*1. Parašykite kokį architektūrinį stilių ar stilius pasirinksite Vaizdo apdorojimo posistemiui ir kodėl. Aprašykite esminį pasirinktą architektūrinį stilių, detalizuokite jo privalumus ir trūkumus.*

**Vamzdeliai ir filtriukai** (Pipes and filters), nes ši architektūra yra tinkamiausia, kai reikia daug duomenų apdorojimo operacijų. Į tai įeina ir video apdorojimas. Ši architektūra yra lanksti, į apdorojimo grandinėlę vėliau nesunkiai galima įterpti naujų apdorojimo metodų.

Architektūrinio stiliaus privalumai:

* Lankstus (grandinėlės detalių keitimas)
* Tinka duomenų apdorojimo operacijoms
* Galima lygiagretinti
* Tinkamas daugkartiniam naudojimui

Trūkumai:

* Kiekvienas grandinėlės elementas reikalauja tam tikros duomenų struktūros, todėl gali būti sunkiau detales apkeisti vietom
* Tinka tik informacijos apdorojimo srautams
* Netinka kai sistemos yra interaktyvios

*2. Parašykite kokį architektūrinį stilių ar stilius pasirinksite  Sąveikos posistemiui ir kodėl. Aprašykite esminį pasirinktą architektūrinį stilių, detalizuokite jo privalumus ir trūkumus.*

**Mikroservisų** (micro-services) architektūra, nes ji leistų kiekvienai norimai implementuoti sistemai dirbti autonomiškai. Kiekviena sistema turi savo duomenų bazę ir funkcionuoja savarankiškai - nulūžus vienai sistemai, kitos dar veiktų. Ši architektūra leistų vartotojams pasiekti šias funkcijas iš įvairių įrenginių ir ji yra labai lengvai plečiama.

Mikroservisų architektūros privalumai:

* Kiekvienas servisas yra atskira programa, kuri turi savo duomenų bazę
* Nulūžus vienam servisui, kiti dar veiktų
* Kadangi galima servisus kurti su atskiromis duombazėmis, derinimo laiko lieka mažiau
* Programa yra išskaidyta į komponentus, todėl lengvai plečiama

Mikroservisų architektūros trūkumai:

* Sudėtinga paslaugas susieti tarpusavyje
* Sudėtingas keitimasis informacija ir įvykiais

*3. Padėkite kompanijai pasirinkti  Transliavimo posistemio architektūrinį stilių- aprašykite abiejų architektūrinių stilių privalumus ir trūkumus susijusius su duota situacija.*

Kompanijai tiktų **Client-Server** - centralizuojame visą sistemą, todėl ją nesudėtinga valdyti, lengva užtikrinti saugumą, tačiau šią architektūrą reikia realizuoti tinkamai, nes jos silpnybė yra - vienintelis lūžio taškas. Nulūžus centrinei daliai, sulūžtų ir visa sistema.

Client-Server privalumai:

* Centralizuota sistema - lengva valdyti
* Nesudėtinga palaikyti saugumą

Client-Server trūkumai:

* Yra vienintelis lūžio taškas - nulūžus internetui, sulūžtų visa sistema
* Gali neatlaikyti didelių apkrovų

**Peer-to-peer**, labiau tinka kai sistemoms reikia dalintis bendra, dažna informacija, įvykiais ir resursų reikalavimais.

Peer-to-peer privalumai:

* Paskirsto darbus ir apkrovą tarp peers
* Gerai daug resursų reikalaujančioms sistemoms

Peer-to-peer trūkumai:

* Netinka jei informacija negali būti siunčiama tarp serverių
* Programų dydis turi būti prižiūrimas
* Sudėtinga palaikyti saugią
* Atskirų peers nekontroliuojame

*1. Parašykite į kokias fundamentalias savybes (fundamental security dimensions/properties) reikia atsižvelgti kuriant sistemą.*

* **Konfidencialumas** (Confidentiality) - Ar informacijos nepasiekia žmonės ar programos, kurioms neleista tos informacijos pasiekti
* **Vientisumas** (Integrity) - Ar kažkas išoriškai nepakeitė duomenų, ar jie dar patikimi
* **Pasiekiamumas** (Availability) - Sistema turi dirbti kai jos reikia

*2.Parašykite į kokius  grėsmių saugumui  tipus  (fundamental  threat types) reikia atsižvelgti kuriant sistemą.*

* **Perėmimas** (Interception) - informacijos nutekinimas
* **Pertraukimas** (Interruption) - padaro dalį sistemos nepasiekiamą
* **Modifikavimas** (Modification) - pakeičiami gauti duomenys ar pranešimai ir vėl išsiunčiami
* **Sufabrikavimas** (Fabrication) - pagaminama netikra informacija ir ji persiunčiama

*3. Koks  architektūrinis stilius rekomenduojamas, kuriant į saugumą orientuotas sistemas ir kodėl?*

**Sluoksniuota architektūra**, nes visos dalys yra atskirtos, kiekviename lygyje galima pridėti saugumo tikrinimus, tai neleistų atakoms prasiskverbti pro visus sluoksnius.

*4. Kaip bus užtikrinamas sistemos saugumas (security assurance)?*

* **Pažeidžiamumo vengimas** (Vulnerability avoidance) - programavimo technikų ar sistemų taikymas, kad išvengti atakos
* **Atakų aptikimas ir eliminavimas** (Attack detection and elimination) - antivirusinės sistemos (atakos pašalinimas jai pasirodžius)
* **Žalos ribojimas ir sugebėjimas atsistatyti** (Exposure limitation and recovery) - pasirinkti ir turėti strategiją ką daryti kai sistema bus nulaužta