

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ ДО БЪЛГАРСКА НАРОДНА БАНКА

Открита процедура за възлагане на обществена поръчка с предмет:
„Развитие и абонаментно обслужване на Системата за провеждане на аукциони за ДЦК (АДЦК)“

УВАЖАЕМИ ДАМИ И ГОСПОДА,

С настоящото Ви представяме нашето техническо предложение за участие в обявената от Вас открита процедура за възлагане на обществена поръчка с предмет: **„Развитие и абонаментно обслужване на Системата за провеждане на аукциони за ДЦК (АДЦК)“**.

1. Декларираме, че ще изпълним поръчката, съобразявайки се с условията по изпълнение, посочени от Възложителя в документацията за участие.

2. Декларирам, че представляваният от мен участник е запознат с подробното описание на „Системата за провеждане на аукциони за ДЦК (АДЦК) в БНБ („система/та“), представено в Приложение № 1 – „Системата за провеждане на аукциони за ДЦК (АДЦК)“ в БНБ (описание на съществуващата система)“.

3. Декларирам, че срокът на валидността на офертата ни е 3 (три) месеца, считано от датата посочена в обявлението като краен срок за получаването на оферти.

4. Декларирам, че съм запознат с условията и приемам клаузите в проекта на договора, приложен към документацията на обществената поръчка с гореописания предмет.

5. Декларирам, че представляваният от мен участник ще извършва развитие на системата, в съответствие с условията и изискванията на Възложителя, посочени в проекта на договора и Приложение № 3 – „Съществуваща инфраструктура и изисквания при разработване на новата версия на „Системата за провеждане на аукциони за ДЦК (АДЦК) в БНБ“, Приложение № 4 – „Задание за доработка на „Системата за провеждане на аукциони за ДЦК (АДЦК) в БНБ“ и Приложение № 5 – „Подробна функционална и техническа спецификация към Заданието за доработка на „Системата за провеждане на аукциони за ДЦК (АДЦК) в БНБ“. Предложението ни за извършване на развитието на системата, в случай че бъдем определени за изпълнител на поръчката се съдържа в *Приложение 1 – Предложение за изпълнение на поръчката*

Забележка: Предложението за извършване на развитие на системата се изготвя съгласно изискванията на възложителя, съдържащи се в посочените Приложение № 3, Приложение № 4 и Приложение № 5.

6. Декларирам, че представляваният от мен участник ще осигурява абонаментно обслужване на системата в съответствие с условията и изискванията на Възложителя, посочени в проекта на договора и Приложение № 2 „Изисквания, обхват и условия за абонаментното обслужване на „Системата за провеждане на Аукциони за ДЦК

Заличаванията на информация в документа са на основание на чл. 2, ал. 1 от Закона за защита на личните данни.

100

Като неразделна част от настоящето представяне прилагаме всички изискани от възложителя документи”.

София

Подпись:.....

Име на участника: Обединение Флайинг

СЪЛЮШЪНС

[illegible]

100

1. ПРОГРАМНО - ТЕХНИЧЕСКИ УСЛУГИ ЗА МИГРАЦИЯ КЪМ НОВА ТЕХНИЧЕСКА АРХИТЕКТУРА

Техническа архитектура

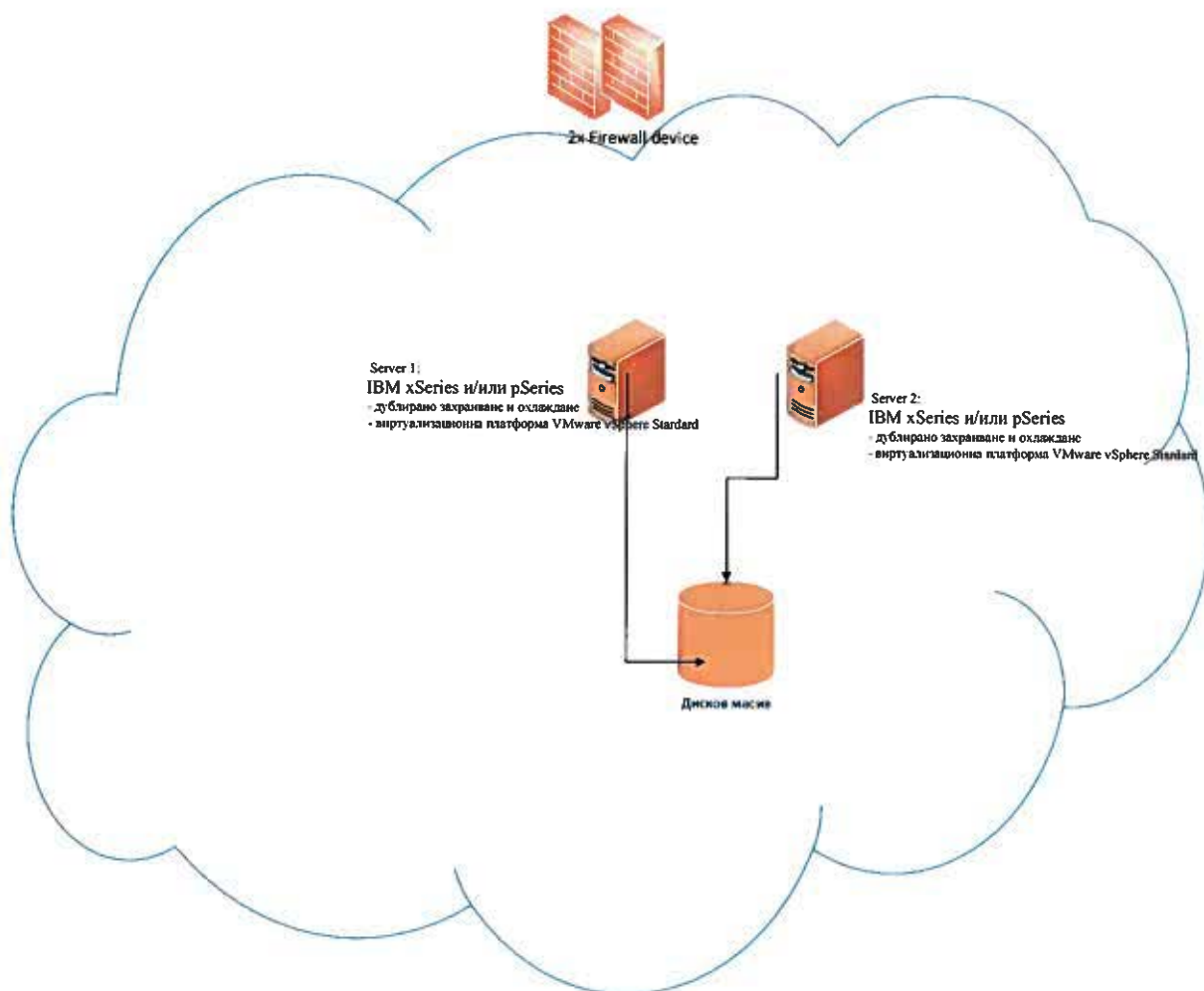
Флайинг Салюшънс стриктно ще спазва изискванията на Възложителя към техническата архитектура описани в Техническото задание:

- Ще осигури ефективно използване на ИТ инфраструктурата;
- Ще бъде съвместима с виртуализационните технологии използвани в БНБ;
- Ще осигурява максимална непрекъсваемост на процеса на работа;
- Ще осигурява ефективен мониторинг и управление;
- Ще бъде интегрирана с наличните средства за мониторинг;
- Ще осигурява бързо възстановяване след срив или отпадане на компонент;
- Ще осигурява надежден механизъм за архивиране и възстановяване на данните;
- Ще осигурява минимизиране на разходите за поддръжка на ИТ инфраструктурата.

Флайинг Салюшънс ще използва данните от направения анализ от основните характеристики на съществуващата инфраструктура в БНБ - техническо осигуряване, базов софтуер, комуникационна среда и ще реализира облачна архитектура от вида „Инфраструктура като услуга“ (IaaS - Infrastructure-as-a-Service), като Виртуална среда от типа частен облак за хостване на Системата за провеждане на аукциони за ДЦК (АДЦК) като използва наличните за проекта оборудване и лицензи, а именно:

- тип сървъри – IBM xSeries и/или pSeries;
- среда за виртуализация –VMWare;
- сървърни операционни системи – IBM AIX, SuseLinux, Windows;
- среда за съхранение на данни – SAN, реализирана с оборудване на IBM;
- база данни и средства за разработка - Oracle база данни;
- архивираща среда – реализирана с оборудване на IBM;
- комуникационна среда – реализирана с оборудване на Cisco Systems;
- средства за мониторинг - Oracle Enterprise Manager Cloud Control;

При изпълнението на поръчката Флайинг Салюшънс ще проектира, конфигурира и пусне в реална експлоатация всички необходими компоненти, описани в предложението, като по този начин ще осигури работеща виртуална среда, хостваща виртуалните сървъри, върху които ще се инсталира Системата за провеждане на аукциони за ДЦК (АДЦК).



Фигура 1 Схематично представяне на виртуалната среда от типа „частен облак“

Флайинг Салюшънс ще използва архитектурата визуализирана на фигурата „Схематично представяне на виртуалната среда от типа „частен облак“, като инсталира за проекта два броя сървъри с виртуализационна платформа VMware vSphere Standard и трети сървър с виртуализационна платформа VMware vCenter в режим на работа Fail-over Cluster. По този начин ще бъде реализирана високонадеждна и отказоустойчива виртуална среда, върху която могат да бъдат инсталирани и конфигурирани необходимите на Възложителя виртуални сървъри. При използване на Fail-over Cluster се гарантира, че при отпадане на единият от физическите сървъри, виртуалните сървъри, хоствани на него, се прехвърлят на другия/те работещи сървъри. Тази архитектура позволява лесно добавяне на

физически сървъри, към съществуващия сървър, при необходимост от разширяването му. За управление на сигурността и достъпа до предложеното решение за изграждане на ИТ инфраструктура от типа „частен облак“ ще се използва системата от 2x Firewall device (2 бр. Защитни стени) от комуникационна среда – реализирана с оборудване на Cisco Systems с възможност за автоматично балансиране на натоварването.

Детайлен дизайн на предложената инфраструктура ще бъде предложен и след съгласуване с Възложителя, инсталиран, конфигуриран и пуснат в експлоатация, след извършването на анализ на съществуващата ИТ инфраструктура на Възложителят.

Логическата архитектура на частния облак е представен на фигурата:

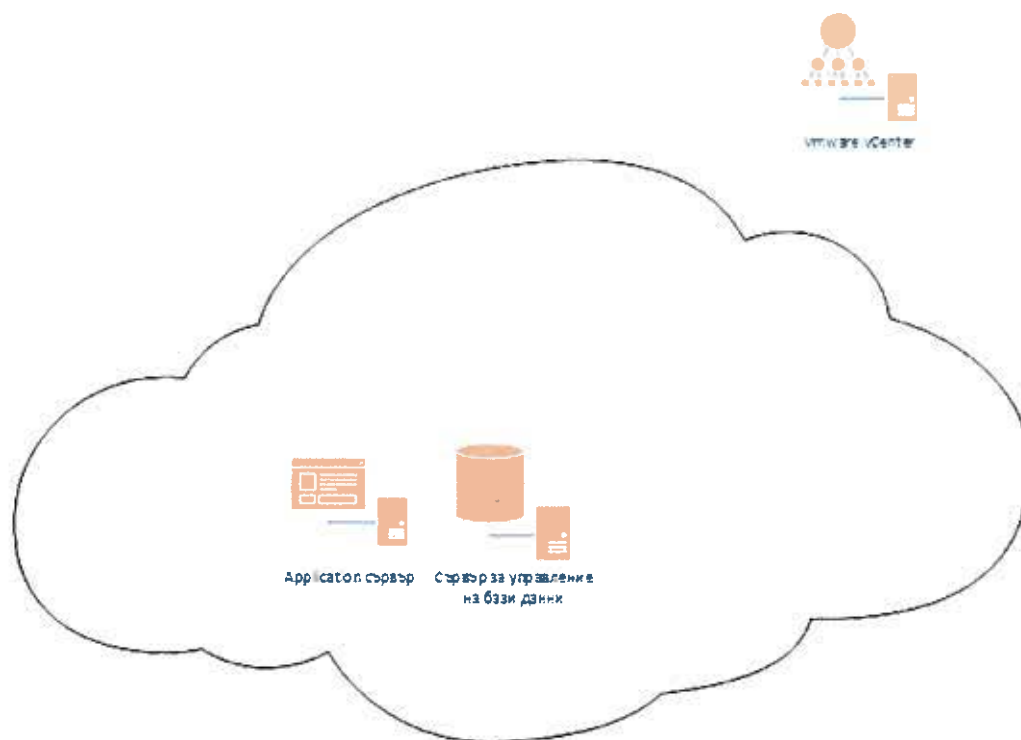


Фигура 2: Логическата архитектура на частния облак

Флайинг Салюшънс ще инсталира, конфигурира и пусне в експлоатация следните виртуални сървъри:

- Сървъри за управление на бази данни:
- Ще функционират върху машини IBM pSeries, с операционна система IBM AIX v.7.2 или по-висока версия и база данни Oracle RDBMS v.11.2.0.3
- Приложни (application) сървъри
 - Виртуални сървъри, върху изградената ИТ инфраструктура, в защитена мрежа, без достъп до Интернет с цел осигуряване на сигурността и защитата на данните.
 - Операционна система Windows Server 2012 или по-висока;
 - Oracle WebLogic, Oracle Application Server;

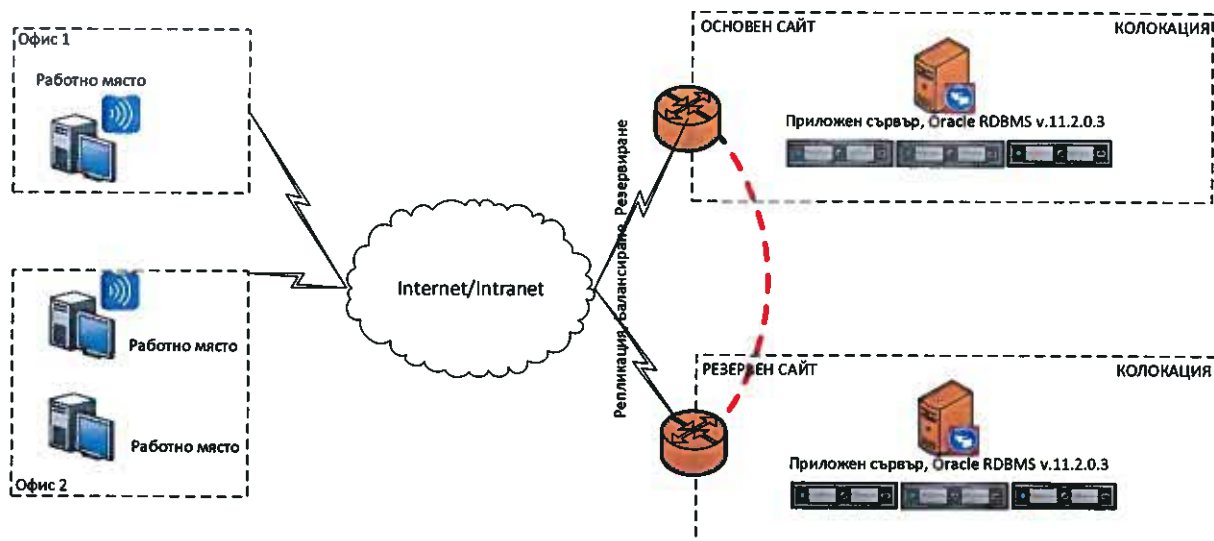
Примерно схематично предложените сървъри се представени по следния начин:



Фигура 3: Схематично представяне на виртуалните сървъри

С цел осигуряване на максимална надеждност на Системата за провеждане на аукциони за ДЦК (АДЦК) и възможността и за продължаване на работата в случай на срыв на съществен хардуерен компонент Флайинг Салюшънс ще осигури дублиране на компонентите или прилагане на други решения, гарантиращи наличност на услугите. Системата ще бъде подсикурена чрез възможност за работа на 2-та сайта (основен и резервен). Данните на системата ще бъдат разположени на дискови системи, разположени съответно в основния и резервния сайт с репликация на данните. Между двата сайта ще има изградена единна SAN среда. Архивирането на системата ще се извършва едновременно и на двата сайта.

За защита на данните и възстановяване след бедствия или увреждания ще се приложат най-добрите решения като Oracle DataGuard.



Фигура 4 Концепция за резервираност на сайтовете

- За гарантиране на висока надеждност и непрекъсваемост на продукционната среда ще се използват IBM PowerHA решение, IBM PowerVM LPM или Oracle RAC.
- За мониторинг и управление на ресурсите и компонентите на системата ще бъдат инсталирани агенти за Oracle Enterprise Manager Cloud Control.
- Данните ще се съхраняват върху дискови системи от фамилията IBM DS8000.
- Архивирането на данните ще се осъществява върху лентови системи, IBM TS3300 и IBM TS3500. Целта е да се осигури нормален backup (създаване на резервно копие), позволяващ възстановяване на фирмената информация, съхранявана на сървърите поддържащи Системата за провеждане на аукциони за ДЦК (АДЦК).

Носители на информация, използвани за направа на backup:

След запознаване с вида на магнитните ленти и големината на данните за архивиране Флайинг Салюшънс ще избере правилния подход (брой магнитни ленти) за извършване на процедурата за архивиране на информацията:

Пример:

- 11 бр. ленти към всяко устройство – 5 бр. за седмичните backup-и от понеделник до петък.
- 6-та и 7-та лента се използват за направата на седмичен backup (2 еднакви копия)
- 8-та и 9-та лента - за месечния backup (2 еднакви копия)

→ 10-та и 11-та лента - за годишен backup

График за направата на backup:

→ Дневен - Дневен backup се прави на всички бизнес приложения и данни;

→ Седмичен - седмичен backup се прави на всички бизнес приложения и данни;

→ Месечен - Месечен backup се прави на всички приложения и данни;

На месечна база ще се използва и магнитна лента за почистване на лентовите библиотеки;

→ Годишен

Годишен backup се прави на всички приложения и данни;

Съхранение на backup-ите/Backup storage:

→ Дневен

Съхранява се в Отдел посочен от Възложителя в пригодени за целта заключени контейнери. До тях имат достъп само служителите на отдела.

→ Седмичен

Едно копие се съхранява се в специален сейф в Отдел посочен от Възложителя. Второ копие се съхранява в трезор на банка извън пределите на предприятието. Записът върху лентите за седмичен backup се обновява ежеседмично. За подмяната и съхранението на лентите със седмичния backup отговарят екипи посочени от Възложителя.

→ Месечен

Едно копие се съхранява се в специален сейф в Отдел посочен от Възложителя. Второ копие се съхранява в трезор на банка извън пределите на Възложителя. Записът върху лентите за месечен backup се обновява ежемесечно. За подмяната и съхранението на лентите със седмичния backup отговарят екипи посочени от Възложителя.

→ Годишен

Едно копие се съхранява се в специален сейф в Отдел екип посочен от Възложителя. Второ копие се съхранява в трезор на банка извън пределите на Възложителя. Записът върху лентите за годишен backup се обновява ежегодно. За подмяната и съхранението на лентите със годишен backup отговарят екипи посочени от Възложителя.

➤ Процедура по възстановяване/Recovery procedure:

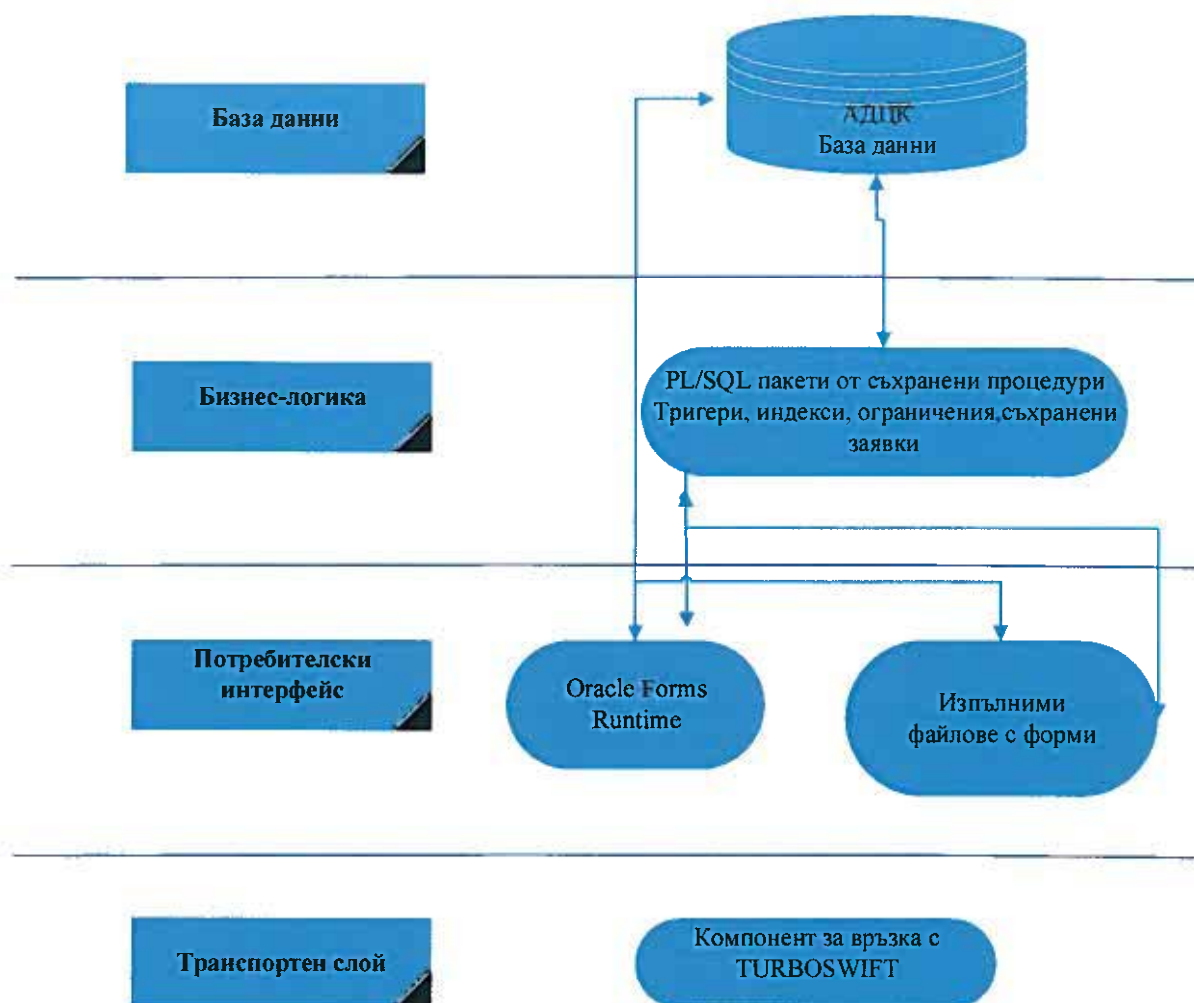
- Възстановяването на данните от направен backup се извършва само с одобрението на Възложителя.

Софтуерна архитектура

Опитът и практиката показват, че една от най-добрите и най-подходящите архитектури за изграждане на система за извършване на комплексна услуга, свързваща както бизнес модули, така и модул за данни, модули за презентация и услуги е архитектура тип Многослойна архитектура (Multilayered Architecture). Клиентската част ще бъде разработена с Oracle Forms и достъпна за инсталиране на клиентските станции, работещи под операционна система MS Windows 7, 8 или по-висока версия.

Многослойната архитектура е архитектура от тип клиент-сървър, в която съхранението на данни, бизнес логиката и потребителският интерфейс са раздели на различни слоеве. Флайинг Салюшънс ще проектира и реализира Системата за провеждане на аукциони за ДЦК (АДЦК) чрез многослойна архитектура, като ще дефинира следните слоеве:

- Слой за данни
- Слой за бизнес процеси
- Приложен слой
- Слой за потребителски интерфейс и взаимодействие с потребителите
- Транспортен слой



Фигура 5 Многослойна архитектура

Всеки модул ще бъде относително независим от останалите модули. Това разделяне на слоеве ще донесе множество ползи в процесите на разработка на Системата за провеждане на аукциони за ДЦК (АДЦК):

Подобряване на проектирането: Разделянето на отговорността по модули подпомага изчистване на логиката на опериране на модула, а от там и самото проектиране.

Подобряване на планирането и ресурсите, нужни за изпълнение на договора: Тъй като всеки модул изисква специфичен набор от умения и технологии, то ресурсите могат да се планират според тях.

Подобряване на тестването на проекта: Предимството на проекти с многослойна архитектура е, че всеки слой може да се тества поотделно и независимо от останалите. По този начин тестването се концентрира върху конкретен слой, който има набор от функционалности, далеч не толкова сложни, колкото на цялата система. Когато отделните слоеве са тествани и е потвърдено тяхното коректно

функциониране, се провеждат и тестове за взаимодействието между отделните слоеве. Това са така наречените интеграционни тестове и те имат за цел да подсилят правилната комуникация между слоевете. Многослойната архитектура улеснява до голяма степен локализирането на проблемните зони в един проект, тъй като тестовете са на ниво слой.

→ Подобряване на гъвкавостта и скалируемостта на проекта: Тъй като многослойната архитектура има за цел да раздели управлението и функциите на всеки слой, така че те да са относително независими един от друг, то промяната на един слой няма да доведе до промяна на слоевете под и над него. По този начин се постига много по-добро подобряване на проблеми в даден слой, и дори неговата промяна на чисто функционално ниво, ако това е наложимо.

Разделянето на слоеве ще даде възможности за устойчивост, лесна интеграция и по-добро тестване, като по този начин ще се гарантира сигурността и доброто функциониране на системата. В архитектурния модел на Системата за провеждане на аукциони за ДЦК (АДЦК) ще се заложат основните слоеве:

- Слой за връзка с базата данни и опериране върху данните;
- Слой за опериране на бизнес модулите – извършване на различните бизнес процеси;
- Слой за взаимодействие с потребителите на системата;

Към системата ще бъде разработен потребителски интерфейс за публичен достъп до нея след идентификация с потребителско име и парола и/или електронен подпис и/или еИД и/или чрез специално генериран сертификат като се спазва закона за „Електронния документ и електронния подпис“ и наредбите по неговото прилагане и най-добрите практики със SAML 2.0.

Транспортен слой

Транспортният слой ще бъде реализиран чрез съхранени в базата данни програмни пакети и външни за системата програмни модули. Транспортният слой доставя данните и файловете от външните системи до АДЦК и обратно.

По отношение на входния поток информация транспортният слой:

- следи за пристигане на входни съобщения и файлове;
- транспортира файловете до сървъра на АДЦК;
- следи за успешното зареждане;
- архивира файловете след зареждането им;
- поддържа журнал на зареждането.

По отношение на изходния поток информация транспортният слой:

- следи за генерирани файлове от АДЦК;
- транспортира файловете до сървъра на TURBOSWIFT;
- архивира файловете след зареждането им;
- поддържа журнал на зареждането;

Допълнително към основните слоеве на системата ще се добавят и слоеве, които не покриват бизнес процесите, но са задължителни за правилното и опериране. Това са така наречените нефункционални слоеве, имащи за цел не да предоставят функционалност, а да подсиgurят системата и нейното правилно функциониране:

- Слой за подсигуряване на сигурността на система.
- Слой за прихващане на грешки и реакция на грешки.
- Слой за запис на системни съобщения с цел наблюдение.

Връзката между слоевете на едно многослойно приложение се осъществява от интерфейси за комуникация, които се изграждат на върха на всеки слой. По този начин слоевете ще могат да оперират самостоятелно или взаимосвързано.

Трислойната архитектура, която ще използва Флайинг Салюшънс включва и взаимодействие с доставчици на външни услуги (еИД), както и създаване на връзка посредством SOAP уеб услуги към съответни организации определени от Възложителя.

Допълнително системата ще включва и презентационен слой за физическите и юридически лица.

Презентационен слой (потребителски интерфейс) – Презентационният слой е най-високият слой в рамките на един софтуерен продукт. Той предоставя нужните визуални и интерактивни средства за комуникация с крайните потребители на услугата. Презентационният слой ще се реализира като потребителски интерфейс, който ще е уеб базиран.

Отговорностите на презентационния слой ще са:

- ✓ Да осигури потребителски интерфейс за опериране със системата;
- ✓ Да валидира данните, въвеждани от потребителите;
- ✓ Да преведе данните и командите от потребителя към бизнес слоя, като предварително ги подготви в подходящ формат;
- ✓ Да преведе данните или съобщенията за грешки от бизнес слоя към потребителския интерфейс, като ги представи в подходящ за това вид.

Презентационният слой на системата ще представлява портал за достъп на Физически / Юридически лица / служители на държавната администрация.

Флайинг Салюшънс ще използва следните средства за разработване на Системата за провеждане на аукциони за ДЦК (АДЦК):

→ PL/SQL

Всички програмируеми елементи от бизнес логиката на системата, които не са пряко свързани с потребителския интерфейс, ще са разработени на PL/SQL. Програмното осигуряване на АДЦК ще бъде разработено под формата на пакети, с цел улесняване на поддръжката.

→ Oracle Forms

Oracle Forms ще бъде използван като стандартно средство за създаване на графичен интерфейс към базата данни и разработване на екранните форми на системата.

СУБД

За целите а настоящия проект се предвижда да се ползва БД Oracle 11g. В рамките на проекта се предвижда повдигане на версията на сега съществуващата и използвана от приложението база Oracle 8 до версия 11.2, което ще се извърши на стъпки. Стъпковият подход предвижда преминаване, повдигане на версията до Oracle BD 9.2 и след което повдигане на версията до Oracle BD 11.2. След повдигане на версията ще се направи и преместване на данните на системата в новата версия/ среда.

Флайинг Салюшънс ще използва три типа на резервни копия (backup) на базата от данни, обслужващи работата на системата:

- Пълен архив (Full backup) – създаване на пълно резервно копие на базата от данни всяка нощ, гарантиращ пълно възстановяване.
- Диференциален архив (Differential backup) – създаване на диференциални резервни копия на базата от данни на всеки 12 часа.
- Архивиране на транзакциите (Transaction log backup) – архивиране на транзакциите в базата от данни на всеки 1 час.

Унифициран език за моделиране (UML)

Описва обектите, обменящи информация и съдържащи данни (атрибути на обектите). Обектно-ориентираното моделиране използва съществено **UML** (Unified Modeling Language) като стандартен език за описание на процесите и класовете.

Анализът обхваща следните дейности:

→ Структуриране на информацията, събрана по време на проучването:

Осъществява предварителна подготовка на анализа – идентифициране и групиране на сходни процеси, декомпозиране на сложни процеси и функции и други трансформации, способстващи за по-доброто и пълно разбиране на процесите и тяхното взаимодействие;

→ Създаване на модел на процесите:

На база на структурираната информация се изготвя модел на процесите. Моделът описва текущото състояние на разглежданата система (или част от система попадаща в обхвата на проекта), както и бъдещите аспекти на нейното оптимизиране и разширяване;

→ Съответствие на потребителските изисквания с процесите:

Анализира нуждите и изискванията на отделните потребители, участници в процесите. Този анализ се фокусира върху взаимодействието между потребителите и процесите и върху това как самите процеси посрещат и удовлетворяват изискванията на участниците в тях.

Детайлното описание на функциите на системите е пряко отражение на бизнес логиката на отделните й процеси. Функционалната спецификация ще бъде структурирана в съответствие с всички модули и тяхната взаимовръзка. Вътре в модулите функциите ще бъдат групирани в зависимост от предназначението им и потребителските роли, които ги използват.

Описанието на всяка функция ще съдържа като минимум:

→ Предназначение;

→ Потребителски роли, имащи право за достъп до функцията;

→ Предварителни условия за активирането на функцията;

→ Описание на логиката на функцията, включващо детайлен алгоритъм на последователността на отделните действия, правила за валидиране на данните и операциите, обработка на изключителните ситуации и т.н.;

→ Входните и изходни данни;

→ Връзка с други функции или обръщение към външни системи;

→ Изход от функцията – предаване на управлението след приключване.

При необходимост, в описанието на функцията или в отделен рефериран документ се прилага и макета на съответния й потребителски интерфейс (един или повече екрани).

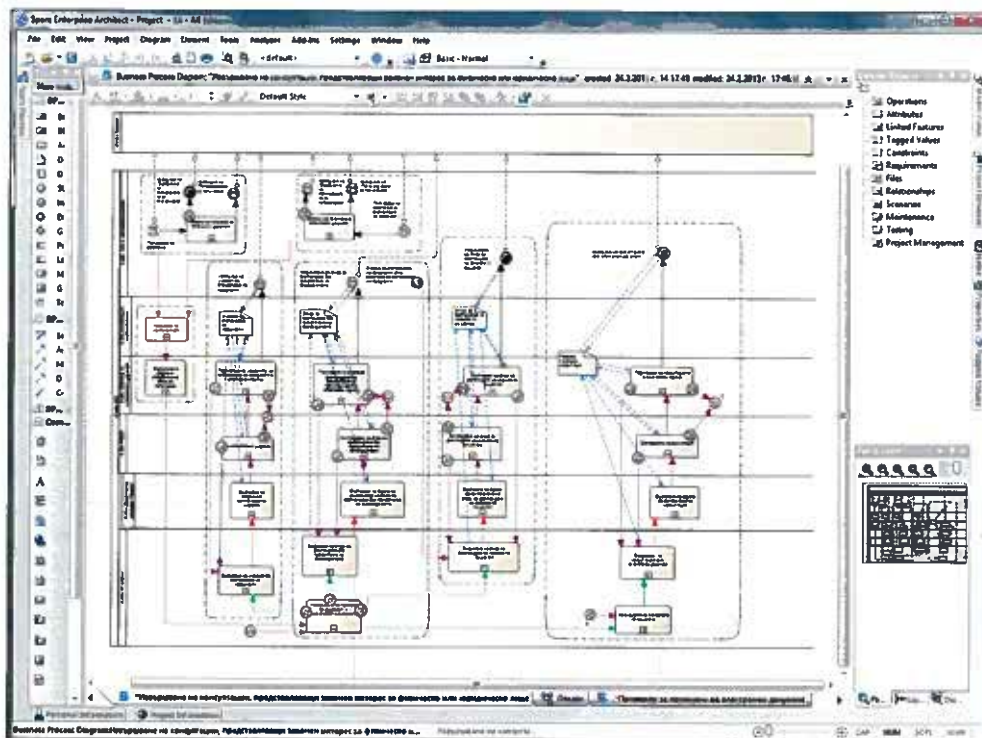
Алгоритъмът на функцията се описва с помощта на една или повече диаграми (в UML или друга подходяща графична нотация), съпроводени с детайлно описание на съдържанието и взаимовръзките на всички елементи на диаграмите.

Софтуерният инструмент, който ще бъде използван за моделиране и анализ е **Sparx Enterprise Architect**. Той представлява визуален инструмент за моделиране и проектиране, базиран на езика **UML (Unified Modeling Language)**. Платформата поддържа проектиране на софтуерни системи, моделиране на бизнес процеси и моделиране на индустриално базирани домейни. Инструментът се използва не само при моделиране на архитектурата на софтуерната система, но и по време на целия процес на разработка на софтуерното решение.

Чрез функционалностите на приложението се определят следващите стъпки в сценария за употреба (**Use case**), като решението се базира на редица критерии. Други функционалности предоставят пълен контрол над симулацията чрез манипулиране на променливи и извършване на изчисления в определен момент от симулацията.

Enterprise Architect предоставя възможността за използването на ревизионни точки (**breakpoints**), които спомагат анализа и вземането на решения, както и за подобряването на резултатите. Симулацията спомага за подобряване на комуникацията, извличане на основните идеи и намаляване на сложността чрез моделиране на по-високо ниво на абстракция.

Опитът ни с подобен инструмент ще бъде от полза при моделирането и анализа на ключови връзки в разработването на технически документи. Предоставените функции в инструмента дават възможност за разработване на добре структуриран модел под формата на лесно разбираема диаграма. Представените по-долу екранни форми представляват примерни диаграми използвани от Флайинг Салюшънс при разработване на техническа документация за сходни по същност проекти.



Фигура 6 Примерни диаграми

Концепция за изпълнение на изискванията за сигурността на информационните системи в БНБ

Системата за провеждане на аукциони за ДЦК (АДЦК) ще бъде реализирана със стандартни технологии, и ще поддържа общо приети комуникационни стандарти, които ще гарантират нейната съвместимост. Услугите и бизнес процесите ще бъдат проектирани така, че да бъдат независими за бъдещо разширяване и обслужване и позволяващи настройване и промяна на параметрите през потребителски интерфейс. Информационната система ще осигури функционалност за текущ мониторинг, анализ и контрол на изпълнението на бизнес процесите. Разработената система ще осигурява възможности за разширяване, резервно обезпечаване и балансиране на натоварването. При разработването на АДЦК ще се предвидят възможни промени, продиктувани от непрекъснато променящата се среда. Информационната система ще бъде разработена като гъвкава и лесно адаптивна, която отчита законодателни, административни, структурни или организационни промени, водещи до промени в работните процеси. Системата за провеждане на аукциони за ДЦК (АДЦК) ще може да се интегрира с интерфейсите за предоставяне на информация на други институции посредством SOAP уеб услуги. При реализация на уеб услугите ще се спазват ограниченията, описани в WS-I Basic Profile 2.0.

Ще бъде използван подход, който да спре нерегламентиран достъп до данните в АДЦК интеграцията към външните системи чрез прилагане на решения за сигурност.

Основните стандарти, технологии и модули, които осигуряват изискваната функционалност, са:

- HTTPS; HTTP върху SSL (Secure Socket Layer) за осигуряване на криптирана комуникация (интегритет и конфиденциалност);
- Single Sign On, осигуряващ надежден и сигурен единен достъп до всички приложения, реализиран чрез Central Authentication Server (CAS) Single Sign-On;
- Автентификация – за нея ще се използва Windows Authentication Provider, който ще се внедри чрез Windows Authentication Module, който конструира WindowsIdentity на основата на акредитация предоставена от уеб сървър;
- Оторизация въз основа на роли:
 - Потребителят се свързва с роли и съответно получава разрешение да ползва конкретни функции/модули/услуги. Управлението на ролите се извършва на високо ниво чрез специален модул за Управление на потребителите, поддържащ потребителски групи, организации, нива на достъп и високоспециализирани роли (по приложение, модул, функция, работен поток и др.);
 - Одит на достъпа: всички действия на потребители, изискващи автентификация и оторизация, ще се записват и могат да бъдат разглеждани от технически експерт по сигурността. Функционалността се отнася до:
 - ✓ защита на ниво потребителски интерфейс;
 - ✓ защита на ниво бизнес процеси;
 - ✓ защита на ниво бизнес услуги;
 - ✓ конфиденциалност по отношение на предоставените от клиента данни;
 - ✓ надеждни технологии за криптиране на пароли и служебна информация;
 - ✓ надеждна защита на данните, която не разрешава пряк неконтролиран от системата достъп на клиент до тях, копирането им и разрушаването на тяхната цялост;
 - ✓ надеждност на изпълнение на процесите без прекъсване и получаване на нежелани или грешни резултати.

Сигурност



Фигура 7: Логическа архитектура на компонент „Услуги за сигурност“

Флайинг Салюшънс ще използва компонент „Услуги за сигурност“, за да предостави множество разнообразни услуги за сигурност, включващи:

- Презентационен слой:
 - Защита на ниво протокол TLS/SSL;
 - Идентификация, автентикация и авторизация на потребители с потребителско име и парола и/или КЕП в Контейнер web-приложения, с възможност за интеграция и с eИД.
 - Контролиран достъп до екрани и части от него (само за потребители с определена роля)
- Слой „Бизнес процеси“:
 - Контролиран достъп до бизнес процеси (само за потребители с определена роля);
 - Авторизация на потребители за изпълнение на бизнес процеси с помощта на бизнес правила.
- Слой „Бизнес Услуги“:
 - WS-Security като част от WS-I Basic Profile;

➤ SAML

• Слой „Компоненти“:

- Декларативен и програмен подход за задаване на права на изпълнение и достъп до обекти.
- Подход за задаване на права на изпълнение и достъп до обекти на основата на бизнес правила.
- WindowsAuthenticationModule
- Подход, основан на сложни бизнес правила

• Слой „Данни“:

- Достъп до таблици, изгледи и определени колони само за потребители с определени права по потребителско име и парола.
- Съхраняване на криптирани данни в специални полета.

• Слой „Информационен модел, информационни услуги“:

- Достъп до информационни услуги само за потребители с определени права (роли);
- Генериране на отчети само за потребители с определени права (роли)

• Слой „Интеграция“:

- Използване на КЕП;
- Криптиране на съобщения с DES/RSA;
- WS-Security;
- Обмен на данни по защитен канал, например SSL, FTP/S.
- VPN.

VPN е частна мрежа, която се изгражда върху съществуваща вече публична мрежа (най – често Internet). Вместо да се използват физически наети линии, VPN се изгражда върху виртуални тунели, които осигуряват връзката между отдалечените мрежи (потребители).

VPN предоставя следните услуги:

- Свързаност между физически разделени места.
- Подобрена сигурност
- Ниски разходи за поддръжка на мрежата
- Подобрена продуктивност
- Проста мрежова топология

- Сигурност
- Надеждност
- Разширяемост
- Лесно управление

VPN сигурност: Криптиране

Криптирането представлява промяна на данните по начин, по който само този, за когото са предназначени може да използва. Повечето системи за криптиране работят на някой от следните два принципа:

- Симетрично криптиране
- Асиметрично криптиране
- При криптирането със симетричен ключ и за кодиране и за декодиране на данните се използва един и същи ключ, което предполага определена несигурност от гледна точка на преноса на ключа. Поради тези причини в реализацията на интеграцията на АДЦК с външните системи Флайинг Салюшънс ще се използва асиметрично криптиране. Асиметричното криптиране представлява комбинация от частен и публичен ключ.

VPN сигурност: IPSec

IPSec (Internet Protocol Security) протоколът осигурява нужната сигурност при комуникация в незащитени мрежи. Използва се режим на тунелиране, където се криптира и заглавната част (header), и информационната част. IPSec може да криптира данни между устройства като:

- Маршрутизатор към маршрутизатор
- „Защитна стена“ към маршрутизатор
- Компютър към маршрутизатор
- Компютър към сървър

VPN сигурност: AAA сървъри

AAA (authentication, authorization and accounting) се използват за по – улеснен достъп. Когато постъпи заявка за сесия от отдалечен клиент, заявката се предава към AAA сървър, който след това проверява:

- Кой сте вие - автентикация (authentication)
- Какво ви е позволено да правите – авторизация(authorization)
- Какво всъщност правите - акаунтинг (accounting)

VPN технологии

- Клиентски софтуер
- Клиентски хардуер
- VPN сървър
- NAS (network access server) използва се от доставчиците за VPN достъп до тях
- Център за управление на VPN

Тунелиране

VPN решението разчита на изграждането на тунел през Интернет. Като цяло тунелирането представлява поставяне на пакета в друг пакет и изпращането му. Протокола на външния пакет е познат на преносната мрежа и на двете страни, които ползват тунела. Тунелирането изисква три различни протокола:

- Транспортен протокол – този протокол се използва от мрежата, която извършва преноса.
- Капсулиращ протокол - Протоколът (GRE, IPSec, L2F, PPTP, L2TP), който “покрива” оригиналните данни
- Passenger протокол – Оригиналните данни (IPX, NetBeui, IP).

Тунелиране между мрежи

При VPN-а между мрежи, GRE (generic routing encapsulation) е обичайно използван протокол. Той включва информация за това какъв вид пакет се капсулира, както и информация за връзката между клиента и сървъра. Вместо GRE понякога се използва IPSec в тунелен режим.

Тунелиране: Отдалечен достъп

При отдалечен достъп, най – често се използва PPP. Като част от TCP/IP стека, PPP е преносител на други IP протоколи. Протоколите за изграждане на VPN с отдалечен достъп са:

- L2F (Layer 2 Forwarding) – Разработен от CISCO, L2F работи с всички типове автентикация използвани от PPP.
- PPTP (Point-to-Point Tunneling Protocol) - PPTP е създаден от PPTP Forum – Обединение „ТурСис“ включващ US Robotics, Microsoft, 3COM, Ascend и ECI Telematics. PPTP поддържа 40-bit и 128-bit криптиране и като L2F работи с всички видове автентикация на PPP.
- L2TP (Layer 2 Tunneling Protocol) - L2TP е разработка на PPTP Forum, Cisco и IETF (Internet Engineering Task Force). L2TP комбинира чертите на PPTP и L2F, като напълно поддържа IPSec

L2TP може да се използва и за VPN между мрежи. Този протокол може да изгражда тунел между:

- Клиент и маршрутизатор
- NAS и маршрутизатор
- Маршрутизатор и маршрутизатор

Флайинг Салюшънс ще предприеме следните мерки за защита на системите:

- За вход в системата ще се използват методи на аутентикация и оторизация – чрез въвеждане на потребителско име и парола, чрез квалифициран електронен подпис или чрез еИД или чрез специално генериран сертификат като се спазва закона за „Електронния документ и електронния подпис“ и наредбите по неговото прилагане и най-добрите практики със SAML 2.0. Флайинг Салюшънс ще използва най-добрите практики за повишаване на нивото на сигурността, посредством адекватна дължина на паролата (минимум 8 знака), изискване за наличие на малки, големи букви и/или специални символи. По този начин ще се повиши нивото на сигурност на паролите и ще ограничи възможностите за неправомерен достъп.
- Въвеждане на изискване за смяна на паролата на потребителите на максимум 3 месеца и невъзможност за избор на парола, използвана в рамките на предходната календарна година, като при промяна на паролата задължително да се въведе и старата парола.
- За вътрешни потребители може да бъде реализирана система от правила по отношение на достъпа до системата само от определени машини, зони, времеви интервали и др.. Потребителите с високи права на достъп би трябвало да се автентикират пред системата при по-стриктни процедури (например комбинация от IP контрол + силна парола + контрол на времето на достъпа, защитени частни канали, задължителен личен сертификат за идентификация на потребителя и др. Системите ще бъдат проектирани, така че да осигурят различни права на достъп според потребителските групи (използване на различни функции, достъп до данните (по ниво и по териториален обхват, до конкретен обект), достъп до видове справки (териториален обхват, конкретен обект), визуализация, печат);
- Флайинг Салюшънс използва стандарти при изработването на Системата за провеждане на аукциони за ДЦК (АДЦК), така че те да поддържат йерархично ниво на достъпа.
- Клиентските сесии ще се унищожават след предварително дефиниран период от време (time out), който ще бъде съгласуван с Възложителят;