# Глава 1. Проблеми на информационното осигуряване при управление на поръчките от клиенти

## 1.1. Същност и принципи на информационните системи, поддържащи дейността на производствено предприятие

### 1.1.1. Характеристика на ERP системите

ERP информационните системи позволяват ефективното планиране на дейността на предприятие, в т.ч. разходи за обновяване на оборудването и инвестициите в производството на нови изделия (Банабакова, В. К, 2019). Те произхождат от RP технологията (Requirements/resource planning - планиране на потребностите/ресурсите). Основната цел на RP е съкращаване на количеството на запасите от материали, незавършено производство и готова продукция, съгласуване на графика на доставките с работата на отделните производствени звена и процеса на закупуване (Филипов, Ст. Г., 2019). С логистичните технологии и тяхното приложение се цели осигуряване на оптимални решения в логистичната система (Благоев, Бл., 2010). Логистичната технология се определя като стандартизирана последователност (алгоритъм) на изпълнение на отделни логистични функции, и/или процеси в логистичната система или в отделни нейни функционални области (Сергеева, В., 2004). Някои от тези алгоритми и поддържащите ги информационно управляващи системи са получили и нормативна регламентация. Такива са MRP I и MRP II, за които са разработени и утвърдени международни стандарти ISO (Стоянов, Ст. Хр., 2019). ER спомагат преодоляването на проблеми свързани с управление на складовите наличности, като:

• Забавяне на постъпването на материали;

• Натрупване на излишни складови запаси;

• Нарушаване баланса на доставката;

• Намаление на ефективността на производство;

• Сложност при процеса на контрол и анализ на производствената дейност;

Подобренията от въвеждането на ERP се изразяват в увеличаване броя на изпълнените поръчки, повишаване качеството на логистичното обслужване към клиентите, възможности за промени в обема на поръчките, съкращаване на времето от поръчката до доставката и други (Банабакова, В. К, 2019).

Нека разгледаме SAP, който бива пуснат за първи път преди 50 години в Германия. В рамките на тази система се управляват всички функционални области на даден бизнес: от човешки ресурси, до финанси и функции за закриване на отчетен период, продажби, управление на клиенти, фактуриране и задължения, управление на инвентара, логистика, и други. Всяка отделна функция, от която едно предприятие може да има нужда, е напълно достъпна и интегрирана в SAP. Както беше отбелязано, SAP е водещата ERP система на пазара, като около 87% от глобалните организации го използват. SAP може да поддържа производствена (например Harley Davidson), нефтената и газовата индустрия (Shell), държавни органи.

В зависимост от компанията и много други фактори, внедряването на SAP може да отнеме дълго време и много ресурси. За сметка на това, SAP предлага и автоматизация, инструменти, които автоматично ще получават, съгласуват и извършват определени действия. Това позволява съсредоточаването върху други задачи, които могат да помогнат за растежа на компанията. SAP разполага с огромни количества данни, които да бъдат използвани за вземане на ефективни и сигурни бизнес решения.

SAP е разделен на различни области, които работят заедно, наречени модули. В SAP има два вида модули: технически и функционални модули. В техническите модули работят програмисти или ИТ персонал. Функционалните модули, които се използват от потребителите на системата, съдържат вградени транзакции, съответстващи на бизнес процесите. SAP има много функционални модули. Следната фигура представя 3 от най-използваните. 

***Фигура 1.1****: Модули в САП.*

Първата група е от модул Логистика. Sales and Distribution е насочен към обработка и доставка на поръчки за продажби. Модулът за управление на материалите включва закупуване и управление на инвентара. Производственото планиране съдържа основни данни като спецификация на материалите, маршрути и изпълнение на планирането на материалните изисквания. SAP Quality Management управлява контрола на качеството и несъответствията. Финансовото счетоводство на SAP включва главната книга, дължимите сметки и вземанията. SAP Controlling е мястото, където се извършва анализът на себестойността на продукта и рентабилността. Project Systems управлява счетоводните аспекти на планирането на проекта, мониторинга на проекта и функциите за изчисляване на разходите по проекта. Управлението на човешките ресурси обхваща целия цикъл на един служител в една компания, от наемане до прекратяване, включително ведомост. Функционалните модули са тясно интегрирани. Те ефективно изпращат информация помежду си, което е една от най-силните страни на SAP ERP системата.

SAP се състои от два типа данни: основни и транзакционни. Основните данни са градивните елементи за всички транзакции, като клиенти, доставчици, активи, материали и други. Те са относително статични. Необходими са специални разрешения за да се манипулират или създават основните данни. Данните за транзакциите, като продажби, покупки и фактуриране, се променят непрекъснато. Всеки SAP модул има своя собствена независима организационна структура, която определя взаимоотношенията между различните работни групи и отдели. Следващата таблица подчертава някои, но не всички аспекти на организационните структури.

***Таблица 1.2****:* Организационни структури *в САП.*



Модула за финанси съдържа **сметкоплан**, който изброява всички сметки и се основава на счетоводни правила, определени от държавата. Следва **компания**, на чието ниво могат да се създават индивидуални финансови отчети. По-долу са **фирмените кодове**. Една компания може да има множество кодове и всеки фирмен код може да има **множество бизнес области**. Пример за бизнес област в рамките на фирмен код би било **производство**.

При продажбите и дистрибуцията **търговската организация** е на най-високо ниво и цялото отчитане на продажбените дейности се извършва на ниво търговска организация. След това е **каналът за дистрибуция**, представляващ начин, по който се достига до клиентите. Следващият компонент е **дивизия**, която обработва конкретна продуктова линия. Една компания може да има едно подразделение, което продава потребителски продукти и отделно подразделение за консултантски услуги. Комбинацията от търговска организация, дистрибуционен канал и подразделение се нарича **търговска зона**.

На първо ниво в модула за управление на материалите стои **заводът**. Той може да бъде производствено съоръжение, дистрибуторски център или дори офис. **Местата за съхранение** в заводите са физическите места, където се складират запасите. **Организациите за закупуване** водят преговори и дейности по доставки от доставчици. Организациите за закупуване могат да се справят с доставките за множество фирмени кодове или могат да бъдат ограничени и да извършват покупките за конкретен завод. **Организациите за покупки** често се разделят на групи за покупки, които се занимават със специфични аспекти, като специфични материали в рамките на процеса на закупуване.

В управлението на човешките ресурси отново срещаме **фирмен код**, който е собствена независима счетоводна единица. **Персоналните области** стоят в рамките на фирмения код, като те самите се разделят на **подобласти**. Организационните структури определят взаимоотношенията между различните работни групи и отдели. Те биват конфигурирани първоначално и обикновено остават статични, освен ако дадена компания не придобие друга или се откаже от части от своя бизнес.

Фокусът на дисертацията е върху модула за продажби и дистрибуция. Цялата функция на този модул е да „продава стоки и услуги на клиентите на предприятието“. Основен обект на модула за продажби и дистрибуция е „материал“. Той може да се закупи, произведе, продаде, върне и/или прехвърли. Фигура 1.1. представя данните, които са част от този запис: продажби и логистика, количества за материали и доставки и други:



***Фигура 1.1****: Данни, част от записа за материал в модул за продажби и дистрибуция.*

Вторият най-критичен обект от гледна точка на продажбите и дистрибуцията е главният запис на клиента. Той представлява субект, на който се продават стоки и/или услуги. Част от атрибутите на запис на клиент са: името и адреса на клиента, условия на плащане, специфични опции за ценообразуване, които може да се прилагат само за този клиент, както и различните партньорски функции. ERP системите поддържат няколко версии на клиент. Първата партньорска функция представлява субектът, на който продаваме стоки и услуги (sold‑to party). Партньор за доставка (sold‑to partner) представлява мястото, където изпращаме стоки или услуги. С други думи, това е адреса за доставка на клиента, който може да е различен от адреса на купувача. Партньорът за фактуриране представя къде трябва да бъде изпратена фактура. Местоположението, на което се изпращат фактури, може отново да бъде напълно различно от това на адреса за доставка. Функцията партньор на платеца представлява субектът, който отговаря за плащането на фактура. В много случаи и четирите функции може да имат едни и същи данни, но в някои случаи тези четири функции са не само различни физически адреси, но и напълно различни обекти. Фигура 1.2. илюстрира на кратко четирите вида:



***Фигура 1.2****: Видове партньорски функции.*

Ценообразуването в SAP е свързано с различни видове условия. Всеки тип условие се свързва с различен тип цена. Например, цената на артикул, е цената, която е публикувана в продуктовия каталог. Възможно е обаче да има специфична за клиент цена. В SAP тези настройки се поддържат като отделен тип условие. Типа състояние позволява да се поддържа ценообразуване на различни нива. Например, каталожна цена за един материал, е различна в зависимост от това къде се доставя материала. Това се определя, когато се настройва ценовия запис в този тип условие. SAP разполага с отчети за цените. Те позволяват сравняване и анализиране на всякакви ценови условия въз основа на всяка комбинация от критерии. Това е инструмент, който позволява да се анализира всяко поддържано ценообразуване. Таксите са друг вид запис на условие, който трябва да бъде създаден. Ако ценообразуването, което влиза в договорената позиция, не е очакваното ценообразуване, тогава техника за отстраняване на неизправности е анализа чрез доклад на цените. Следната фигура показва пример за такъв доклад.



***Фигура 1.3****: Примерен доклад за цените.*

Фигура 1.8. представя примерен документ на поръчка за продажба.



***Фигура 1.8****: Примерен документ на поръчка за продажба.*

Притежава три секции: заглавна част, секция за общ преглед на артикула и секция с подробности. Има стандартни типове поръчки, които са налични по подразбиране. Най-често срещаният е стандартният запис. Този тип поръчка се използва за продажба на действителни стоки на клиент. Следва тип поръчка за връщане. Това е точно обратното на стандартна поръчка. В този случай се връща инвентар от клиент обратно в склада, по някаква причина. Може да е дефект или грешен продукт, но в края на краищата причината е без значение, по важното е дали връщането е разрешено или не. Те обикновено са обвързани с възстановяване на сумата обратно на клиента. Други типове документи, като дебитни и кредитни известия, са техническа част от модула Продажби и дистрибуция, но тези типове поръчки всъщност не влияят върху инвентара. Въздействието, което тези видове поръчки имат, е върху счетоводните книги. В този случай клиентът бива таксуван или кредитиран. SAP поддържа създаването на персонализирани типове поръчки. Те започват с буквата Z. Такива примери могат да бъдат групова поръчка или тип безплатна поръчка.

SD се интегрира към модула за управление на материалите, за да провери дали има наличен инвентар за количеството на поръчка. Ако е така, той бива разпределен автоматично. Тази функция се нарича проверка на наличността. Друга важна концепция на SD модула са „изчерпаните поръчки“. Това означава, че има повече поръчки, отколкото инвентар. Разпределянето на инвентара се случва на принципа: първи дошъл, първи обслужен. Това означава, че първата поръчка, създадена в системата, ще получи първа наличност в инвентара. Ако инвентара е напълно изчерпан, следващата поръчка, която влиза в системата, се счита за изчерпана поръчка. Проверката на наличността няма да доведе до потвърждение или резервация на инвентар, тъй като наличното количеството е 0. В SAP съществуват поръчки, които могат да бъдат блокирани по различни причини, като например блокирани за преглед, доставка или фактуриране. Също така съществуват и просрочени поръчки, които не са изпратени навреме.

Документа за доставка е транзакционен документ, използван за управление на логистичната страна по процеса на поръчка. Това е дистрибуторската страна на модула за продажби. Документа за доставка позволява да се управляват функциите за опаковане и изпращане. Създаването на доставка за поръчка може да стане чрез ръчен процес, изпълнявайки транзакцията VL01N. Потребителите могат също да създават колективни доставки, като използват транзакцията VL10A. Този метод обикновено се предпочита, тъй като VL10A може да се автоматизира чрез пакетно задание, което да се изпълнява периодично. След като документ за доставка бъде създаден в системата, той автоматично бива свързан с първоначалната поръчка за продажба. Чрез функцията за документооборот, показана на фигура 1.9, може лесно да се види кои доставки са създадени за дадена поръчка. Потокът на документи проследява състоянието, както и навигация за детайлизиране. Ако поръчка има няколко редови позиции, всяка с различна дата на доставка, това води до отделни документи за доставката. Индивидуалните доставки могат да се обработват с транзакцията VL02N, а колективните чрез VL060. Кой метод се използва зависи от това колко доставки се обработват за даден ден, както и с това как са настроени и управлявани физическите процеси. Има транзакции в SAP, които позволят да се консолидират множество доставки до един и същ клиент, обобщено като пратка (shipment). В рамките на пратка можете да се използват и единици за обработка, представляващи гигантски кутии, които опаковат по-малки в една единица, която да се транспортира на палет. Това дава допълнителен слой за проследяване при изпращане на голям микс от продукти. И накрая, възможност за сторниране (премахване на грешка).



***Фигура 1.9****: Екран за дейности на изпращане на поръчка за продажба.*

Документът за фактуриране, който създава финансовите осчетоводявания, свързани с продажбите и разпространението на стоки и услуги. Документът за доставка предоставя функции, които позволяват поръчаните стоки или услуги да бъдат изпратени до клиент. Документът за фактуриране е реалното фактуриране на клиента за тези стоки или услуги. Обикновено тези два документа са свързани. Много рядко се генерира фактура на ниво поръчка, защото таксуването към клиента се случва след предоставяне на стоките. Следната фигура представя примерен документ за фактуриране.



***Фигура 1.10****: Примерен документ на фактура.*

Точно както при създаването на доставка, за създаване на фактури също има два метода: индивидуално чрез транзакция VF01 или колективно чрез VF04. VF04 е предпочитан, защото може да се изпълнява автоматично, търсейки всички документи за доставка, които са били обработени през деня. Фактурите са свързани с документ за доставка, тя с поръчка. Тези връзки са видими през документния поток. Фигура 1.11 показва връзките между документите. Подобно на доставките в т.н. пратки, фактурите могат да бъдат консолидирани в т.н. месечно извлечение. SAP може да съхранява всички фактури до определен етап, например в края на месеца, и след това да ги комбинира в едно извлечение. Това извлечение е документът за изпращане към клиента. Заявката VF05 позволява търсене на фактури по платец, материал или по организационната структура. В счетоводния изглед се намират публикациите на главната книга, които показват връзката между приходите и себестойността на продадените стоки. След изпращане на фактурата към клиент се очаква и плащане, което се прилага към фактуриране. Продажбите и дистрибуцията продължават до момента на създаване на фактура. Всичко след това попада във финансовия модул.



***Фигура 1.11****: Връзки между документите на поръчка, доставка и фактура.*

### 1.1.2. Характеристика на управлението на веригата за доставки

Управлението на веригата за доставки представлява надзора над информацията за материалите и финансите, докато те се движат в процеса от производител до потребител. Състои се от взаимосвързани мрежи, канали и предприятия, комбинирани в предоставянето на продукти и услуги, изисквани от крайния клиент. Практиката за управление на веригата за доставки черпи до голяма степен от областите на индустриалното, системното инженерство, управлението на операциите, логистиката, информационните технологии. Ролята на този модел е насочена към продажбата на продукти, увеличаване на производителността, ефективността, навременността, намаляване на разходите за преработване.

ERP системите дават възможност за комуникация с доставчици и клиенти, по начин, чрез който обменяме информация, подобряваща преминаването на материали, консумативи и услуги. Тази взаимосвързаност бива разгледана от гледна точка на клиентското обслужване. Управлението на веригата за доставки се дефинира като проектиране, планиране, изпълнение, контрол, наблюдение на дейностите по веригата за доставки с цел създаване на нетна стойност, изграждане на конкурентна инфраструктура, използване на световната логистика, синхронизиране на предлагането с търсенето и измерване на производителността в световен мащаб. Глобалните компании се стремят към пазари, където имат предимството както с доставките, така и с клиентите. Разглеждайки предлагането с търсенето, осигурявайки поток от информация, който определя, в кой момент трябват повече запаси или например кои продукти трябва да биват предлагани в определен момент. Интегрираното планиране и изпълнение на процеса, необходим за оптимизиране на потока от материали, информация и финансов капитал, включва планиране на търсенето, снабдяване, производство, управление на запасите и съхранение, транспортиране или логистика, връщане на излишни или дефектни продукти.

Управление на веригата за доставки се използва за да осигуряване на непрекъснато снабдяване, управление на договорните задължения и предотвратяване на прекъсвания в доставките. Също така управление на риска, спазването на организационните разпоредби и споразумения. В зависимост от естеството на бизнеса, трябва да се спазват индустриални и правителствени изисквания, да се извличат анализи на поръчките.

Управление на веригата за доставки служи за увеличаване на печалбата, увеличаване на паричния поток, подобряване обслужването на клиентите, намаляване на оперативните разходи, подобряване на финансовите позиции.

За планиране на търсенето, приемаме търсенето от клиента, поддържано в ERP системите. Също така помагат в планирането за производство или снабдяване с материали, транспорта и логистиката. Тези модули помагат за изграждането на веригата. SD, MM, PP съдържат тези градивни елементи. Анализирането на информацията идваща от ERP, в частност взаимоотношенията с клиенти и доставчици, полага добра основа за изграждането на персоналната верига за доставки. Тъй като процесът е сложен, ERP не поддържа такъв подмодул по подразбиране. В случая разглеждането на информацията предпоставя изготвянето на стратегия и план. Веригата за доставки започва с управлението на материалите, включва логистично изпълнение и производствено планиране.

Както беше споменато в точка 1.1.1, логистичния модул, поддържащ оферти, обработката на поръчки, доставки и транспорт. Свързани с веригата за доставки, прогнозите за продажбите са основно разбиране какво биха поискали клиентите в бъдеще. Тази прогноза бива въведена в производственото планиране. Друг аспект на логистичния модул е функционалността за доставки към клиенти. Логистичното изпълнение, като част от модула за управление на материалите, е мястото, където ще открием нашите складови операции. Ключов момент в логистиката са трансферите до местата за съхранение, при постъпване на материалите. Планирането на производството е друг подмодул в рамките на логистиката. Използва се за създаване на графици за производство и доставки за готов продукт и компонентни материали.

На фигура е представен модел, показващ потока от информация по отношение на търсенето чрез реалното издаване на готовите материали за клиент. Основните данни са част от почти цялата ERP: материали, доставчици, клиенти се създават под формата на **вътрешни,** основни записи. Фигурата илюстрира търсене от MRP, ( клиенти, които имат нужда от определено количество продукт). От гледна точка на MRP, това е планиране на изискванията за материали. Ако разполагаме с продукта или услугата, можем да го изпратим директно на клиента. В противен случай трябва да изпратим вътрешна предложение за закупуване на материал. След като бъде одобрено, материалът бива получен в инвентар. Ако компанията има на склад, този материал се премества там. Ако част от процес подлежи на инспекция, се насочваме към модула за управление на качеството, където, след като материалите бъдат инспектирани, те се освобождават за неограничена употреба. Въз основа на поръчките, материалите биват издадени и след това започва изходящия логистичен процес. 

***Фиг 1.5****: Принципи за проектиране на облачни системи.*

## 1.2. Възможности за дигитализация на процесите по управление чрез прилагане на облачни технологии

В последните години облачните технологии се превърнаха във водеща тенденция в софтуерната индустрия. Те предоставят нов начин за изграждане на големи и сложни системи, като по този начин използват пълноценно съвременните практики за разработка на високо-качествен софтуер и налична инфраструктура. Това променя начина на проектиране, интегриране и внедряване на системите. Облачно базираните решения са проектирани да приемат бързо промените, да обслужват голям мащаб от хора и да бъдат устойчиви на всякакъв вид натоварване или хакерски атаки (Vettor, 2022).

Организацията Cloud Native Computing Foundation предлага следното определение: "*Технологиите, базирани на облак, дават възможност на организациите да създават и изпълняват приложения в модерни, динамични среди като публични, частни и хибридни облаци, чрез мрежи от услуги и микроуслуги. Качества на системите са устойчивост, висока наличност и достъпност, мащабируемост и управляемост, които са от критично значение за много от бизнес единиците. Автоматизацията на тези процеси позволява на инженерите да правят промени, с голямо въздействие, но с минимални усилия."*

Приложенията стават все по-сложни, като изискванията, от страна на потребителите, стават все повече и повече, главно насочени към бърза реакция и иновативни функции. Проблеми с производителността или повтарящи се грешки вече не са приемливи.

Предимствата на облачните системи поставят бизнеса една стъпка пред конкурентите. Бизнес системите се развиват от способностите на бизнеса да бъдат инструменти за стратегическа трансформация, която ускорява растежа на компанията. Облачно базираните системи се свързват главно с бързина (Smith, 2022). Незабавното пускане на иновативните идеи на пазара е важна тема за всички модерни  компании, например следните компании са приложили успешно тези техники:

• Netflix има над 600 услуги в производствена среда. Стотици пъти на ден се изпълняват нови внедрявания и разгръщания на съществуващи;

• Uber има над 1000 услуги в производствена среда. Обновяват се няколко хиляди пъти всяка седмица;

Както е видно, бизнесът на тези две компании се базира на системи, които се състоят от стотици независими микроуслуги. Този архитектурен стил им позволява бързо да реагират на пазарните условия като постоянно актуализират малки, но важни области. Скоростта на облачния носител се дължат на редица фактори, като на първо място е инфраструктурата на изчислителните ресурси.

На фигура 1.3. са показани пет основополагащи стълба, осигуряващи основата за базирани в облак системи.



***Фиг 1.6****: Фундаментни стълбове на облачните системи.*

Проектирани да процъфтяват в динамична, виртуализирана облачна среда, облачните системи използват широко „платформата като услуга“ (PaaS) изчислителна инфраструктура и управлявани услуги. Те третират основната инфраструктура като за еднократна употреба - осигуряват се за минути и се преоразмеряват, мащабират или унищожават при поискване - чрез автоматизация.

Нека разгледаме DevOps концепция наречена: „Pets vs. Cattle“ (Menchaca, 2018). В традиционния център за данни сървърите се третират като домашни любимци (pets), като всеки един от тях представлява физическа машина, която трябва да бъде поддържана. Мащабирането се случва като се добавят ресурси към нея. Възникването на проблем в сървър, рефлектира върху всички потребители. Моделът на услугата Cattle е по-различен. При него всеки ресурс се предоставя като виртуална машина или контейнер. Те са идентични и присвояват системни идентификатори като Service-01, Service-02 и т.н. Мащабирането се случва като се създадат нови екземпляри. Ако един от тях стане недостъпен, друг поема неговата роля. Облачните системи поддържат този модел. Те продължават да работят, независимо от машините.

Дванадесетфакторното приложение (Wiggins, A., 2017), представено в таблица 1.2, е известна методология за конструиране на облачно базирани приложения. Изготвена от разработчици в Heroku, компания, преглагаща, платформа като услуга, описва набор от принципи и практики, които разработчиците следват, за да създават приложения, оптимизирани за модерни облачни среди. Много практици смятат Twelve-Factor за солидна основа за изграждане на облачни приложения, защото е приложим за всяко уеб-базирано приложение. Системите, изградени на този принцип, могат да се внедряват и мащабират бързо, както и да добавят нови или да променят съществуващи функции, за да реагират бързо на пазарните промени.

***Таблица 1.6****: Описание на методологията на дванадесетте фактора.*

| **Factor** | **Explanation** |
| --- | --- |
| 1 - Code Base | A single code base for each microservice, stored in its own repository. Tracked with version control, it can deploy to multiple environments (QA, Staging, Production). |
| 2 - Dependencies | Each microservice isolates and packages its own dependencies, embracing changes without impacting the entire system. |
| 3 - Configurations | Configuration information is moved out of the microservice and externalized through a configuration management tool outside of the code. The same deployment can propagate across environments with the correct configuration applied. |
| 4 - Backing Services | Ancillary resources (data stores, caches, message brokers) should be exposed via an addressable URL. Doing so decouples the resource from the application, enabling it to be interchangeable. |
| 5 - Build, Release, Run | Each release must enforce a strict separation across the build, release, and run stages. Each should be tagged with a unique ID and support the ability to roll back. Modern CI/CD systems help fulfill this principle. |
| 6 - Processes | Each microservice should execute in its own process, isolated from other running services. Externalize required state to a backing service such as a distributed cache or data store. |
| 7 - Port Binding | Each microservice should be self-contained with its interfaces and functionality exposed on its own port. Doing so provides isolation from other microservices. |
| 8 - Concurrency | When capacity needs to increase, scale out services horizontally across multiple identical processes (copies) as opposed to scaling-up a single large instance on the most powerful machine available. Develop the application to be concurrent making scaling out in cloud environments seamless. |
| 9 - Disposability | Service instances should be disposable. Favor fast startup to increase scalability opportunities and graceful shutdowns to leave the system in a correct state. Docker containers along with an orchestrator inherently satisfy this requirement. |
| 10 - Dev/Prod Parity | Keep environments across the application lifecycle as similar as possible, avoiding costly shortcuts. Here, the adoption of containers can greatly contribute by promoting the same execution environment. |
| 11 - Logging | Treat logs generated by microservices as event streams. Process them with an event aggregator. Propagate log data to data-mining/log management tools like Azure Monitor or Splunk and eventually to long-term archival. |
| 12 - Admin Processes | Run administrative/management tasks, such as data cleanup or computing analytics, as one-off processes. Use independent tools to invoke these tasks from the production environment, but separately from the application. |

В книгата Beyond the Twelve-Factor App авторът Кевин Хофман описва подробно всеки от оригиналните 12 фактора, като добавя три допълнителни, които отразяват модерен дизайн на облачни приложения.

***Таблица 1.7****:ТОДО.*

| **New Factor** | **Explanation** |
| --- | --- |
| 13 - API First | Make everything a service. Assume your code will be consumed by a front-end client, gateway, or another service. |
| 14 - Telemetry | On a workstation, you have deep visibility into your application and its behavior. In the cloud, you don't. Make sure your design includes the collection of monitoring, domain-specific, and health/system data. |
| 15 - Authentication/ Authorization | Implement identity from the start. Consider [RBAC (role-based access control)](https://learn.microsoft.com/en-us/azure/role-based-access-control/overview) features available in public clouds. |

Проектирането и внедряването на облачно базирани работни натоварвания може да бъде предизвикателство. Microsoft Well-Architected Framework (Stanford D. et al, 2022) предоставя набор от ръководни принципи, които се използват за подобряване качеството на работното натоварване. Следната таблица представя пет важни стълба на добра архитектурата.

***Таблица 1.8****: Стандартни за добри практики на облачаната индустрията.*

| **Tenets** | **Description** |
| --- | --- |
| [Cost management](https://learn.microsoft.com/en-us/azure/architecture/framework/#cost-optimization) | Focus on generating incremental value early. Apply Build-Measure-Learn principles to accelerate time to market while avoiding capital-intensive solutions. Using a pay-as-you-go strategy, invest as you scale out, rather than delivering a large investment up front. |
| [Operational excellence](https://learn.microsoft.com/en-us/azure/architecture/framework/#operational-excellence) | Automate the environment and operations to increase speed and reduce human error. Roll problem updates back or forward quickly. Implement monitoring and diagnostics from the start. |
| [Performance efficiency](https://learn.microsoft.com/en-us/azure/architecture/framework/#performance-efficiency) | Efficiently meet demands placed on your workloads. Favor horizontal scaling (scaling out) and design it into your systems. Continually conduct performance and load testing to identify potential bottlenecks. |
| [Reliability](https://learn.microsoft.com/en-us/azure/architecture/framework/#reliability) | Build workloads that are both resilient and available. Resiliency enables workloads to recover from failures and continue functioning. Availability ensures users access to your workload at all times. Design applications to expect failures and recover from them. |
| [Security](https://learn.microsoft.com/en-us/azure/architecture/framework/#security) | Implement security across the entire lifecycle of an application, from design and implementation to deployment and operations. Pay close attention to identity management, infrastructure access, application security, and data sovereignty and encryption. |

Облачните системи поддържат ориентирания към микроуслуги архитектурен стил за конструиране на системи. Това е подход за изграждане на сървърно приложение като набор от малки, но високо-качествени подуслуги. Съотвено, клиентите, на сървърните услуги, могат да бъдат отделни приложения, които да се поддържат и управляват самостоятелно. Всяка услуга работи в собствен процес и комуникира с други процеси, използвайки различен тип и вид протоколи като: HTTP/HTTPS, WebSockets, AMQP и мн други. Всеки микросървис притежава специфична бизнес способност. Предимства на това архитектурен стил са:

• Всяка микроуслуга може да бъде проектирана, разработена и внедрена независимо една от друга, което осигурява възможно за независима работа по отделни области на приложението;

• Работата може да бъде дистрибутирана между отделни екипи;

• Проблемите са по-изолирани;

• Позволява използването на различни технологии;

Микроуслугите насърчават фактор #6 от принципите на дванадесетфакторното приложение.

…….

***Таблица 2.2****: Принципи за проектиране на облачни системи.*

|  |  |  |
| --- | --- | --- |
| име на български | име на английски | Описание (тук ще има доста цитати) |
| Разделяне на грижите | Separation of Concerns | всеки обект и модул трябва да бъде в своя собствена грижа и контекст |
| Капсулиране | Encapsulation |  |
| Инверсия на зависимостта | Dependency Inversion |  |
| Изрични компоненти | Explicit Components |  |
| Единична отговорност | Single Responsibility |  |
| Не се повтаряйте | Don’t Repeat Yourself |  |
| Устойчивост и невежество относно инфраструктурата | Presentation Ignorance |  |
| Ограничени контексти | Bounded Contexts |  |

Всяка микроуслуга притежава своя собствена логика и данни, в рамките на автономен жизнен цикъл. Концептуалните модели се различават между подсистемите или микроуслугите. Този принцип е заложен в дизайнът, управляван от домейн (DDD), където всяка услуга притежава свой модел на домейн (данни плюс логика и поведение).

Традиционният (монолитен) подход, използван в много приложения, притежава единична централизирана база данни (или няколко бази), която често е нормализирана SQL база, използвана за цялото приложение и всички негови вътрешни подсистеми. Този подходът изглежда по-прост, позволява повторно използване на обекти. В крайна сметка се стига до огромни таблици, които обслужват много различни подсистеми, включващи атрибути и колони, които в повечето случаи не са необходими. Монолитните приложения: ACID транзакции и SQL език, като и двете работят във всички таблици и данни, свързани с приложението. Това допринася за сравнително лесно комбиниране данни от множество таблици.

Достъпът до данни, става много по-сложен в архитектурата на микроуслуги. Дори когато използвате ACID транзакции в рамките на микроуслуга или ограничен контекст, е изключително важно да се има предвид, че данните, притежавани от всяка микроуслуга, са частни за тази и трябва да бъдат достъпвани синхронно, чрез нейните API крайни точки (REST, gRPC, SOAP и т.н.) или асинхронно чрез съобщения (AMQP). Капсулирането на данните гарантира, че микроуслугите са слабо свързани и могат да се развиват независимо една от друга. Ако множество услуги имат достъп до едни и същи бази данни, актуализациите на схемата ще изискват координация. Това би нарушило автономността на жизнения цикъл. Когато един бизнес процес обхваща множество микроуслуги трябва се да използва т.н. „евентуална последователност“. Това е много по-трудно за изпълнение от обикновените SQL съединения. Различните микроуслуги често използват различни видове бази данни. Съвременните приложения съхраняват и обработват различни видове данни. За някои случаи на употреба NoSQL база данни като Azure CosmosDB или MongoDB може да има по-удобен модел, както и да предлага по-добра производителност и мащабируемост от SQL база данни. Микроуслугите често използват смесица от SQL и NoSQL бази данни, което се нарича подход на „полиглотна устойчивост“ (Polyglot Persistence).

Концепцията за микроуслуга произлиза от модела на ограничен контекст (Bounded Context) в управлявания от домейн дизайн (DDD). DDD се занимава с големи модели, като ги разделя на множество BC и определя техните граници. Всеки BC има собствен модел и база данни. По същия начин всяка микроуслуга притежава свързаните с нея данни. В допълнение, BC притежават така нареченият повсеместен език, който помага на комуникацията между разработчици на софтуер и експерти в бизнеса. Ограничен контекст може да бъде отделна услуга или е просто логическа граница.

Предизвикателства и решения за управление на разпределени данни

Определянето на границите на микросервиз основно предизвикателство, което съсредоточава върху логическите модели на приложението и свързаните с него данни. Всеки контекст може да има различни бизнес термини. Термините и обектите, може да звучат подобно, но понякога имат различни цели в различни контексти. Например, даден потребител може да бъде посочен като потребител на системата, като клиент в контекста на ERP и т.н. Начинът, по който се идентифицират границите между множество контексти на приложения с различен домейн, е сходен с начина за ограничаване границите за всяка бизнес микроуслуга. Зависимостите между микроуслугите трябва да е сведена до минимум.

## 1.3. Специфики при управление на поръчките от клиенти в производствено предприятие

Софтуерните приложения трябва да имат познание за потребителя или процеса, който ги извиква. Потребителят или процесът, взаимодействащ с приложение, е известен като принципал за сигурност, а процесът на удостоверяване и упълномощаване на тези принципали е известен като управление на самоличността (Vettor, 2022). Простите приложения могат да включват цялото им управление на самоличността в приложението, но този подход не се мащабира добре с много приложения и много видове принципали за сигурност. Windows, например, поддържа използването на Active Directory за предоставяне на централизирано удостоверяване и оторизация. Въпреки че това решение е ефективно в рамките на корпоративни мрежи, то не е предназначено за използване от потребители или приложения, които са извън домейна.

Удостоверяването е процес на определяне на самоличността на потребител. Упълномощаването е актът на предоставяне на удостоверено разрешение за извършване на действие или достъп до ресурс (Wike R, 2022).

Съвременните решения за самоличност обикновено използват токени за достъп, които се издават от защитена услуга/сървър (STS) на принципал за сигурност, след като тяхната самоличност бъде определена (Anil N, 2022).

Удостоверяването чрез токени е механизъм без състояние, тъй като никаква информация за потребителя не се съхранява в паметта на сървъра или базaтa от данни, за разлика от бисквитките (Gichuhi , 2021).

Стандарт (RFC 7519) за уеб приложенията е JSON уеб токен (JWT). Той се състои от три части:

• Заглавна - JSON обект, кодиран във формат base64. Съдържа информация за типа на токена и алгоритъма за криптиране;

• Полезен товар - съдържа информация за текущия потребител (потребителско име, роля и др). Тук не трябва да се включват чувствителни данни, защотп лесно се могат да бъдат декодирани със публични сайтове като jwt.io;

• Подпис – Използва се от сървъра, за да провери дали токенът е валиден. Той се генерира чрез комбиниране на двете части (заглавна и полезен товар) заедно. Базира се на таен ключ, който само сървърът за удостоверяване знае. По този начин злонамерен потребител не може да фалшифицира валиден токен;

Мобилни и базирани на JavaScript приложения се изпълняват на ниво клиент. Те трябва да комуникират с публичен API, което означава че не може да се използва защита като VPN. Изпращането на потребителско име и парола (Basic Authentication) при всяка заявка от клиент към API е лоша идея, защото например с анализатор на мрежови протоколи, има вероятност някои да проследи паролата и така да получи достъп до много информация.

Вместо да се изпраща комбинацията от потребителско име и парола при всяко повикване към API, се използват токени. Те представляват съгласие, например съгласие, дадено от потребителя за достъп. Токените се издават от централен компонент за решаване на общи задачи, свързани с идентичността. Отговорност на доставчика на самоличност е да удостовери потребител и безопасно да предостави доказателство на приложение. Често, доставчика на самоличност е и портал към задачи, свързани с потребителя и управлението на акаунта.

Регистрация на потребители, управление на акаунти, прилагане на политики за пароли с правила за силата, блокиране на потребители и т.н. са задачи към подсистемата за управление на идентичност и достъп. Тя позволява съвместимo използване в различни приложения, както и възможност цялата система да бъде тествана за пробив (penetration test). Важна функционалност е многофакторното удостоверяване, при което потребителят трябва да предостави допълнителна информация (освен име и парола), за да докаже своята самоличност, като например цифров пропуск, издаден от смартфон, който има приложение за удостоверяване.

OAuth2 е отворен протокол, който позволява сигурно оторизиране по стандартен метод от уеб, мобилни и настолни приложения. OAuth2 дефинира токен, който може да бъде поискан от клиентско приложение за да получи достъп до API, като го предаде по HTTP. OAuth определя крайни точки за оторизация, дефинирани по стандарт, като също така посочва как да бъдат използвани от различни типове приложения.

Следната таблица представя различни доставчици на самоличност които прилагат OAuth2.

|  |  |
| --- | --- |
| Okta |  |
| Ping |  |
| Trust Builder |  |
| Identity Server |  |

OpenID Connect е слой за идентичност, разширяващ, прилагащ принципите на OAuth2, който помага на приложенията да получат токен за самоличност/достъп. Той се използва за влизане в клиентско приложение, докато същото приложение използва токена за достъп до API.

Фигура 1.11. илюстрира комуникацията за получаване на токен.



***Фигура 1.11****: Схема на OpenID Connect.*

Създава се заявка от клиентското приложение, което пренасочва потребителя към доставчика на самоличност, където потребителят доказва кой е, чрез предоставяне на потребителско име (или например имейл, телефонен номер) и парола. Това действие може да е познато от влизане в сайт чрез Google или Microsoft. Това е началото на OpenID Connect потока. В крайна сметка доставчикът на самоличност създава токен, подписва го и го връща на клиентското приложение. Така то има доказателство за самоличност. OpenID Connect е проектиран да работи за различни видове приложения (уеб приложения от страна на сървъра или от страна на клиента, мобилни приложения, уеб услуги и др.), като дефинира типове клиенти и потоци.

Има два дефинирани типа клиенти: поверителни и публични клиенти. Поверителният клиент в състояние да запази поверителност на идентификационните си данни, които са клиентски идентификатор и тайна. Това не са идентификационните данни на потребителя. В OpenID Connect може да се удостовери както потребител, така и самото клиентско приложение. Идентификационните данни се съхраняват на ниво приложение, като например ASP.NET Core MVC уеб приложение, което работи на уеб сървър. Тъй като това приложение работи на сървъра, то може безопасно да съхранява идентификационните си данни, тъй като не са достъпни от потребителя. Публичните клиенти не са в състояние да запазят поверителност, тъй като изпълнението на програмата е в браузъра или на мобилно устройство, на ниво потребител. „Тайна“, съхранена в JavaScript или на мобилно устройство, не е тайна. Винаги е достъпна. В частност мобилните операционни системи позволяват използването на хардуерни API за безопасно съхраняване на тайни, но все още се считат за публични клиенти, поради факта, че тайната се съхранява на устройството.

Потокът в OpenID определя как кодът и/или токените се връщат на клиента. В случая разглеждате поток като редица заявки и отговори, често между клиентските приложения и доставчика на идентичност. Пример за такъв поток е сайт, който предлага опция за влизане с акаунт от Microsoft или Google. Браузър пренасочва към сайт, където се предоставя потребителско име и парола. След това се пренасочва обратно към основния сайт. В повечето от тези потоци има набор от заявки и отговори, които се случват, без да бъдат визуализирани от браузъра. OpenID потока се определя в зависимост от изискванията на клиента.

Заявките за оторизация се изпращат до крайна точка на ниво доставчик на идентичност. Тази крайна точка се използва от клиентското приложение за получаване на удостоверяване за токени за самоличност и/или оторизация за токени за достъп от потребителя. Това става чрез пренасочване на клиентското приложение към доставчика на идентичност. Код за оторизация или токен могат да бъдат върнати към клиентското приложение. TLS (SSL) е изискване за OpenID Connect, трафикът трябва да винаги е криптиран. Липсата на криптиран трафик прави потока уязвим към атаки от тип „човек по средата“.

Крайна точка за пренасочване е URI адресът, към който IDP пренасочва обратно клиента. Той е на ниво клиентско приложение и се използва от доставчика на идентичност, за да достави кода за оторизация или токен на клиентското приложение.

Крайна точка за токен е на ниво доставчик на идентичност. Клиентските приложения могат програмно да изискат токени. Обикновено става без пренасочване чрез методът HTTP POST. Повикванията могат да бъдат удостоверени с идентификатор и тайна за поверителните клиенти.

Както за поверителни, така и за публични клиенти се препоръчва използването на вариации на потока „Кода за оторизация“ (Authorization Code Flow) подплатен с PKCE защита (OAuth 2.0 Security Best Current Practice RFC / <https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics-19>). Потокът „код за оторизация“ получава името си от факта, че започва с код за оторизация. Този код за оторизация може да се разгледа като краткотраен идентификационен номер за еднократна употреба, който се използва за проверка дали влезлият на ниво доставчик на идентичност е същият, който е започнал на ниво клиентско приложение. Този поток позволява дълготраен достъп за поверителни клиенти, но за публичните е ограничен. Разрешена е вариация на токен за опресняване. Изборът на правилен вариант на поток е важен, защото може да доведе до уязвимости в сигурността. Технически, много от подходите ще работят, но повечето ще доведат до сериозен риск.

Всеки OpenID Connect поток започва със заявка към крайната точка за оторизация. Пример за URI е представен на следната фигура.



***Фигура 1.12****: URI for the authentication code flow endpoint.*

На първо място е самата крайна точка на ниво IDP. След това са идентификаторът на клиентското приложение (client\_id), URI за пренасочване. Това е URI на ниво клиентско приложение, до което ще бъде доставен отговорът от заявката за оторизация. В случая, зададения обхват показва, че приложението изисква достъп до и до идентификатора на потребителя (openid) и твърденията, свързани с профила, като собствено име и фамилия. След това е стойността на типа отговор (response\_type), която определя потока, който се използва. Стойностите, зададени като response\_type, са нещата или токените, върнати от доставчика на идентичност към клиента, чрез пренасочване от браузъра. Фигура 1.13 представа модела на този поток.



***Фигура 1.12****: authentication code flow model.*

Уеб приложение създава и изпраща заявка за удостоверяване с код. На ниво IDP потребителят предоставя комбинация от потребителско име и парола. В този момент доставчикът на самоличност знае кой е потребителят. Клиентското приложение все още не. Доставчикът на самоличност по избор иска съгласие от потребителя, като например да изиска разрешение за получаване на достъп до информацията от профила. След това доставчикът на самоличност изпраща обратно към уеб приложението чрез URI пренасочване или POST формуляр. Това е комуникация, която е видима за браузъра. Кода за оторизация може да се разглежда като много краткотраен токен, който е доказателство за удостоверяване. Той е свързан с потребителя, който току-що е влязъл в доставчика на самоличност. В следващата стъпка уеб клиентът извиква крайната точка за токен. Тази заявка не използва пренасочване и следователно не е видима за браузъра. Това е HTTP заявка от сървър към сървър, към която се предава кода за оторизация и комбинация от clientid и clientsecret. Доставчикът на самоличност генерира токен и го връща на клиента в HTTP отговора. На ниво клиент токенът се валидира и извлича идентификатора на потребителя.