

YOPIQ VA OCHIQ AXBOROT TIZIMLARI VA RESURLARINI INTEGRATSIYALASH MODELI

Razzokov Jaloliddin Zaynitdinovich

University of Management and Future Technologies

Telekommunikatsiya injiniringi magistranti.

<https://doi.org/10.5281/zenodo.15348211>

Annotatsiya. Mazkur maqolada yopiq va ochiq axborot tizimlari va resurslarini yagona axborot makonida integratsiyalashning konseptual va amaliy asoslari keng qamrovda tahlil etiladi. Integratsiyalash modeli doirasida axborot almashinuvi, tizimlararo moslashuvchanlik (interoperabilitet), xavfsizlik strategiyalari, huquqiy va axloqiy masalalar, texnik arxitektura hamda standartlashtirish muammolari har tomonlama ko'rib chiqiladi.

Yopiq tizimlarning ishonchlilik va maxfiylik talablari bilan ochiq tizimlarning ochiqlik, innovatsion yondashuv va shaffoflik prinsiplari o'rtasida muvozanatni ta'minlash modelning markaziy vazifasidir. Tahlil davomida SOA (Xizmatga asoslangan arxitektura), API Gateway, ETL texnologiyalari, axborot xavfsizligi protokollari, va mashina-o'qilishi mumkin bo'lgan interfeyslar kabi zamonaviy texnik yechimlar misolida amaliy yondashuvlar yoritiladi. Ushbu maqola ilmiy izlanishlar, davlat va korporativ axborot infratuzilmalari hamda raqamli transformatsiya loyihalari uchun zaruriy nazariy va metodologik asosni shakllantiradi.

Kalit so'zlar: Axborot tizimlari, tizimlararo integratsiya, yopiq resurslar, ochiq platformalar, ma'lumotlar xavfsizligi, API, SOA, qonunchilik, mashina-o'qilishi mumkin bo'lgan interfeyslar.

МОДЕЛЬ ИНТЕГРАЦИИ ЗАКРЫТЫХ И ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И РЕСУРСОВ

Аннотация. В данной статье комплексно рассматриваются теоретические и практические аспекты интеграции закрытых и открытых информационных систем и ресурсов в едином информационном пространстве. Анализ охватывает обмен данными, вопросы совместимости, стратегии информационной безопасности, юридические и этические аспекты, техническую архитектуру и стандартизацию.

Основная задача модели — обеспечить баланс между конфиденциальностью и надежностью закрытых систем и прозрачностью и инновационностью открытых платформ. Особое внимание уделяется современным технологиям, таким как SOA, API Gateway, ETL-процессы, протоколы безопасности и машинно-читаемые интерфейсы. Статья представляет научно обоснованную платформу для цифровых трансформаций в госсекторе и корпоративной сфере.

Ключевые слова: информационные системы, системная интеграция, закрытые ресурсы, открытые платформы, безопасность данных, API, SOA, законодательство, машинно-читаемые интерфейсы

MODEL OF INTEGRATION OF CLOSED AND OPEN INFORMATION SYSTEMS AND RESOURCES

Abstract. This article provides a comprehensive analysis of the conceptual and practical foundations for integrating closed and open information systems and resources within a unified digital ecosystem.

The study addresses key challenges including data exchange mechanisms, interoperability, cybersecurity strategies, legal and ethical constraints, technical architecture, and standardization issues. The integration model focuses on achieving a balance between the confidentiality of closed systems and the transparency and innovation offered by open platforms. Emphasis is placed on modern technological solutions such as Service-Oriented Architecture (SOA), API gateways, ETL tools, security protocols, and machine-readable interfaces. The article offers a robust theoretical and methodological framework for researchers, digital governance architects, and organizations undergoing digital transformation.

Keywords: *information systems, system integration, closed resources, open platforms, data security, APIs, SOA, legislation, machine-readable interfaces.*

Axborot-kommunikatsiya texnologiyalarining jadal sur'atlar bilan rivojlanishi zamonaviy axborot tizimlarini yaratish, boshqarish va ularni samarali integratsiyalashga bo'lgan ehtiyojni keskin oshirmoqda.

Hozirgi zamonda deyarli barcha tashkilot va muassasalar o'z faoliyatida turli axborot tizimlari va platformalardan foydalanmoqda.

Bular orasida **yopiq tizimlar** (masalan, ichki hujjat aylanishi, buxgalteriya, personal boshqaruvi tizimlari) va **ochiq tizimlar** (masalan, veb-saytlar, mobil ilovalar, ochiq ma'lumotlar portallari) muhim o'rin tutadi.

Ushbu tizimlarning har biri o'zining maqsadi, xavfsizlik talablari, texnologik chegaralari va funksional imkoniyatlariga ega.

Zamonaviy boshqaruv, sog'liqni saqlash, ta'lim, logistika, moliya, energetika kabi sohalarda axborot resurslarining optimal ishlatilishini ta'minlash, ularning o'zaro uzviy bog'liqligini tashkil etish orqali yagona raqamli muhitni shakllantirish zarurati tobora ortib bormoqda.

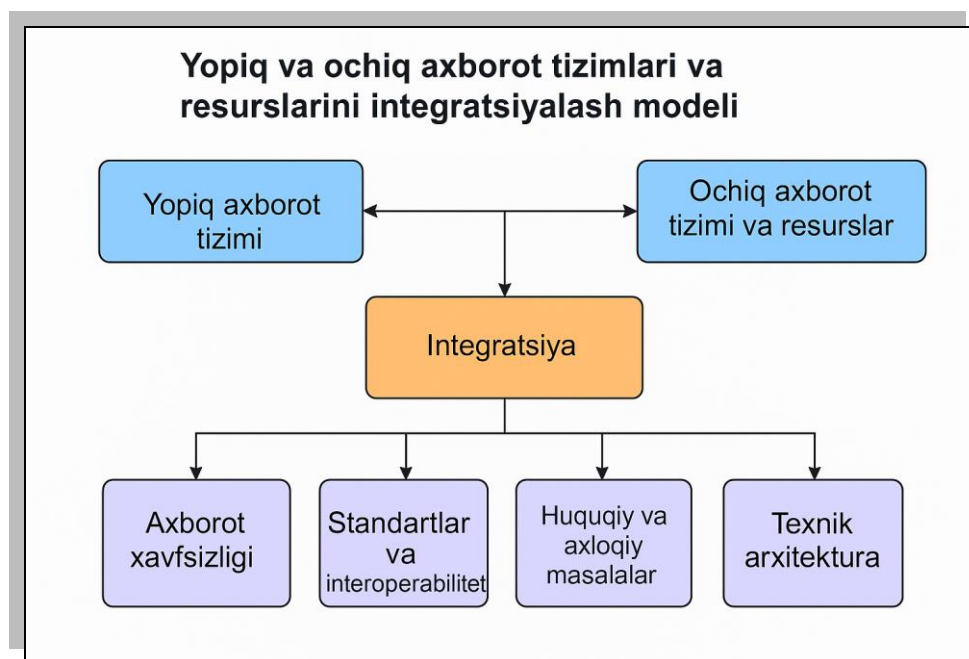
Shu nuqtai nazardan, **yopiq va ochiq axborot tizimlari va resurslarini yagona axborot makoniga birlashtirish** — dolzarb ilmiy-amaliy muammodir.

Bunday integratsiyani muvaffaqiyatli amalga oshirishda bir qator murakkab omillar — texnologik moslik, tizimlararo interfeyslar, ma'lumotlar formatining standartlashtirilganligi, axborot xavfsizligi, qonunchilik talablari va foydalanuvchi huquqlari inobatga olinishi shart.

Shu sababli, samarali integratsiyalash modeli nafaqat texnik yondashuvlar, balki konseptual, huquqiy va metodologik asoslarni ham o'z ichiga olgan bo'lishi lozim.

Mazkur maqola ana shu ehtiyoj va talablar negizida, yopiq va ochiq axborot tizimlari o'rtasida o'zaro aloqani ta'minlovchi **ko'p qatlamli, modulli, xavfsizlikka yo'naltirilgan integratsiya modelini** ishlab chiqish, uni arxitektura, texnologik komponentlar, xavfsizlik yondashuvlari, standartlar va amaliy misollar orqali asoslashga qaratilgan.

2. Asosiy tushunchalar va klassifikatsiya



Yopiq va ochiq axborot tizimlari oʻrtasidagi farqni toʻliq tushunish, ularni samarali integratsiyalashning ilmiy va texnik asoslarini aniqlashda muhim ahamiyatga ega. Bu boʻlimda ushbu tizimlarning taʼrifi, oʻziga xos jihatlari, arxitektura darajalari va ularni integratsiyalashning asosiy yondashuvlari chuqur tahlil qilinadi.

• 2.1. Yopiq axborot tizimlari (Closed Information Systems)

Yopiq axborot tizimlari — bu faqat tashkilot ichki foydalanuvchilari uchun moʻljallangan, tashqi kirish va axborot almashinuvini cheklaydigan, yuqori darajadagi xavfsizlik va maxfiylikni talab qiluvchi tizimlardir.

Asosiy xususiyatlari:

- Mahalliy tarmoq (LAN) asosida ishlaydi.
- Avtorizatsiyadan oʻtgan foydalanuvchilarga xizmat koʻrsatadi.
- Yopiq manba kodi va tashqi API'larning yoʻqligi.
- Maxfiy ma'lumotlar (moliyaviy, tibbiy, strategik) bilan ishlaydi.
- Qattiq xavfsizlik siyosati (firewall, IDS/IPS, audit log).

Misollar:

- Korxona ichki buxgalteriya tizimi (1C, SAP FI).
- Klinik axborot tizimlari (HIS).
- Kadrlar boshqaruvi moduli (HRMS).
- Hukumatning yopiq tarmoqdagi hujjat aylanish tizimlari.

2.2. Ochiq axborot tizimlari (Open Information Systems)

Ochiq axborot tizimlari keng auditoriya uchun moʻljallangan, tashqi integratsiyaga ochiq, koʻpincha Internet orqali erkin foydalaniladigan platformalar va xizmatlardir.

Asosiy xususiyatlari:

- Veb asosidagi va global tarmoqqa ulangan.
- API yoki mashina-oʻqilishi mumkin boʻlgan interfeysga ega.
- Ochiq manba kodli (open-source) yoki ochiq ma'lumotlar bazasiga ega.
- Interaktiv xizmatlar (veb-formalar, real vaqt tahlillari) bilan boyitilgan.

- Ommaviy foydalanish, shaffoflik, qayta ishlatish (reusability) imkoniyatlari mavjud.

Misollar:

- Davlat ochiq ma'lumot portallari (data.egov.uz).
- Ochiq API'ga ega xizmatlar (Google Maps API, OpenWeather).
- Elektron ta'lim platformalari (Moodle, Coursera).
- Ommaviy mobil ilovalar va veb-saytlar.

2.3. Yopiq va ochiq tizimlar o'rtasidagi asosiy farqlar

Belgilar	Yopiq tizimlar	Ochiq tizimlar
Kirish imkoniyati	Cheklangan (faqat tasdiqlangan foydalanuvchilar)	Erkin yoki ro'yxatdan o'tgan foydalanuvchilar uchun
Ma'lumot almashinuvi	Ichki tarmoqlar orqali	Internet orqali ochiq protokollar orqali
Xavfsizlik darajasi	Juda yuqori	O'rta yoki moslashtirilgan
Standartlarga moslik	Ichki (mahalliy) standartlar	Xalqaro va ochiq standartlar (REST, JSON, XML)
Moslashuvchanlik va kengayish	Cheklangan	Yuqori (modullik, API orqali)

2.4. Integratsiyalash turlari va klassifikatsiyasi

Integratsiya uslubi tizimlararo aloqaning murakkabligiga va texnologik vositalarga bog'liq. Quyidagi integratsiya yondashuvlari mavjud:

A) Arxitektura asosida:

- **SOA (Service-Oriented Architecture):** Har bir xizmat mustaqil bo'lib, API orqali chaqiriladi.

- **Microservices:** Yengil xizmatlar majmuasi bo'lib, alohida joylashadi va mos ravishda integratsiyalashadi.

- **ESB (Enterprise Service Bus):** Tizimlararo aloqa markazlashtirilgan marshrutizator orqali amalga oshiriladi.

B) Ma'lumot uzatish mexanizmi asosida:

- **Senkron (synchronous):** Real vaqt rejimida, REST/GraphQL orqali.

- **Asenkron (asynchronous):** Queue (navbat) va Broker'lar (RabbitMQ, Kafka) orqali.

C) Axborot resurslari darajasiga ko'ra:

- **Ma'lumotlar integratsiyasi (Data-level):** ETL vositalari, Data Lake, Data Warehouse.

- **Ilova darajasida integratsiya (Application-level):** Webhooks, mashina-o'qilishi mumkin bo'lgan API.

- **Interfeys darajasida integratsiya (UI-level):** iframe, mashina interfeyslar, OpenID Connect.

2.5. Tizimlararo integratsiya mezonlari

Samarali integratsiya quyidagi mezonlarga javob berishi kerak:

- **Interoperabilitet:** Turli platforma va dasturiy vositalar o'rtasida ishlay olish.
- **Moslashuvchanlik:** Yangiliklarni tez qabul qilish va modernizatsiya qilish imkoniyati.

- **Xavfsizlik:** Ma'lumot uzatishda xavfsiz protokollardan foydalanish (TLS, OAuth).
- **Shkalanish:** Tizimlarning ko'payishi va hajmi ortganida ham barqaror ishlashi.
- **Standartlashtirish:** XML, JSON, HL7, SCORM, xAPI kabi universal formatlardan foydalanish.

3. Integratsiya modelining arxitekturası

Yopiq va ochiq axborot tizimlarini yagona infratuzilmada samarali integratsiyalash uchun ko'p qatlamli, modulli va xavfsizlikka yo'naltirilgan arxitektura modeli talab etiladi. Ushbu arxitektura turli darajadagi tizimlar o'rtasida ishonchli va moslashuvchan axborot almashinuvini ta'minlash, resurslardan optimal foydalanish, modernizatsiyaga ochiqlik va xavfsizlikni kafolatlash kabi talablarga javob berishi lozim.

3.1. Arxitektura modeli tarkibiy qismlari

Integratsiya arxitekturasi quyidagi asosiy qatlamlardan iborat:

A) Ma'lumotlar qatlam (Data Layer)

Bu qatlamda har ikkala turdagi tizimlarda mavjud ma'lumotlar omborlari (RDBMS, NoSQL, fayl tizimlari, Data Lake) joylashgan. Ular turli format va tuzilmada bo'lishi mumkin (CSV, JSON, XML, HL7, SQL va h.k.). Bu qatlam orqali ma'lumotlar tahlili, ETL (Extract, Transform, Load) jarayonlari amalga oshiriladi.

Texnologiyalar: PostgreSQL, MySQL, MongoDB, Hadoop, Apache Spark, Talend.

B) Integratsiya qatlami (Integration Layer)

Yopiq va ochiq tizimlar o'rtasidagi real yoki asenkron axborot almashinuvini ta'minlaydi. API Gateway, ESB (Enterprise Service Bus), yoki mikroxizmatlar arxitekturasi asosida yaratilgan vositalar shu qatlamda ishlaydi.

Komponentlari:

- API Gateway (Kong, Apigee, Amazon API Gateway)
- ETL/ELT vositalari (Apache NiFi, Informatica)
- Broker'lar (RabbitMQ, Apache Kafka)
- Web Service'lar (RESTful, SOAP)

Funktsiyalari:

- Ma'lumotlarni transformatsiya qilish va formatlash
- Protokollarni moslashtirish
- Avtenticatsiya va avtorizatsiya (OAuth 2.0, JWT)

C) Xizmatlar va logika qatlami (Service Layer)

Bu qatlamda foydalanuvchi ehtiyojlariga moslashtirilgan biznes xizmatlar (mikroxizmatlar) joylashgan bo'ladi. Har bir xizmat alohida modulli shaklda ishlab chiqilib, kerakli API orqali tizimlarga taqdim etiladi.

Texnologiyalar: Spring Boot, Node.js, ASP.NET Core, FastAPI, GraphQL

Misollar:

- Hujjatlarni elektron imzolash xizmati
- Rejimga muvofiqlik (compliance) tekshiruvi
- Foydalanuvchi profilini sinxronlash
- To'lov jarayonlarini boshqarish

D) Tashqi interfeyslar va foydalanuvchi qatlam (Presentation Layer)

Ushbu qatlam orqali ochiq tizim foydalanuvchilari (yoki integratsiyalashgan tashkilotlar) tizim bilan o'zaro aloqada bo'ladi. Bu qatlamda veb-ilovalar, mobil interfeyslar, hamda mashina-o'qilishi mumkin bo'lgan APIlar (OpenAPI, Swagger) mavjud bo'ladi.

Texnologiyalar: React, Angular, Flutter, OpenAPI, Swagger UI

3.2. Xavfsizlik infratuzilmasi

Integratsiyalashgan muhitda ma'lumotlar oqimi ko'paygani sari, axborot xavfsizligi eng muhim omilga aylanadi. Shu sababli quyidagi xavfsizlik choralari model arxitekturasiga majburiy tarzda integratsiyalanadi:

- **Avtentifikatsiya va avtorizatsiya:** OAuth 2.0, OpenID Connect, LDAP, Active Directory

- **Ma'lumotlarni shifrlash:** TLS/SSL, AES, PGP

- **Audit log va monitoring:** ELK Stack (Elasticsearch, Logstash, Kibana), Prometheus, Grafana

- **Xavfsizlik devorlari va IDS/IPS:** WAF (Web Application Firewall), Suricata, Snort

3.3. Integratsiya modeli arxitekturasining umumiy tuzilmasi

Quyidagi sxema asosida model arxitekturasini ifodalaydi (izohlari bilan):

lua

КопироватьРедактировать

+-----+

| Tashqi foydalanuvchilar |

+-----+

|

+-----v-----+

| API Gateway | ← Kirish nuqtasi, xavfsizlik darvozasi

+-----+

|

+-----v-----+

| Integratsiya vositalari (ESB, MQ, ETL) |

+-----+

|

+-----v-----+ +-----v-----+

| Yopiq tizimlar | | Ochiq tizimlar |

| (ERP, HIS, CRM, HRMS) | | (eGov API, Ochiq ma'lumotlar)|

+-----+ +-----+

3.4. Modelning afzalliklari

- **Moslashuvchanlik:** Yangi tizimlarni osongina ulash imkoniyati

- **Shkalanish:** Yuklama oshgan sari modullarni alohida kengaytirish mumkin

- **Xavfsizlik:** Kirish nazorati, protokollar orqali yuqori darajada kafolatlangan

- **Standartlashtirish:** Xalqaro standartlarga asoslangan (REST, JSON, HL7)

- **Audit va monitoring:** Tizim faoliyatini real vaqt rejimida nazorat qilish imkoniyati

4. Axborot xavfsizligi muammolari

Yopiq va ochiq axborot tizimlarining integratsiyalashuvi nafaqat texnologik sinxronlashuvni, balki ularning axborot xavfsizligi siyosatlari o'rtasidagi muvofiqlikni ham talab etadi. Tizimlararo axborot oqimini tashkil qilishda har xil xavf omillari yuzaga keladi: maxfiylikning buzilishi, ma'lumotlarning o'zgartirilishi, ruxsatsiz kirishlar, foydalanuvchilar identifikatsiyasining buzilishi, kiberhujumlar va boshqalar. Ayniqsa, ochiq tizimlar orqali kelayotgan ma'lumot oqimlari va tashqi API'lar, integratsiyalashgan muhitda xavfsizlik devorlarini zaiflashtirishi mumkin.

4.1. Asosiy xavfsizlik tahdidlari

Integratsiyalashgan axborot tizimlarida kuzatiladigan asosiy xavfsizlik tahdidlari quyidagilardan iborat:

Tahdid turi	Tavsif
Ruxsatsiz kirish (Unauthorized access)	Tashqi yoki ichki foydalanuvchilarning tizimga noqonuniy yo'l bilan kirishi
Xizmatdan mahrum qilish (DoS/DDoS)	Tizim resurslarini haddan ziyod yuklab, uni ishdan chiqarish
Ma'lumotlar o'g'irlanishi	Shifrlanmagan yoki zaif protokollar orqali yuborilgan ma'lumotlarning ushlab olinishi
Identifikatsiya buzilishi (Session hijacking)	Avtorizatsiya sessiyalarining yomon niyatli foydalanuvchilar tomonidan egallanishi
Zararkunanda dasturlar (malware)	Ochiq interfeyslar orqali tizimga kirib, ichki jarayonlarga zarar yetkazuvchi viruslar
Ichki xodim tahdidi (Insider threat)	Ichki tizim foydalanuvchilari tomonidan maxfiy yoki muhim ma'lumotlarni qasddan sızdırilishi

4.2. Xavfsizlikdagi strukturaviy zaifliklar

Yopiq va ochiq tizimlar orasidagi farqlarning keskinligi xavfsizlik siyosatlarini uyg'unlashtirishda qiyinchilik tug'diradi:

- **Standardlar nomuvofiqligi:** Yopiq tizimlar ichki protokollar va regulyatorlarga tayanadi, ochiq tizimlar esa RESTful, JSON kabi global interfeyslar asosida ishlaydi.
- **Moslashtirilmagan avtorizatsiya mexanizmlari:** OAuth 2.0 va LDAP kabi mexanizmlar o'zaro to'g'ri sozlanmasa, xavfsizlik teshiklari paydo bo'ladi.
- **Audit mexanizmlarining yo'qligi:** Tizimlararo faoliyat ustidan doimiy monitoring olib borilmasa, hujumlarni erta aniqlash qiyinlashadi.
- **Zamonaviy kriptografiya protokollarining yetishmasligi:** TLS 1.0 yoki zaif shifrlash algoritmlari hali ham ishlatilayotgan tizimlar mavjud.

4.3. Xavfsizlikni ta'minlash strategiyalari

Yopiq va ochiq tizimlarni integratsiyalashuvida quyidagi xavfsizlik choralarini qo'llash maqsadga muvofiq:

A) Autentifikatsiya va avtorizatsiya:

- OAuth 2.0, OpenID Connect yordamida kirishni boshqarish
- Role-Based Access Control (RBAC) yoki Attribute-Based Access Control (ABAC)

B) Shifrlash:

- TLS 1.2+ asosidagi transport qatlamini himoya qilish
- Ma'lumotlar omborida AES-256, RSA kabi algoritmlardan foydalanish

C) Monitoring va Audit:

- Real vaqt rejimida log tahlili (ELK stack, Splunk)
- Intrusion Detection Systems (IDS): Snort, OSSEC
- Intrusion Prevention Systems (IPS): Suricata, Zeek

D) Segmentatsiya va zonalashtirish:

- Tizimlarni xavfsizlik zonolari (DMZ, Internal, Restricted) asosida ajratish
- Har bir zona uchun alohida xavfsizlik devori va qoidalar to'plami

E) API xavfsizligi:

- Rate limiting (chegaralangan so'rovlar soni)
- API key, JWT (JSON Web Token) asosida himoya
- Input validation va XSS/SQLi oldini olish uchun WAF (Web Application Firewall)

4.4. Huquqiy va tartibga solish muammolari

Xavfsizlik faqat texnik darajada emas, balki huquqiy va siyosiy jihatdan ham qo'llab-quvvatlanishi lozim. Jumladan:

- **Ma'lumotlarni himoya qilish to'g'risidagi qonunlar:** GDPR (Yevropa), DPA (Buyuk Britaniya), O'zbekiston Respublikasi "Shaxsiy ma'lumotlar to'g'risida"gi Qonuni.
- **Ochiq ma'lumotlar siyosati bilan yopiq tizimlar xavfsizlik siyosatining ziddiyati.**
- **Data residency va Data sovereignty:** Ma'lumotlar qayerda saqlanishi, qaysi yurisdiksiya bo'yicha boshqarilishi.

4.5. Tavsiyalar

- Integratsiya loyihalarida **"Security by Design"** yondashuvini joriy etish.
- Har bir tizim uchun **xavfsizlik tahlili (risk assessment)** olib borish.
- Yagona **Security Operation Center (SOC)** tashkil etish.
- **Penetratsion testlar va Red/Blue Team** simulyatsiyalarini o'tkazish.

5. Standartlar va interoperabilitet

Yopiq va ochiq axborot tizimlarini integratsiyalash jarayonida ularning o'zaro to'g'ri va xavfsiz ishlashini ta'minlash uchun yagona **standartlar bazasi** va yuqori darajadagi **interoperabilitet (moslik va o'zaro tushunish)** zarurdir. Interoperabilitet — bu turli axborot tizimlarining bir-biri bilan muammosiz axborot almashish, ma'lumotlarni qayta ishlash va umumiy funksiyalarni bajarish qobiliyatidir.

Standartlashtirish va interoperabilitet — tizimlararo ishonch, xavfsizlik, barqarorlik va texnologik kengayishning kafolatidir.

5.1. Interoperabilitet turlari

Interoperabilitet quyidagi asosiy turlarda namoyon bo'ladi:

Interoperabilitet turi	Tavsif
Texnik interoperabilitet	Tizimlar bir xil texnologiyalar, protokollar (TCP/IP, HTTP, TLS) va formatlar (XML, JSON, CSV) asosida ishlaydi.
Semantik interoperabilitet	Tizimlar ma'lumotlarni bir xil ma'noda tushunadi, ya'ni

Interoperabilitet turi	Tavsif
	kontentda yotgan tushunchalar yagona semantikaga ega bo'ladi.
Tashkiliy (organizatsion) interoperabilitet	Turli tashkilotlar, idoralar va xizmatlar o'rtasidagi siyosiy, huquqiy, reglament va ish jarayonlarining muvofiqligi.
Hujjatli interoperabilitet	Axborot almashinuv protokollari, API spetsifikatsiyalari va integratsiya hujjatlari mavjud bo'ladi.

5.2. Asosiy xalqaro standartlar

Quyidagi xalqaro standartlar ochiq va yopiq tizimlar orasida integratsiyani qo'llab-quvvatlaydi:

Standart	Tavsifi
ISO/IEC 27001	Axborot xavfsizligini boshqarish tizimi (ISMS) uchun standart
ISO/IEC 20000	IT xizmatlarini boshqarish bo'yicha xalqaro standart
ISO/IEC 11179	Ma'lumotlar elementlarini ro'yxatga olish va tavsiflash standarti (metadata registrlari)
FHIR (Fast Healthcare Interoperability Resources)	Sog'liqni saqlash tizimlari uchun interoperabilitet standarti
HL7	Tibbiyotdagi tizimlararo ma'lumot almashuv protokollari
OData (Open Data Protocol)	RESTful xizmatlar orqali ma'lumotlarga kirishni standartlashtiradi
OpenAPI/Swagger	API spetsifikatsiyalarini hujjatlashtirish va avtomatlashtirish standarti
WSDL & SOAP	Veb xizmatlar uchun interoperabilitetni ta'minlaydi

5.3. Milliy standartlar va tashabbuslar

O'zbekiston Respublikasi ham davlat organlari va fuqarolar o'rtasidagi ochiq, ishonchli va xavfsiz ma'lumot almashinuvi uchun quyidagi hujjatlar va tashabbiyalarni ilgari surmoqda:

- **“Ochiq ma'lumotlar to'g'risida”gi qonun**
- **Davlat xizmatlari agentligi tomonidan boshqariladigan yagona davlat interaktiv xizmatlari portali (my.gov.uz)**
- **“Elektron hukumat” kontsepsiyasi**
- **Milliy axborot-kommunikatsiya infratuzilmasi standartlari (MAKIS)**
- **UZ-GOVNet – davlat tarmoqlari uchun yopiq, xavfsiz tarmoq**

5.4. Interoperabilitetni ta'minlashdagi muammolar

Yopiq va ochiq tizimlar orasidagi farqlar quyidagi muammolarga sabab bo'ladi:

- **Standartlar ziddiyati:** Ba'zi tizimlar faqat ichki, maxsus protokollar (masalan, SOAP) bilan ishlaydi, boshqalari esa RESTful API'larni talab qiladi.

- **Format nomuvofiqligi:** XML ↔ JSON konversiyasi va ma'lumot strukturasiidagi tafovutlar.

- **Til va kodlash muammolari:** UTF-8 ↔ Windows-1251 kabi kodlash farqlari, ko'p tillilikni qo'llab-quvvatlamaslik.

- **Metama'lumotlar yo'qligi:** Tizimlar o'zaro bog'lanadi, ammo ma'lumotlarning semantik izohi mavjud emas.

5.5. Interoperabilitetni ta'minlash bo'yicha tavsiyalar

- **Standartlar katalogini shakllantirish:** Har bir tashkilot o'z API va ma'lumot formatlari uchun umumiy spetsifikatsiya tayyorlashi lozim.

- **Middleware va API Gateway ishlatish:** Har xil texnologik muhitlarda muvofiqlikni API orqali ta'minlash.

- **Metadata Registry joriy etish:** Ma'lumot elementlari, ularning tavsifi, turlari va bog'liqliklarini yagona reyestrda yuritish.

- **Semantic Mapping va Ontologiyalar:** Turli tizimlar o'rtasida atamalar va tushunchalarning mos kelishini ta'minlash (masalan, "foydalanuvchi" ↔ "mijoz").

- **Testlash va sertifikatlash:** Har bir integratsiyalashgan modul o'zaro muvofiqlik testlaridan o'tkazilishi kerak (interoperability testing).

6. Huquqiy va axloqiy masalalar

Yopiq va ochiq axborot tizimlarining integratsiyasi faqat texnologik va xavfsizlik jihatidan emas, balki **huquqiy** va **axloqiy** asoslardan kelib chiqib ham muvofiqlashtirilishi lozim. Integratsiyalashgan tizimlarda ma'lumotlar almashinuvi kengaygan sari, shaxsiy hayot daxlsizligi, axborotdan foydalanish chegaralari, mualliflik huquqlari, ma'lumotlarning qonuniy statusi va etik me'yorlarga rioya qilish masalalari dolzarb bo'lib bormoqda.

6.1. Huquqiy asoslar

Axborot tizimlari bilan ishlovchi tashkilotlar va foydalanuvchilar quyidagi asosiy qonun va huquqiy me'yorlarga amal qilishi shart:

Qonun/huquqiy hujjat	Tavsifi
O'zbekiston Respublikasi "Shaxsiy ma'lumotlar to'g'risida"gi Qonuni (2019)	Shaxsiy ma'lumotlarni yig'ish, saqlash, qayta ishlash va tarqatishga doir tartiblarni belgilaydi.
Elektron hukumat to'g'risidagi Qonun	Davlat axborot tizimlari o'rtasidagi integratsiyani tartibga soladi.
Axborotlashtirish to'g'risida"gi Qonun	Axborot resurslari va tizimlarining yuritilishi, huquqiy asoslari va xavfsizligini ta'minlash masalalari.
Copyright va mualliflik huquqlari qonunlari	Ochiq tizimlarga joylashtirilayotgan fayllar, kodlar yoki hujjatlar mualliflik himoyasida bo'lishi mumkin.
Xalqaro qonunlar: GDPR (Yevropa), CCPA (Kaliforniya)	Chet el resurslari bilan integratsiya qilinganda xorijiy yurisdiksiyalarni ham hisobga olish zarur.

6.2. Shaxsiy ma'lumotlarni himoya qilish muammolari

Integratsiya qilish jarayonida shaxsiy ma'lumotlar turli tizimlar o'rtasida harakatlanadi. Bu holat:

- **Roziliksiz ishlov berish (Consent violation):** Foydalanuvchidan rozilik olinmasdan uning ma'lumotlari boshqa tizimlarga uzatilishi.

- **Ma'lumotlar sızıntisi:** Ochiq API orqali yopiq tizimga kirgan ma'lumotlarning uchinchi tomonlar tomonidan ushlab olinishi.

- **Noaniq mas'uliyat chegaralari:** Ma'lumotdan foydalanish natijasidagi huquqiy javobgarlik kimga yuklatilishi mavhum bo'lishi mumkin.

Tavsiyalar:

- Har bir foydalanuvchining **roziligini rasmiylashtirish**.
- Ma'lumot almashishda **data minimization** (zarurdan ortiqcha ma'lumot yubormaslik) prinsipi.

- Shaxsiy ma'lumotlar uchun alohida **Data Protection Officer (DPO)** tayinlash.

6.3. Axborot etikasi (axloqiy masalalar)

Axborot etikasi — bu axborot texnologiyalaridan foydalanishda odob, mas'uliyat va hurmat tamoyillariga asoslangan yondashuvdir. Axborot tizimlari integratsiyasida quyidagi axloqiy muammolar kuzatiladi:

- **Foydalanuvchini kuzatish (surveillance):** Ochiq resurslar orqali foydalanuvchi harakatlarini nazorat qilish — axloqan ziddiyatli hisoblanadi.

- **Sun'iy intellekt va qaror qabul qilish:** Avtomatlashtirilgan tizimlar foydalanuvchi haqidagi qarorlarni shaffof bo'lmagan asosda qabul qilishi mumkin.

- **Ma'lumotlarni manipulyatsiya qilish:** Ochiq tizimlardan olingan ma'lumotlar maqsadga muvofiq tarzda buzib talqin qilinishi mumkin.

- **Axborot notengligi (digital divide):** Ochiq tizimlardan foydalanish imkoniyatiga ega bo'lmagan qatlamlar raqamli tengsizlikka uchrashi mumkin.

Etik tamoyillar:

- Shaffoflik (transparency)
- Rozilik va xabardorlik (informed consent)
- Javobgarlik (accountability)
- Adolat (equity)
- Foydalanuvchiga hurmat (respect for users)

6.4. Muvofiqlikni ta'minlash choralar

- **Ma'lumotlar boshqaruvi siyosatini (Data Governance Policy)** ishlab chiqish.

- **Etik ko'rsatmalar (Ethical Guidelines)** asosida xizmatlarni loyihalash.

- **Axborotga kirish darajalarini qat'iy belgilash (Access Control Matrix).**

- **Audit va monitoring tizimlari yordamida shubhali harakatlarni aniqlash.**

- ****Axloqiy audit (Ethical Impact Assessment)**ni joriy etish.**

6.5. Holatlar asosidagi misollar

1. Yopiq sog'liqni saqlash tizimi va ochiq e-portal integratsiyasi:

- Foydalanuvchi tibbiy tarixini ko'rish huquqiga ega bo'ladi.
- Shaxsiy sog'liq ma'lumotlarini himoyalash bo'yicha maxsus rozilik talab etiladi.

2. Ta'limda axborot tizimlari integratsiyasi:

- Ochiq resurslardan o'quvchilar ma'lumotlarini yig'ish va uni yopiq tizimga saqlash.
- Yosh foydalanuvchilarning ma'lumotlarini ishlatishda maxsus axloqiy me'yorlar mavjud.

• 7. Amaliy tadqiqotlar va qo'llanma misollar

Yopiq va ochiq axborot tizimlarini integratsiyalash bo'yicha bir qancha real amaliy loyihalar va tajribalar mavjud bo'lib, ular ushbu modelning samaradorligini amalda isbotlab bermoqda. Quyida ba'zi misollar bilan tanishamiz:

7.1. O'zbekiston Respublikasida E-Hukumat integratsiyasi

• **Tizimlar:** Yagona interaktiv davlat xizmatlari portali (my.gov.uz), Davlat soliq qo'mitasi, YHXBB, DTM, Adliya vazirligi.

• **Integratsiya shakli:** API va servislar orqali real vaqtda ma'lumot almashuvi, yagona login orqali kirish (SSO), ijtimoiy va moliyaviy axborotlar almashuvi.

• **Natija:** Xizmatlar soddalashti, byurokratiya kamaydi, fuqaro davlat bilan samarali aloqada bo'la oldi.

7.2. "Elektron universitet" tizimi integratsiyasi

• **Tizimlar:** Oliy ta'lim muassasalari ichki axborot tizimlari va Oliy ta'lim vazirligining ochiq statistik platformasi.

• **Foydalanuvchilar:** Talabalar, o'qituvchilar, tahlilchilar.

• **Foyda:** Talabalar reytinglari, ilmiy faoliyati, diplomlar haqidagi ma'lumotlar ochiq statistik tahlil platformasi bilan uyg'unlashtirildi.

7.3. Xalqaro misol: Estoniya – X-Road loyihasi

• **Xususiyat:** Ochiq va yopiq davlat ma'lumotlar bazalari o'rtasida xavfsiz, standartlashtirilgan, logli, nazorat ostida ishlovchi data almashuv platformasi.

• **Darslik:** Butun Estoniya davlat boshqaruvi tizimi shu asosda ishlaydi.

• **Model:** Yagona raqamli identifikatsiya, qattiq shifrlash, desentralizatsiya.

7.4. "OpenStreetMap" + yopiq transport tizimlari integratsiyasi

• **Model:** Ochiq xarita platformalari (OSM) bilan yopiq transport nazorati tizimlari bog'langan.

• **Foyda:** Tranzit monitoringi, real vaqtda transport harakati, tahliliy vizualizatsiya.

8. Kelajak istiqbollari

Yopiq va ochiq tizimlar integratsiyasi kelajakda yanada rivojlanishi va quyidagi yo'nalishlarda chuqurlashishi kutilmoqda:

Yo'nalish	Tavsif
Sun'iy intellekt asosidagi avtomatik integratsiyalar	Tizimlar bir-birini avtomatik aniqlab, API-larni moslashtiradi.
IoT tizimlar bilan integratsiya	Yopiq tizimlarda ishlovchi qurilmalar (masalan, smart sensorlar) ochiq platformalar bilan bog'lanadi.
Desentralizatsiyalashgan identifikatsiya (DID)	Shaxsiy ma'lumotlar markazlashtirilmagan blokcheyn asosida boshqariladi.
Data trust'lar tashkil etilishi	Foydalanuvchi ma'lumotlari maxsus vakolatli

Yoʻnalish	Tavsif
	tashkilotlar orqali nazorat qilinadi.
Metaverse va AR/VR muhitlar bilan integratsiya	Yopiq tizimlar ochiq 3D virtual interfeyslar bilan uygʻunlashadi.

Xulosa

Yopiq va ochiq axborot tizimlari va resurslarini integratsiyalash — zamonaviy raqamli infratuzilmaning ajralmas qismiga aylanmoqda. Bu jarayon samarali boʻlishi uchun quyidagi jihatlarga eʼtibor qaratish zarur:

- Texnik, semantik, tashkiliy interoperabilitetni taʼminlash.
- Xalqaro va milliy standartlarga qatʼiy amal qilish.
- Axborot xavfsizligi va shaxsiy maʼlumotlar himoyasini ustuvor qilish.
- Huquqiy va axloqiy masalalarni eʼtibordan chetda qoldirmaslik.
- Foydalanuvchi markazida ishlaydigan, ochiq, ishonchli va shaffof integratsiya modellari yaratish.

Kelgusida bu soha yangi texnologiyalar bilan uygʻunlashgan holda, ijtimoiy, iqtisodiy va madaniy taraqqiyotga ulkan hissa qoʻshadi.

REFERENCES

1. Oʻzbekiston Respublikasi "Shaxsiy maʼlumotlar toʻgʻrisida"gi Qonuni. 2019.
2. Axborotlashtirish toʻgʻrisidagi Qonun. 2003 (oʻzgartirishlar bilan).
3. Oʻzbekiston Respublikasi Prezidentining "Raqamli Oʻzbekiston – 2030" strategiyasi.
4. ISO/IEC 27001:2022 — Information Security Management Systems.
5. ISO/IEC 11179 — Metadata Registries.
6. European Union General Data Protection Regulation (GDPR). 2018.
7. OpenAPI Specification 3.0. Swagger.io.
8. HL7 FHIR Standard for Health Information Exchange.
9. Estonia's X-Road Architecture White Paper. 2021.
10. Tim Berners-Lee. "Weaving the Web." Harper San Francisco, 2000.
11. Data Governance Institute. "Data Governance Framework." www.datagovernance.com.
12. Oxford Internet Institute. "Ethics in the Digital Age." 2022.
13. OECD. "Digital Government Strategies for Transforming Public Services." 2020.