четене) трябва да съдържа следните атрибути:

- Уникален номер;
- Точно време на възникване на събитието;
- Вид (номенклатура от идентификатори за вид събитие);
- Данни за информационна система, където е възникнало събитието;
- Име или идентификатор на компонент в информационната система, регистрирал събитието;
- Приоритет;
- Описание на събитието;
- Данни за събитието.

▪ Астрономическото време за удостоверяване настъпването на факти с правно или техническо значение се отчита с точност до година, дата, час, минута, секунда и при технологична необходимост - милисекунда, изписани в съответствие със стандарта БДС ISO 8601:2006;

▪ Астрономическото време за удостоверяване настъпването на факти с правно значение и на такива, за които се изисква противопоставимост, трябва да бъде удостоверявано с електронен времеви печат по смисъла на Глава III, Раздел 6 от Регламент ЕС 910/2014. Трябва да бъде реализирана

функционалност за получаване на точно астрономическо време, отговарящо на горните условия, и от доставчик на доверителни услуги или от държавен орган, осигуряващ такава услуга, отговаряща на изискванията на RFC 3161;

▪ Трябва да бъдат проведени тестове за проникване (penetration tests), с които да се идентифицират и коригират слаби места в сигурността на Системата.

7.2.8. Използваемост

7.2.8.1 Общи изисквания за използваемост и достъпност

▪ При проектирането и разработката на софтуерните компоненти и потребителските интерфейси трябва да се спазват стандартите за достъпност на потребителския интерфейс за хора с увреждания WCAG 2.0, съответстващ на ISO/IEC 40500:2012;

▪ Всички ресурси трябва да са достъпни чрез GET заявка на уникален адрес (URL). Не се допуска използване на POST за достигане до формуляр за подаване не заявление, за генериране на справка и други;

▪ Функционалностите на потребителския интерфейс на Системата трябва да бъдат независими от използваните от потребителите интернет браузъри и устройства, при условие че последните са версии в период на поддръжка от съответните производители. Трябва да бъде осигурена възможност за ползване на публичните модули на приложимите услуги през мобилни устройства – таблети и смарт-телефони, чрез оптимизация на потребителските интерфейси за мобилни устройства (Responsive Design);

▪ Не се допуска използване на Капча (Captcha) като механизъм за ограничаване на достъпа до документи и/или услуги. Алтернативно, Системата трябва да поддържа "Rate Limiting" и/или "Throttling" съгласно изискванията в т. ***7.1.1.*** от настоящите изисквания. Допуска се използването на Captcha единствено при иденетифицирани много последователни опити от предполагаем „бот“;

▪ Трябва да бъде осигурен бърз и лесен достъп до електронните услуги и те да бъдат промотирани с подходящи навигационни елементи на публичната интернет страница – банери, елементи от главното меню и др.;

▪ Публичните уеб страници на Системата трябва да бъдат проектирани и оптимизирани за ефективно и бързо индексиране от търсещи машини с цел популяризиране сред потребителите и по-добра откриваемост при търсене по ключови думи и фрази. При разработката на страниците и при изготвяне на автоматизираните процедури за разгръщане на нова версия на Системата

трябва да се използват инструменти за минимизиране и оптимизация на размера на изходния код (HTML, JavaScript и пр.) с оглед намаляване обема на файловете и по-бързо зареждане на страниците;

▪ При разработката на публични уеббазирани страници трябва да се използват и да се реализира поддръжка на:

- Стандартните семантични елементи на HTML5 (HTML Semantic Elements);
- JSON-LD 1.0 (http://www.w3.org/TR/json-ld/);
- Open Graph Protocol (http://ogp.me) за осигуряване на поддръжка за качествено споделяне на ресурси в социални мрежи и мобилни приложения;

▪ В екранните форми на Системата трябва да се използват потребителски бутони с унифициран размер и лесни за разбиране текстове в еднакъв стил.

▪ Всички текстови елементи от потребителския интерфейс трябва да бъдат визуализирани с шрифтове, които са подходящи за изобразяване на екран и които осигуряват максимална съвместимост и еднакво възпроизвеждане под различни клиентски операционни системи и браузъри. Не се допуска използването на серифни шрифтове (Serif).

▪ Полета, опции от менюта и командни бутони, които не са разрешени конкретно за ролята на влезлия в системата потребител, не трябва да са достъпни за този потребител. Това не отменя необходимостта от ограничаване на достъпа до бизнес логиката на приложението чрез декларативен или програмен подход.

▪ Всяка екранна форма трябва да има наименование, което да се изписва в горната част на екранната форма. Наименованията трябва да подсказват на потребителя какво е предназначението на формата.

▪ Всички търсения трябва да са нечувствителни към малки и главни букви.

▪ Полетата за пароли трябва задължително да различават малки и главни букви.

▪ Полетата за потребителски имена трябва да позволяват използване на имейл адреси като потребителско име, включително да допускат всички символи, регламентирани в RFC 1123, за наименуването на хостове;

▪ Главните и малките букви на въвежданите данни се запазват непроменени, не се допуска Системата да променя капитализацията на данните, въвеждани от потребителите.

▪ Системата трябва да позволява въвеждане на данни, съдържащи както български, така и символи на официалните езици на ЕС.

▪ Наименованията на полетата следва да са достатъчно описателни, като максимално се доближават до характера на съдържащите се в тях данни.

▪ Системата трябва да поддържа прекъсване на потребителски сесии при липса на активност. Времето трябва да може да се променя от администратора на системата без промяна в изходния код. Настройките за време за прекъсване на неактивни сесии трябва да включват и възможността администраторите да дефинират стилизирана страница с информативно съобщение, към която Системата да пренасочва автоматично браузърите на потребителите в случай на прекъсната сесия;

▪ Дългите списъци с резултати трябва да се разделят на номерирани страници с подходящи навигационни елементи за преминаване към предишна, следваща, първа и последна страница, към конкретна страница. Навигационните елементи трябва да са логически обособени и свързани със съответния списък и да се визуализират в началото и в края на HTML контейнера, съдържащ списъка;

▪ За големите йерархически категоризации трябва да се предвиди възможност за навигация по нива или чрез отложено зареждане (lazy load).

7.2.8.2 Интернационализация

▪ Системата трябва да може да съхранява и едновременно да визуализира данни и съдържание, което е въведено/генерирано на различни езици;

▪ Всички софтуерни компоненти на Системата, използваните софтуерни библиотеки и развойни комплекти, приложните сървъри и сървърите за управление на бази данни, елементите от потребителския интерфейс, програмно-приложните интерфейси, уебуслугите и др. трябва да поддържат стандартно и да са конфигурирани изрично за спазване на минимум Unicode 5.2 стандарт при съхранението и обработката на текстови данни, съответно трябва да се използва само UTF-8 кодиране на текстовите данни.

▪ Версиите на съдържанието на съответните езици трябва да включват всички текстове, които се визуализират във всички елементи на потребителския интерфейс, справките, генерираните от системата електронни документи, съобщения, нотификации, имейл съобщения, номенклатурите и таксономиите и др. Данните, които се съхраняват в Системата само на български език, се изписват/визуализират на български език;

▪ При визуализация на числа трябва да се използва разделител за хиляди (интервал).

▪ При визуализация на дати и точно време в елементи от потребителския интерфейс в генерирани справки или в електронни документи всички формати за дата и час трябва да са съобразени с избрания от потребителя език/локация в настройките на неговия профил:

- За България стандартният формат е „DD.MM.YYYY HH:MM:SS”, като наличието на време към датата е в зависимост от вида на визуализираната информация и бизнес-смисъла от показването на точно време;
- Системата трябва да поддържа и всички формати съгласно ISO БДС 8601:2006;

7.2.8.3 Изисквания за използваемост на потребителския интерфейс

▪ Електронните форми за подаване на заявления и за обявяване на обстоятелства трябва да бъдат реализирани с AJAX или с аналогична технология, като по този начин се гарантират следните функционалности:

- Контекстна валидация на въвежданите данни на ниво "поле" от форма и контекстни съобщения за грешка/невалидни данни в реално време;
- Възможност за избор на стойности от номенклатури чрез търсене в списък по част от дума (autocomplete) и визуализиране на записи, отговарящи на въведеното до момента, без да е необходимо пълните номенклатури да са заредени в браузъра на клиента и потребителят да скорлира дълги списъци с повече от 10 стойности;

▪ В електронните форми трябва да бъде реализирана валидация на въвежданите от потребителите данни на ниво "поле" (in-line validation). Валидацията трябва да се извършва в реално време на сървъра, като при успешна валидация данните от съответното поле следва да бъдат запазени от сървъра;

▪ Системата трябва да гарантира, че въведените, валидираните и запазените от сървъра данни остават достъпни за потребителите дори за процеси, които не са приключили, така че при волно, неволно или автоматично прекъсване на потребителската сесия поради изтичане на периода за допустима липса на активност потребителят да може да продължи съответния

процес след повторно влизане в системата, без да загуби въведените до момента данни и прикачените до момента електронни документи;

▪ Трябва да бъде реализирана възможност за добавяне и редактиране от страна на администраторите на Системата, без да са необходими промени в изходния код, на контекстна помощна информация за:

- всяка електронна форма или стъпка от процес, за която има отделен екран/форма;
- всяка група полета за въвеждане на данни (в случаите, в които определени полета от формата са групирани тематично);
- всяко отделно поле за въвеждане на данни;

▪ Трябва да бъде разработена контекстна помощна информация за всички процеси, екрани и електронни форми, включително ясни указания за попълване и разяснения за особеностите при попълване на различните групи полета или на отделни полета;

▪ Контекстната помощна информация, указанията към потребителите и информативните текстове за всяка електронна административна услуга не трябва да съдържат акроними, имена и референции към нормативни документи, които са въведени като обикновен текст (plain-text). Всички акроними, референции към нормативни документи, формуляри, изисквания и др. трябва да бъдат разработени като хипервръзки към съответните актуални версии на нормативни документи и/или към съответния речник/списък с акроними и термини;

▪ Достъпът на потребителя до контекстната помощна информация трябва да бъде реализиран по унифициран и консистентен начин чрез подходящи навигационни елементи, като например чрез подходящо разположени микро-бутони с икони, разположени до/пред/след етикета на съответния елемент, за който се отнася контекстната помощ, или чрез обработка на "Mouse Hover/Mouse Over" събития;

▪ При проектирането и реализацията на потребителския интерфейс трябва да се отчете, че той трябва да бъде еднакво използваем и от мобилни устройства (напр. таблети), които не разполагат с мишка, но имат чувствителни на допир екрани.

▪ Потребителският интерфейс следва да бъде достъпен за хора с увреждания съгласно изискванията на чл. 48, ал. 5 от ЗОП.

7.2.8.4 Изисквания за използваемост в случаи на прекъснати бизнес процеси

▪ Системата трябва да съхранява перманентно всеки започнал процес/процедура по подаване на заявление или обявяване на обстоятелства, текущия му статус и всички въведени данни и прикачени документи дори ако потребителят е прекъснал волно или неволно потребителската си сесия;

▪ При вход в системата потребителят трябва да получава прегледна и ясна нотификация, че има започнати, но недовършени/неизпратени/неподписани заявления, и да бъде подканен да отвори модула за преглед на историята на транзакциите;

▪ Модулът за преглед на историята на транзакциите трябва да поддържа следните функционалности:

- Да визуализира списък с историята на подадените заявления, като минимум със следните колони – дата, входящ номер, код на тупа формуляр, подател (име на потребител и имена на физическото лице - подател), статус на заявлението;
- Да предлага видни и лесни за използване от потребителите контроли/инструменти:
  - за филтриране на списъка (от дата до дата, за предефинирани периоди, като "последния един месец", "последната една година";
  - сортиране на списъка по всяка от колоните, без това да премахва текущия филтър;
  - свободно търсене по ключови думи по всички колони в списъка и метаданните на прикачените/свързаните документи със заявленията, което да води до динамично филтриране на списъка.

7.2.8.5 Изисквания за проактивно информиране на потребителите

7.2.9. Системен журнал

Изграждането решение задължително трябва да осигурява проследимост на действията на всеки потребител (одит), както и версия на предишното състояние на данните, които той е променил в резултат на своите действия (системен журнал).

Атрибутите, които трябва да се запазват при всеки запис, трябва да включват като минимум следните данни:

▪ дата/час на действието;

- модул на системата, в който се извършва действието;
- действие;
- обект, над който е извършено действието;
- допълнителна информация;
- IP адрес и браузър на потребителя.

Размерът на журнала на потребителските действия нараства по време на работа на всяка система, което налага по-различното му третиране от гледна точка на организация на базата данни:

- по време на работа на Системата потребителският журнал трябва да се записва в специализиран компонент, който поддържа много бързо добавяне на записи; този подход се налага, за да не се забавя излишно работата на Системата;
- специална фонова задача трябва да акумулира записаните данни и да ги организира в отделна специално предвидена за целта база данни, отделна от работната база данни на Системата;
- данните в специализираната база данни трябва да се архивират и изчистват, като в специализираната база данни трябва да бъде достъпна информация за не повече от 2 месеца назад; при необходимост от информация за предишен период администраторът на Системата трябва първо да възстанови архивните данни;
- трябва да бъде предоставен достъп до системния журнал на органите на реда чрез потребителски или програмен интерфейс; за достъпа трябва да се изисква електронна идентификация.

7.2.10. Дизайн на бази данни и взаимодействие с тях

При използване на база данни (релационна или нерелационна(NoSQL) следва да бъдат следвани добрите практики за дизайн и взаимоедйствие с базата данни, в т.ч.:

- дизайнът на схемата на базата данни (ако има такава) трябва да бъде с максимално ниво на нормализация, освен ако това не би навредило сериозно на производителността;
- базата данни трябва да може да оперира в клъстър; в определени случаи следва да бъде използван т.нар. sharding;
- имената на таблиците и колоните трябва да следват унифицирана конвенция;

▪ трябва да бъдат създадени индекси по определени колони, така че да се оптимизират най-често използваните заявки; създаването на индекс трябва да е мотивирано и подкрепено със замервания;

▪ връзките между таблици трябва да са дефинирани чрез foreign key;

▪ периодично трябва да бъде правен анализ на заявките, включително чрез EXPLAIN (при SQL бази данни), и да бъдат предприети мерки за оптимизиране на бавните такива;

▪ задължително трябва да се използват транзакции, като нивото на изолация трябва да бъде мотивирано в предадената документация;

▪ при операции върху много записи (batch) следва да се избягват дългопродължаващи транзакции;

▪ заявките трябва да бъдат ограничени в броя записи, които връщат;

▪ при използване на ORM или на друг слой на абстракция между приложението и базата данни, трябва да се минимизира броят на излишните заявки (т.нар. n+1 selects проблем);

▪ при използване на нерелационна база данни трябва да се използват по-бързи и компактни протоколи за комуникация, ако такива са достъпни.

8. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ДЕЙНОСТИТЕ ПО ПРОЕКТА

8.1. Дейност 1 Надграждане и актуализация на информационната система SafeSeaNet

8.1.1. Описание на дейността

В тази дейност Изпълнителя с помощта на Възложителя и други участници в проекта, трябва да направи преглед на настоящата ситуация и на функционалните и интеграционните изисквания, които трябва да се изпълнят. Това включва разработка на нови и надграждане и усъвършенстване на съществуващите функционалности, разработка и промяна на интерфейс за въвеждане на потребителски данни, интерфейс за визуализиране на информация и интерфейс за интегриране.

8.1.2. Изисквания към изпълнение на дейността

8.1.2.1. Докладване на инциденти

За изпълнение на задълженията си спрямо изискванията на директива 2002/59/ЕС, България е длъжна да изпраща данни за инциденти случили се в нейната зона за докладване. Типовете инциденти са следните:

- инциденти свързани с безопасността на кораба съгласно с член 16.1.a и както е описано в членове 17.1.a и 17.1.b (SITREP)
- инциденти свързани със замърсяване на водите и бреговата ивица на държава на ЕС или докладване на кораби за които има доказателства за умишлено изхвърляне на замърсители съгласно член 16.1.b (POLREP)
- доклади за дрейфуващи контейнери или пакети съгласно член 17.1.d (Lost and Found objects)
- доклади за кораби неизпълняващи изискванията за известяване и докладване съгласно член 16.1.a (Failed notification)
- доклади за кораби неизпълняващи правилата дефинирани от системите за навигация и следене на корабите (VTS) съгласно член 16.1.a (VTS rules infringement)
- доклади за кораби, на които им е отказан достъп до пристанища съгласно анекс I-1 от директива 95/21/ЕС от 19 юни 1995 както е описано в член 16.1.c (Banned ship)
- доклади за кораби, които не известили за наличието или липсата на застрахователен сертификат или финансова гаранция съгласно член 16.1.d (Insurance failure)
- доклади за кораби, за които пилотите или управителите на пристанището са докладвали за наличие на проблеми, които могат да доведат до замърсяване или опасност за корабоплаването съгласно член 16.1.e (Pilot or port)
- информация за кораби, които не са предали генерираните отпадъци и остатъци от товара съгласно член 12.3 от директива 2000/59/ЕС (Waste)

За изпълнение на изискванията на директивата за докладване на инциденти трябва да се реализира функционалността за изпращане на нотификации и запитвания за инциденти описана в последната версия на SafeSeaNet XML Messaging Reference Guide.

8.1.2.2. Освобождаване от задължения

Страните членки на ЕС могат да освободят определени кораби от задължението да докладват следната информация:

- Известяване преди пристигане съгласно член 4 от директива 2002/59/ЕС

- Известяване за опасни товари съгласно член 13 от директива 2002/59/ЕС
- Данни свързани със сигурността съгласно член 6 от регулация (ЕС) 725/2004
- Известяване, плащане на такса или предаване на отпадъци и остатъци от товари – едно или комбинация от 3-те съгласно член 6 от директива 2010/65/EU

Освобождаването от задължения за докладване се прилагат по отношение на един кораб. Може да съществуват множество изключения от един тип за един кораб например за различни пътувания или от различен тип за едно пътуване.

За изпълнение на изискванията на директивата за докладване на инциденти трябва да се реализира функционалността за изпращане на информация за инциденти, получаване на информация за инциденти чрез заявка и др. описани в последната версия на SafeSeaNet XML Messaging Reference Guide.

8.1.2.3. Интеграция с Централна база данни с местоположения и терминали (CLD)

Central Location Database (CLD) поддържа всички LOCODE-ове от UN/LOCODE списъка, специфични за SSN локации (SSN Specific locations) както и информация за пристанищни терминали (port facilities) поддържана от IMO Maritime Security модула на системата Global Integrated Shipping Information System (GISIS).

CLD предоставя информация към външни системи с цел унифицирането на тази информация съхранявана в техните бази от данни. За достъп до информацията в CLD системата предлага автоматичен интерфейс за обмен на данни тип система-система чрез SOAP web услуги.

Начините за автоматичен обмен на данни са:

- Запитване/Отговор: външните системи изпращат запитване към CLD за данните на определени LOCODE-ове според различни критерии за търсене напр. държава или наименование. Този механизъм също може да се използва за намиране на историята на промените за определен LOCODE
- Известяване за данни за местоположение: този механизъм позволява CLD да известява за добавяне на нови данни или за промени в данните

за LOCODE всички заинтересувани лица и външни системи, които са се абонирали за това

За изпълнение на изискванията за интеграция е необходимо да се реализират функциите за интеграция с CLD описани в Central Location Database (CLD) System Interface Guide.

8.1.2.4. Актуализиране на националната система SafeSeaNet до версия 4

След измененията в директива 2000/59/ЕС Анекс I се въвеждат промени в информацията, която се докладва от корабите пристигащи и напускащи пристанища на ЕС. Промените включват:

- Добавяне на изискване за докладване информация за бункери
- Изменения в данните за опасните товари (HAZMAT)
- Изменение в механизма за докладване на отпадъците и остатъците от товар (Waste)
- Добавяне на данни за местонахождение на Пристанищно съоръжение
- Премахване на PortPlus v2 нотификации, Ship MRS v2 нотификации и Alert съобщения

За реализацията на тези промени е необходимо да се промени съществуващата функционалност за изпращане на нотификации, изпращане на запитвания и получаване на отговор и изпращане на отговори на получени запитвания съгласно последната версия на SafeSeaNet XML Messaging Reference Guide.

При преминаване към версия 4 на SafeSeaNet трябва да се актуализира интерфейса за обмен на данни с Националния център за електронен документооборот в морският транспорт – НЦЕДМТ (Maritime Single Window).

8.1.1. Очаквани резултати

Националната информационна система SafeSeaNet е актуализирана и инсталирана в тестова среда на Възложителя.

8.2. Дейност 2 Доставка на хардуер и изграждане на работна среда

8.2.1. Описание на дейността

Дейността включва доставка, инсталация и пускане в експлоатация на ИТ инфраструктура.

8.2.2. Изисквания към изпълнение на дейността

1.	**Блейд шаси – 1 бр.**
1.1.	Да се достави и монтира блейд шаси. Блейд шасито да отговаря на следните минимални технически изисквания:
1.2.	Да бъде монтирано в шкаф (rackmounted)
1.3.	Да разполага с достатъчно брой слотове за инсталиране на доставените блейд сървъри;
1.4.	Да включва в конфигурацията си резервирани захранвания (N+1) и вентилатори (N+1), които да могат да бъдат заменяни без спиране на оборудването;
1.5.	Да включва в конфигурацията си резервиран модул за осигуряване на управление и наблюдение на системата и софтуер за управление и диагностика на всички компоненти;
1.6.	Да се осигури мин. 10 Gb мрежова свързаност към локалната мрежа възможност за добавяне на свързване по16 Gb/s към SAN мрежат, чрез добавяне на SFP, посредством минимум два броя резервирани конвергирани мрежови модули. Всеки конвергиран мрежови модул да позволява обслужване на блейд сървърите при максимално запълване на шасито чрез осигуряване на необходимия брой downlink портове за свързаност със скорост мин. 2 x 20 Gb. Поддържани протоколи: минимум Ethernet, iSCSI и FCoE. Всеки конвергиран модул да разполага с мин. 4 бр. 10Gb SR SFP+ модули и необходимите оптични кабели за свързаност към локалната мрежа. Към всеки конвергиран модул да могат да се добавят мин. 4 бр. 16 Gb SFP+ модули и необходимите оптични кабели за свързаност към SAN мрежата;
1.7.	Блейдовете да се инсталират в шасита, които да могат да се свързват с други шасита, образувайки един логически клъстър.

1.8.	Шасито да е не по-голямо от 8U
1.9.	Гаранционна поддръжка – минимум 36 месеца хардуерна поддръжка от производителя
2.	**Сървъри за приложения – 6 бр. (2 за бази данни, 2 за приложение, 1 тестови, 1 за обезпечаване на архив)**
2.1.	Всеки сървър да отговаря на следните минимални технически изисквания:
2.2.	Blade архитектура Пълна съвместимост за работа с доставеното блейд шаси. Размерът на системата (form-factor) да позволява инсталация на всички сървъри в едно шаси
2.3.	Да бъде доставен с минимум 1 брой процесор на сървър Intel Xeon, поне 2.1 GHz, 8 ядра/16 нишки, 11M кеш, DDR4-2400 или еквивалентен
2.4.	Да бъде доставен с минимум 32GB оперативна памет
2.5.	Да бъде доставен с минимум 2 x 240GB Flash диска или карти конфигурирани в RAID 1.Възможност за разширяване с още 2 x HDD във всеки един от сървърите
2.6.	Конвергиран мрежови адаптер, осигуряващ минимум 2 порта 20 Gb Ethernet със следните характеристики: - Обединение на мрежи за данни и мрежи за съхранение на данни -Сегментиране на мрежовите адаптери, Ethernet NIC и/или FC HBA -поддръжка на Fibre Channel over Ethernet Конвергираният мрежови адаптер да е напълно съвместим за работа с конвергираните мрежови модули, осигуряващи свързаността с блейд шасито. Осигуряване на работа в режим boot през SAN;
2.7.	Flash модул за инсталиране на хипервайзор за виртуализация на ресурсите;
2.8.	Гаранционна поддръжка – минимум 36 месеца хардуерна поддръжка от производителя, минимум 36 месеца софтуерна поддръжка от производителя, покритие 24 x 7, време за реакция – до 4 часа, време за отстраняване на проблема – до 24 часа,

	обслужване на място. Срокът на гаранционната поддръжка започва да тече от подписване на приемо-предавателен протокол за доставка и монтаж.
3.	**Непрекъсваемо токозахранване**
	On-line, способно да обезпечи мин. 15 минути работоспособност на оборудването
4.	**6 x Windows Server 2016 Standard Edition, 16 Cores**

8.2.3. Очаквани резултати

Инсталирана и конфигурирана хардуерна инфраструктура.

8.3. Дейност 3 Тестване за приемане и обучение на потребителите

8.3.1. Описание на дейността

В тази дейност Изпълнителят трябва да извърши Тест за приемане (Commissioning Test) на разработените промени в системата да се удостовери готовността ѝ за работа в продукционната среда на EMSA.

При планиране на изпълнението на дейността Изпълнителят трябва да вземе впредвид техническото време за обработка на тестовите резултати от EMSA описани в документа Member State Commissioning Plan.

В случай че Изпълнителят има определени изисквания към квалификацията и образованието на специалистите, които ще бъдат обучавани, той е длъжен да уведоми за това Възложителя, писмено, в срок от 40 (дни) преди започването на Дейност 3. Възложителят предоставя на Изпълнителя списък на лицата, които следва да бъдат обучени за работа със Софтуерните продукти в срок от 10 (десет) дни от получаване на изискванията на Изпълнителя или изтичане на срока по предходното изречение. Възложителят може да заменя специалисти от предоставения списък, не по късно от 3 (дни) дни преди започването на обучението.

Изпълнителят е длъжен да приключи обучението на специалистите на Възложителя според предложения подробен план график за обучение от Изпълнителя. Времето, графикът и мястото за обучение се съгласуват писмено

между Страните, като Изпълнителят осигурява присъствие на обучаващи за договорените в графика период и часове.

8.3.2. Изисквания към изпълнение на дейността

Изисквания за теста за приемане

Целта на Теста за приемане (Commissioning Test) е да се удостовери способността на националната SSN система надеждно, навременно и вярно да обменя информация в мрежата на европейската SSN система. Процеса покрива всички съобщения, които се обменят между националната и европейската система чрез XML. Всички тестови случаи трябва да бъдат изпълнени чрез автоматичен обмен на съобщенията за да се удостовери правилната работа на системата.

Процедурите за тестване, първоначалните изисквания, списъка с тестови случаи и сценарии, тестовата организация и примерните тестови доклади (Test Report) са описани в Member State Commissioning Plan – Part A и Part B.

Процеса за извършване на Теста за приемане (Commissioning Test) се изпълнява в две фази. Двете фази се изпълняват от Тестовата среда на националната система и се изпращат съобщения към Тестовата среда на EMSA (първа фаза) и пре-продукционната среда на EMSA (втора фаза).

Фаза 1

Тази фаза удостоверява правилната работа на техническия интерфейс между националната и централната SSN система. За целта трябва да се изпълни успешно Теста за приемане (Commissioning Test) дефиниран в Member State Commissioning Plan.

Изпълнителят трябва да предостави на EMSA логовете със съобщенията, които са обменени при съответните тестове за извършване на оценка на резултатите. Ако е необходимо EMSA може да изиска повторение на някои тестове и предоставяне на нови логове на съобщенията. След обработка на резултатите EMSA ще предостави Доклад за тестване (Test Report).

Фаза 2

След успешното изпълнение на тестовете по Фаза 1 се провежда тест по Фаза 2. При този тест се използват реални продукционни данни и се извършва в пре-продукционната среда на EMSA.

След приключване на тестовете резултатите се анализират и при успешно изпълнение системата може да започне работа в продукционна среда.

Изисквания към обученията

Обучителните дейности трябва да предоставят на участниците:

- Добро познаване на общата рамка на системата: контекстът на логистиката на пристанищата, потребители, действителни и модифицирани процеси, предимства на системата;
- Добро познаване на системата и ролята, която потребителите могат да играят в пристанищната общност;
- Познаване на ефектите от решенията на потребителите върху други заинтересовани страни при използване на системата;
- Абстрактно познаване на технологията, която има системата: системи, модули, функции, конвенции и концепции;
- Специфични и подробни познания за това как да се използва пълноценно системата и ефективно изпълнение на процедурите.

Участниците трябва да предложат методология за обучение, която най-добре ще постигне посочените цели.

Трябва да се осигурят обучения за системните администратори на системата (технически персонал) и крайни потребители, разделени в групи, съставени от различни заинтересовани страни, както е посочено в целевите групи. Всички групи потребители трябва да бъдат обхванати.

Обучението трябва да се извършва от компетентен и опитен персонал, в помещение осигурено от Възложителя. Обучението се извършва на български език.

Кандидатите трябва да подготвят пълен план на програма за обучение, като гарантират, че потребителите на всички предоставени модули ще бъдат подходящо обучени, подготвени и уверени в използването на системата.

Планът за обучение трябва да бъде включен в цялостния план за изпълнение на проекта и всички свързани с него разходи трябва да бъдат включени във финансовото предложение на проекта за изпълнение (с изключение на изисквания на ниво участник, описани в документа за обучение).

Планът за обучение трябва да описва най-малко следните теми:

- Цели на обучението;
- Целеви групи;
- Изисквания на ниво участник – умения и/или познания, които е необходимо да има даден участник за провеждането на обучението

(например компютърна грамотност, технически познания в областта на информационните технологии и др.);

- Методология за обучение;
- Продължителност на обучението;
- Необходими предпоставки (технология / местоположение / съоръжения);
- Съдържание на обучението;
- Описание на курса на материалите;
- Комуникационен план за обучителни дейности, включително план за оценка на обучението.

Изпълнителят трябва да предостави следните материали за всяка тренировъчна сесия:

- Ръководства за обучение;
- Описание на процедурите;
- Информационна брошура за участниците за по-нататъшно проучване и справка по темата, отнасящи се до адресираните теми, включително използваните екрани, действия за въвеждане на данни и др.

Очаква се, че при предоставените учебни материали ключовите потребители ще обучават нови потребители вътрешно, прилагайки принципа „обучение на обучители“.

Обучителите се изисква да представят писмен отчет за обучителните сесии и неговите участници, както и изготвянето на формуляри за оценка и как тези оценки се използват за подобряване на обучителните дейности.

Мярката за успех на програмата за обучение и трансфер на знания е независимостта на потребителя. Организацията на потребителите трябва да може да поддържа процесите с помощта на предоставената технология, без редовна намеса на групата по поддръжка.

Обучение на техническия персонал

С особено внимание трябва да бъдат проведени обучения за персонала по техническата поддръжка на системата. Очаква се тази група да бъде уверена и ангажирана с бъдещи актуализации или нови версии на софтуера.

Изпълнителят трябва да подготви обучения и да установи необходимата връзка/комуникация между своя екип разработчици и персонала по поддръжката на Възложителя, за да бъдат предадени всички необходими знания.

Целта е да се обучи персонала на Възложителя за ефективна и успешна работа и поддръжка на инсталираното приложение. Изпълнителят трябва да извърши „оценка на нуждите“, въз основа на изисквания за техническите умения на персонала на Възложителя, които ще се изпълняват техническата поддръжка, и трябва да подготви подходящ план за обучение. Окончателният предложен план за обучение ще бъде потвърден от Възложителя.

Техническото обучение трябва да обхваща най-малко следните теми:

- Service Desk процеси и използвани инструменти;
- Мониторинг и отстраняване на неизправности;
- Изисквания за конфигуриране на средата за крайния потребител и помощни средства;
- Поддръжка на системата и тестване, използвани за проверка преди актуализиране или пускане на нови версии;
- Мониторинг и отстраняване на неизправности в междинен интеграционен софтуер (middleware) и съобщенията;
- Сигурност (Security Awareness).

8.3.3. Очаквани резултати

Изпълнени са успешно всички тестови сценарии и случаи описани в последната версия на Member State Commissioning Plan. Предаден е доклад за изпълнените тестове (Member State Commissioning Test Report).

Основните потребители са обучени в съответствие с плана за обучение. Подписан е приемателен протокол за обучение.

8.4. Дейност 4 *Пускане в експлоатация*

8.4.1. Описание на дейността

Тази дейност включва инсталиране промените в системата в продукционна среда, конфигурирането на системата, съдействие на Изпълнителя по време на етапа на пускане в експлоатация на системата и окончателното подписване и предаване на системата.

8.4.2. Изисквания към изпълнение на дейността

След успешното провеждане на тестовете за приемане и успешно преминаване на обученията на потребителите на системата Изпълнителят трябва да стартира системата в продукционна среда.

Подготовка за стартиране на системата в продукционна среда трябва да включва следните дейности:

- Инсталиране на промените в системата в продукционна среда;
- Настройка на конфигурацията и валидиране на продуктивната система;
- Допълнителна миграция и трансформация на данни;
- Проверка на продуктивната среда и потребителската среда за всички заинтересовани страни

По време на този етап Изпълнителят трябва да подготви и предостави окончателните резултати от проекта: Отчет (окончателен доклад) за проекта, техническа документация, ръководства за потребителя и документ за предаване. Отчета (окончателният доклад) за проекта трябва да включва списък на всички изпълнени дейности и постигнатите резултати по време на цикъла на проекта, оценка на степента, до която са постигнати очакваните резултати и предложения за бъдещи нужди на Възложителя във връзка с обхвата на изпълнените договор.

8.4.3. Очаквани резултати

Измененията на системата са напълно функциониращи в продукционна среда. Приемането на промените е удостоверено чрез подписване на приемно-предавателен протокол. Цялата изискана документация и кодовете на внедрената система са предадени на Възложителя в хартиен и електронен вариант. Прехвърляне на правата на интелектуалната собственост върху Софтуерните продукти.

9. ДОКУМЕНТАЦИЯ

9.1. Изисквания към документацията

▪ Цялата документация и всички технически описания, ръководства за работа, администриране и поддръжка на Системата, включително и на нейните съставни части, трябва да бъдат налични и на български език;

▪ Всички документи трябва да бъдат предоставени от Изпълнителя в електронен формат (ODF/ /Office Open XML/MS Word DOC/RTF/PDF/HTML или

др.), позволяващ пълнотекстово търсене/търсене по ключови думи и копиране на части от съдържанието от оригиналните документи във външни документи, за вътрешна употреба на възложителя;

▪ Навсякъде, където в документацията има включени диаграми или графики, те трябва да бъдат вградени в документите в оригиналния си векторен формат;

▪ Детайлна техническа документация на програмния приложен интерфейс (API), включително за поддържаните уебуслуги, команди, структури от данни и др. Документацията да бъде придружена и с примерен програмен код и/или библиотеки (SDK) за реализиране на интеграция с външни системи, разработен(и) на Java или .NET. Примерният код трябва да е напълно работоспособен и да демонстрира базови итерации с API-то:

- Регистриране на крайна точка (end-point) за получаване на актуализации от Системата в реално време;
- Заявки за получаване на номенклатурни данни (списъци, таксономии);
- Заявки за актуализиране на номенклатурни данни (списъци, таксономии);
- Регистрация на потребител;
- Идентификация и оторизация на потребител или уебуслуга;

▪ Документацията за приложния програмен интерфейс (API) трябва да бъде публично достъпна;

▪ Всеки предоставен REST приложно-програмен интерфейс трябва да бъде документиран чрез API Blueprint (https://github.com/apiaryio/api-blueprint), Swagger (http://swagger.io) или чрез аналогична технология. Аналогично представяне трябва да бъде изготвено и за SOAP интерфейсите;

▪ Детайлна техническа документация за схемата на базата данни – структури за данни, индекси, дялове, съхранени процедури, конфигурации за репликация на данни и др.

▪ Ръководства на потребителя и администратора за работа и администриране на Системата

▪ Обща информация, инструкции и процедури за администриране и поддръжка на приложните сървъри, сървърите за бази данни и др.

▪ Обща информация, инструкции и процедури за администриране, архивиране и възстановяване, и поддръжка на сървъра за управление на бази данни.

9.2. Прозрачност и отчетност

▪ В обхвата на проекта е включено извършване на дейности по анализ на бизнес процеси и нормативна уредба, проектиране на системна и приложна архитектура, разработване на компютърни програми и други дейности, свързани с предоставяне на специализирани професионални услуги. Изпълнителят и Възложителят трябва да публикуват подробни месечни отчети в машинночетим отворен формат за извършените дейности, включително количеството изработени човекодни по дейности, извършени от консултанти, експерти, специалисти и служители на Изпълнителя и Възложителя.

Документацията, предоставена от Изпълнителя на Възложителя, трябва да бъде:

▪ на български език;

▪ на хартия и в електронен формат; копирането и редактирането на предоставените документи следва да бъде лесно осъществимо;

▪ актуализирана в съответствие със съгласувана с възложителя процедура, която следва да включва документи, подлежащи на промяна/актуализация, крайни срокове и нужната за случая методология.

Минимално изискуемата документация по проекта включва долуизброените документи.

9.3. Системен проект

Изпълнителят на настоящата поръчка трябва да дефинира в детайли конкретния обхват на реализация на софтуерната разработка и да документира изискванията към софтуера в детайлна техническа спецификация (системен проект), която ще послужи за пряка изходна база за разработка.

При документирането на изискванията, с цел постигане на яснота и стандартизация на документите, е необходимо да се използва утвърдена нотация за описание на бизнес модели. Изготвената детайлна техническа спецификация (системен проект) се представя за одобрение на Възложителя. В случай на забележки, корекции или допълнения от страна на Възложителя Изпълнителят е длъжен да ги отрази в детайлната техническа спецификация (системен проект).

9.4. Техническа документация

Всички продукти, които ще се доставят, трябва да са със специфична документация за инсталиране и/или техническа документация, в това число:

- Ръководство за администратора, включващо всички необходими процедури и скриптове по инсталиране, конфигуриране, архивиране, възстановяване и други, необходими за администриране на Системата;
- Документи за крайния ползвател – Изпълнителят трябва да предостави главното Ръководство на ползвателите на софтуера. Документът е предназначен за крайните ползватели. Той трябва да описва цялостната функционалност на приложния софтуер и съответното му използване от крайни ползватели;
- Детайлно описание на базата данни;
- Описание на софтуерните модули;
- Описание на изходния програмен код.

9.5. Протоколи

Изпълнителят трябва да изготвя протоколи от изпълнението на различните етапи на проекта, описани в раздел 8 на настоящия документ, заедно със съпътстващите ги документи – резултати от изпълнението на етапите.

9.6. Комуникация и доклади

За успешното изпълнение на проекта участниците в настоящата обществена поръчка трябва да предложат адекватен механизъм за управление на проектната комуникация, който е неразделна част от предлаганата цялостна проектна методология.

Управлението на комуникацията трябва да включва изготвяне на минимум следните регулярни доклади за статуса и напредъка на изпълнението на поръчката:

9.6.1. Встъпителен доклад

Встъпителният доклад трябва да бъде предоставен до един месец от подписването на договора и да съдържа описание минимум на:

- Подробен работен план и актуализиран времеви график за периода на проекта;
- Начини на комуникация;
- Отговорни лица и екипи.

Встъпителният доклад следва да бъде одобрен от Възложителя.

9.6.2. Междинни доклади

Междинните доклади трябва да бъдат представяни и да се предават при приключване на всяка от дейностите и поддейностите и/или при настъпване на събитие.

Междинните доклади трябва да съдържат информация относно изпълнението на дейностите и поддейностите по предварително изготвения проектен план.

Докладът за междинния напредък трябва да бъде подготвен по следния начин:

- Общ прогрес по дейностите през периода;
- Постигнати проектни резултати за периода;
- Срещнати проблеми, причини и мерки, предприети за преодоляването им;
- Рискове за изпълнение на свързани дейности и на проекта като цяло и предприети мерки;
- Актуализиран план за изпълнение, ако има такъв.

Всеки междинен доклад следва да бъде одобрен от Възложителя.

9.6.3. Окончателен доклад

В края на периода за изпълнение трябва да се представи окончателен доклад. Окончателният доклад трябва да съдържа описание на изпълнението и резултати.

Докладите се изпращат до отговорния служител на Възложителя. За тази цел Възложителят ще определи в договора отговорния/отговорните служител/служители. Всички доклади се представят на български език в електронен формат и на хартиен носител. Докладите се одобряват от отговорния/отговорните служител/служители в срок до 5 работни дни.

Всички доклади трябва да се представят на възложителя на български език на хартиен и на електронен носител. Представянето на докладите трябва да се извършва чрез подписване на двустранни предавателно-приемателни протоколи, подписани от представители на Изпълнителя и на Възложителя.

Възложителят разглежда представените доклади и уведомява Изпълнителя за приемането им без забележки или ги връща за преработване, допълване и/или окомплектоване, ако не отговарят на изискванията, като чрез упълномощено в договора лице дава указания и определя срок за отстраняване на констатираните недостатъци и пропуски.

10. РЕЗУЛТАТИ

Очакваните резултати от изпълнението на настоящата обществена поръчка са следните:

- Доставена, инсталирана и конфигурирана актуализираната информационна система SafeSeaNet, която да бъде адаптирана и надградена съгласно изискванията на Възложителя;
- Обучени ключови потребители и администратори на системата;
- Инсталиран и конфигуриран базов софтуер - база данни и приложен сървър;
- Доставени лицензи за базов софтуер - в случай, че Изпълнителят е предложил
- Базов софтуер, който подлежи на лицензиране;
- Доставен и приведен в обща работоспособност хардуер.