INNOVATIVE WORLD

ISSN: XXXX-XXXX

ORIENTAL JOURNAL OF ENGINEERING AND MODERN TECHNOLOGIES

SHARQ MUHANDISLIK VA ZAMONAVIY TEXNOLOGIYALAR JURNALI

Scientific Journal

- Civil
- Robotic
- Material
- Chemical
- Computer
- Electrical
- Mechanical
- Agricultural
- Manufacturing

- Qurilish
- Robototexnika
- Materialshunoslik
- Kimyo-texnologiya
- Informatika
- Elektr texnologiya
- Mexanika
- Qishloq xo'jaligi
- Ishlab chiqarish

xomidovanvarbek07@gmail.com
www.innoworld.net
+998 33 5668868

ORIENTAL JOURNAL OF ENGINEERING AND MODERN TECHNOLOGIES

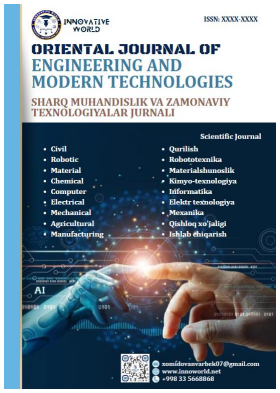
Volume 3, Issue 2
2025

Journal has been listed in different indexings

Google Scholar · doi digital object identifier · ResearchGate · zenodo · ADVANCED SCIENCE INDEX · OpenAIRE · Academic Resource Index ResearchBib · DRJI Directory of Research Journals Indexing

The offical website of the journal:
www.innoworld.net

Uzbekistan-2026



RAQAMLI BANK XIZMATLARIDA KIBERXAVFSIZLIK

Sobirjonov Behzodbek Qahramon o‘gli
Farg‘ona davlat universiteti Axborot texnologiyalari kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Numonjonov Ozodbek Nodirjon o‘gli
Farg‘ona davlat universiteti Axborot tizimlari va texnologiyalari yo‘nalishi 2-kurs talabasi
nomonjonovozodbek720@gmail.com

Annotatsiya: Ushbu maqola bank tizimining yaralishi va undagi xavfsizlik talablari hamda unga qilinayotgan chor tadbir to‘g‘risida tahlil qilindi. Bank tizimidagi raqamli innavatsiyalar kundan kun o‘zgarish va xavfsizlik zamon talabiga mos ravishda oshirib borilmoqda. Shuningdek, maqolada ushbu xizmatlarning amaliy foydalanish misollari keltirilib, kelajakdagi istiqbollari yoritiladi.

Kalit so‘zi: Bank tizimidagi shifrlar, terminal va to‘lov usullari, bank indifikatsiyasi, ximoya parollari va biometrik quluflar.

Abstract: This article analyzes the formation of the banking system and the security requirements in it, as well as the measures being taken to address it. Digital innovations in the banking system are changing day by day and security is increasing in line with the demands of the times. The article also provides examples of practical use of these services and highlights future prospects.

Keywords: Passwords in the banking system, terminals and payment methods, bank identification, protective passwords and biometric locks.

Аннотация: В данной статье проанализировано создание банковской системы и требования к ее безопасности, а также меры, принимаемые против нее. Цифровые инновации в банковской системе растут с каждым днем в соответствии с изменениями и требованиями безопасности времени. Также в статье приведены примеры практического использования данных сервисов и освещены их дальнейшие перспективы.

Ключевые слова: Пароли в банковской системе, терминалы и способы оплаты, банковская идентификация, пароли безопасности и биометрические замки.

Kirish: Bank tizimining moliyaviy resurslarini, mijozlar ma’lumotlarini va tranzaksiyalarni himoya qilish uchun ishlab chiqilgan chora-tadbirlar, texnologiyalar va siyosatlar to‘plamidir. Hozirgi kunda, banklar nafaqat an’anaviy operatsiyalarni, balki raqamli xizmatlarni ham taqdim etmoqda, bu esa yangi xavf-xatarlarni keltirib chiqaradi. Kiberhujumlar, firibgarlik, ma’lumotlarning o‘g‘irlanishi va boshqa turli xavf-xatarlar banklar uchun jiddiy tahdid solmoqda. Shuning uchun bank xavfsizligi iqtisodiyotning barqarorligi va mijozlarning ishonchini saqlashda juda muhim rol o‘ynaydi. Bank xavfsizligi tizimi bir necha asosiy elementlardan iborat bo‘lib, ular o‘zaro muvofiqlashgan holda bank operatsiyalarining xavfsiz va samarali amalga oshirilishini ta’minlaydi. Bular

orasida kiberxavfsizlik, ma’lumotlarni shifrlash, kredit kartalari va to‘lov tizimlarining himoyasi, pul yuvishga qarshi kurashish, ichki audit va nazorat jarayonlari mavjud. Xavfsizlik choralarining samaradorligi banklarning global moliyaviy tizimdagi o‘rniga va mijozlarga bo‘lgan ishonchiga bevosita ta’sir ko‘rsatadi. Shu bois, banklar uchun xavfsizlik strategiyalarini ishlab chiqish va ularni doimiy ravishda yangilash zarur. Texnologik taraqqiyot va yangi xavf-xatarlar bilan kurashish uchun banklar xavfsizlik choralarini yaxshilash, zamonaviy tizimlarni joriy etish va mijozlarni onlayn xizmatlarda ehtiyotkorlikka chaqirishni o‘rganishlari muhimdir.

Bugungi kunda bank tizimi nafaqat an’anaviy, balki raqamli xizmatlar orqali ham o‘z mijozlariga xizmat ko‘rsatadi. Bu esa o‘z navbatida banklar uchun yangi xavf-xatarlar yaratadi, xususan, kiberhujumlar. Kiberhujumlar bank tizimining asosiy komponentlarini buzib, moliyaviy resurslar, mijoz ma’lumotlari va tranzaksiyalarni xavf ostiga qo‘yishi mumkin. Shuning uchun banklar kiberxavfsizlikni o‘z tizimlarining eng muhim qismi sifatida ko‘rib, unga qarshi chora-tadbirlarni kuchaytirishlari zarur. Bunga bir qator chora tadbirlar qilinmoqda. Mijozlarning hisoblariga kirishda ikki bosqichli autentifikatsiya tizimi qo‘llaniladi. Bu xavfsizlik chorasida foydalanuvchi parolni kiritgandan so‘ng, qo‘shimcha kodni telefon yoki email orqali oladi, bu esa tizimga kirishni faqat qonuniy foydalanuvchi amalga oshirishi mumkinligini ta’minlaydi. Banklar tarmoqlarini kuzatib boruvchi tizimlar yordamida kiberhujumlarni tahlil qilib, ularni erta aniqlashga harakat qilishadi. Hujum aniqlanganida, tezkor ogohlantirish va choralar ko‘rish jarayonlari boshlanadi.

Asosiy qism: Bank — bu aholi va tashkilotlardan pul mablag‘larini qabul qilish, ularni saqlash va himoya qilishni ta’minlash, shuningdek kreditlar va boshqa molyaviy xizmatlarni taqdim etish bilan shug‘ullanadigan moliyaviy muassasa. Dastlab bank Milddan avvalgi yillarda ibodatxonlar odamlar pulini saqlab qo‘yish vazifasni bargan. Banklar moliya bozorining asosiy ishtirokchilari bo‘lib, ularning faoliyati mamlakat iqtisodiyotiga sezilarli ta’sir ko‘rsatadi. urli mamlakatlarda bank tizimi turli xil tuzilishga ega bo‘lishi mumkin. Ammo odatda bank tizimi bir necha darajalarga bo‘linadi. Birinchi darajada mamlakatning bank tizimini tartibga soluvchi Markaziy bank mavjud. Markaziy bank foiz stavkalarini belgilash, pul massasini tartibga solish, boshqa banklarni nazorat qilish kabi funktsiyalarni bajarishi mumkin. Keyingi bosqichda mijozlarga xizmat ko‘rsatadigan va depozitlarni qabul qiladigan, kreditlar beradigan va hokazo tijorat banklari mavjud. Yana bir daraja mintaqaviy bankla bo‘lib, ular mahalliy jamoalar uchun moliyaviy xizmatlarni taqdim etish orqali bitta mintaqada yoki shtatda ishlashlari mumkin. Ba’zi mamlakatlarda, shuningdek, bitta korxona xodimlari yoki bitta jamoa aholisini o‘z ichiga olishi mumkin bo‘lgan ittifoq a’zolari uchun moliyaviy xizmatlar ko‘rsatadigan kredit uyushmalari bo‘lishi mumkin. Uyg‘onish davrida bank ishi yanada rivojlandi. Bank uylari juda yuqori obro‘ga ega bo‘ldi. Zamonaviy bank tizimi ilk bor 1587-yil Venetsiyada “ Banko di Rialto ” tashkil etilganida paydo bo‘lgan.

XIX asr Grigoriy taqvimiga ko‘ra, 1-yanvar 1801-yildan 31-dekabr 1900-yilgacha bo‘lgan davr bank sektori yanada jadal rivojlana boshladi. Sanoat inqilobining boshlanishi kreditlash hajmini oshirishni talab qildi va kredit berish uchun yirik banklar tashkil etildi. O‘shandan beri bank tizimi o‘zgaruvchan iqtisodiy sharoitlarga mos ravishda rivojlanishda davom etmoqda.

Bank tizimi tarixidagi eng muhim davrlardan biri bu 1929-yildagi inqiroz. Ushbu inqiroz banklarning global qulashiga sabab bo‘ldi. Ko‘pgina banklar o‘z eshiklarini yopishga majbur bo‘lishdi, bu esa bank tizimining qisqarishiga olib keldi. Ikkinchi jahon urushi davrida dunyoning barcha asosiy kuchlari iqtisodiyotga faol aralashishga majbur bo‘ldilar va bank tizimini jadal tartibga solishni boshladilar.

20-asrning oxirida bozor iqtisodiyotiga sodiq qolgan mamlakatlarning aksariyati bank tizimini to‘liq tartibga solishdan voz kechishdi. Bu banklarga raqobatbardosh bo‘lish va yuqori daromad olish imkonini berdi. Biroq, bank tizimi hali ham xavf ostida. So‘nggi paytlarda davlat tomonidan xatarlarni nazorat qilinadigan darajada ushlab turishga qaratilgan nazorat kuchaymoqda. Bank tizimi o‘sishda va rivojlanishda davom etmoqda, bu bizga kredit kartalaridan tortib elektron hisoblargacha bo‘lgan ko‘plab vositalarni taqdim etadi. Bank tizimi oddiy odamlarning biznesiga, iqtisodiyotiga va hayotiga sezilarli ta’sir ko‘rsatadi.

Xavfsizik bu eng asosiy talabdir. Ya’ni sizga oid bo‘lgan malumotlarni xavfsiz saqlash uchun siz shifirarga murojat qilasiz. Shifir bu siz yashiroqchi bo‘lgan fayil yoki birorbir sayit kirish chun kerak bo‘ladigon kalt.

Asosan kaltlarni hayotimizda ko‘p uchratadigon hollardan biri bu kartaga qo‘yiladigon ximoya kodlaridir. Lekin ko‘p odamlar sodda shifirlardan foidalanar ekan. Ma’lumolara qaragada 30-40% odamlar o‘zlari tug‘ulgan yil yoki kun oyin ximoya kod sifatida foydalanadi. Bunga sabab esa odamlar ximoy kodlari yodda tutish uchun shunday sodda ximoya kodlaridan foydalanadi. Bundan shuni bilsak bo‘ladiki karta xafsizligi yetarli darajada xavfsiz emasligi. Karta xavfsizligi yanada kuchaytirish maqsadida biametrik ximoyalardan foydalanish va biametrik ximoyani karta egasi va oilasi biametriyasi kiritish. Oila biametriyasini kiritishdan maqsad esa faqat karta egasi bo‘lgan holda kartadan foydalanish emas balki egasi o‘rniga farzandi nevarasi yoki boshqasi oila azolari ham bir dek foydalanishi uchun.

Email pochta manzili ximoyasi juda a’lo darajada ximoyalanadi chunki oson kodlarni rad etadi va minimal 8 ta belgidan tashkil topgan va hech bo‘lmaganda bitta harif bo‘lmasa siz qo‘ygan kodni qabul qilmaydi. Email pochtaga ketma-ket raqamlardan himoya kodi o‘rnida foydalanib bo‘lmaydi chunki bunday himoyani buzish osonligi uchun bunday himoy kodini qabul qilmaydi. Email pochtaga qo‘yiladigon kodlar soni cheklangan va bu chegara 16 ta belgi. Nega 16 ta belgi emas degan savollar ham uchratamiz, “kodlar soni qancha ko‘paygan sari eslab qoslish shu darajada qiynlashib boradi. Bu kodni buzub bo‘lmas darajada bo‘ladi lekin eslab qolish ham qiyinlashib boradi. Shu sababli 16 ta belgidan ko‘p bo‘lmasligi kerak”.

Shunday holarni uchratamizki bazigi saytlarga karta orqali to‘lov qilayotganimizda kartaga ulanga nomerga SMS tarizda 6 ta raqamdan iborat kod keladi.Lekin bu holat siz saytdan birinchi bor foidalanayotganizda bunday hol bo‘ladi, keyincha esa smartfonga qo‘yilgan bioindifikatsiyasidan foydalanadi va to‘lov amalga oshiriladi. Agar sizning smartfonizni ochishni bilgan odam bu ikki xil usuldan ham foydalana oladi. Lekin boshqa yo‘l orqali ham sizning kartangizdagi summalarni yechib olishi mumkun. Ya’ni kartangizni o‘g‘irlatib qo‘ysangiz va o‘zingiz bilmasangiz u sizni kartangizdan supper market, dorixona va shunga o‘xshash masulyati cheklanmagan savdo komplikislariga borib 50 minggacha bo‘lgan summada harid qilishi va parolsiz terminal orqali pul yechib o‘zmanfatlari ishlatishi mumkun. Keyin u savdo qilgan masulyati cheklangan savdo komplikisi ayibtor bo‘lmaydi chunki bunday terminallar davlat tomonidan savdo komplikisda navbat ko‘payib ketmasligi uchun savda do‘konlarga ishlatishga ruxsat bergan. Sizga yaxshi habar bunday terminalga ega bo‘lgan savdo komplikislari tashqiva ichki kameralar bilon jihozlangan bo‘ladi va siz to‘lov yechib olingan masulyati cheklangan xizmatiga borgan holda masular ishtirokida kamera tekshirib gumondor topiladi. Gumondorga qonun doirasida jazoga tortiriladi va mablag‘ undirilib beriladi.

Bank tizimidagi shifirlar: ASE, RSA, SHA, TLS va SLL dir.

ASE - shifrlash va deshifrlash uchun bitta kalitdan foydalanadi. Bu degani, agar ma’lumot bir tomonlama shifrlangan bo‘lsa, uni boshqa tomonda faqat shu kalit bilan qayta ochish mumkin.AES, xususan, moliyaviy tizimlarda, davlat tashkilotlarida va boshqa xavfsizlikka talab yuqori bo‘lgan sohalarda keng qo‘llaniladi. AES, faqat ilmiy-texnik xavfsizlik sohasida emas, balki real dunyoda ham katta ishonchni qo‘lga kiritgan.

RSA - bu asimmetrik shifrlash algoritmi bo‘lib, u internetda xavfsiz ma’lumot uzatish va autentifikatsiyani ta’minlashda keng qo‘llaniladi. RSA 1977 yilda Ron Rivest, Adi Shamir va Leonard Adleman tomonidan ishlab chiqilgan. RSA algoritmi asosida ishlaydi, ya’ni ikkita kalitdan foydalaniladi: biri ochiq kalit (public key), ikkinchisi esa yopiq kalit (private key).

SHA - bu kriptografik xesh funksiyalar to‘plami bo‘lib, ma’lumotlarni bir tomonlama shifrlashda ishlatiladi. SHA algoritmlari ma’lumotlarga (masalan, matn, fayl yoki boshqa ma’lumotlar) qarshi xesh (yoki hash) qiymatini yaratadi, bu esa ma’lumotning yaxlitligini va o‘zgarmasligini tekshirish uchun ishlatiladi. SHA algoritmlarining asosiy xususiyati shundaki, ular shifrlangan ma’lumotni qayta tiklab bo‘lmaydi — ya’ni, xesh qiymatidan asl ma’lumotni olish mumkin emas. SHA algoritmlari ko‘pincha parollarni saqlashda, ma’lumotlar yaxlitligini tekshirishda va raqamli imzolarni yaratishda ishlatiladi.

TLS - bu internetdagi ma’lumotlarni shifrlash va xavfsiz uzatishni ta’minlash uchun ishlatiladigan kriptografik protokol. TLS — bu internet aloqalarining maxfiyligini, yaxlitligini va autentifikatsiyasini ta’minlashda muhim rol o‘ynaydi. TLS, asosan, HTTPS (Hypertext Transfer Protocol Secure) protokoli yordamida veb-brauzerlar va serverlar o‘rtasidagi xavfsiz aloqalarni yaratish uchun ishlatiladi.Server o‘zining identifikatsiyasini tasdiqlash uchun sertifikatni yuboradi.

Bu sertifikatda serverning ochiq kaliti bo‘ladi. Agar serverning sertifikati ishonchli bo‘lsa, mijoz o‘zaro aloqani davom ettiradi.

SLL - bu internetda ma’lumotlarni xavfsiz uzatish uchun ishlatiladigan kriptografik protokoldir. SSL — bu veb-brauzer va server o‘rtasida ma’lumotlar almashinishni shifrlash va autentifikatsiya qilish uchun ishlatiladigan dastlabki protokol bo‘lib, uning vazifasi foydalanuvchi va veb-server o‘rtasidagi aloqa xavfsizligini ta’minlashdir. SSL 1990-yillarda Netscape tomonidan ishlab chiqilgan va veb-saytlarda, masalan, online banklar, elektron pochta va boshqa xavfsiz xizmatlarda keng qo‘llaniladi.SSL, aloqani shifrlash, autentifikatsiya qilish va ma’lumotlar yaxlitligini ta’minlash uchun quyidagi qadamlarni amalga oshiradi.

Afzalliklari:

Ma’lumotlarni himoyalash – AES , RSA , SHA kabi zamshaxsiy valash ma’lumotlarini ishonchli sifatli himoya – AES, RSA, SHA kabi zamonaviy shifrlash algoritmlarining shaxsiy va ma’lumotlarini ishonchli himoya qiladi.

Kibermakon – TLS va SSL protokoll– TLS va SSL protokollari orqali internet orqali uzatiladigan ma’lumotlar ma’lumotlar ta’minlanadi.

Ikki bosqichli autentifikatsiya – foydalarning akkauntlariga rux.– mahsulotlarning akkauntlariga ruxsatsiz kirishlarning oldi, bu asosiy narsa uchun foydalanish.

Vosital biometriya – Barmoq izitexnik kabi tex – Barmoq iz yuzni texnologiya kabi texnologiya orqali, aniq va ishonchli ishonchli identifikatsiya.

Firibgarlikni boshqarish tizimlariholati .– Sun’iy intellekt asosidagi monitoring tizimlari shubhali tranzaksiyalarni aniqlab, firibgarlikning holati oladi.

Mijozlar ishonchini tasdiqlang – Yuqori tekshiruvbank xizmati– Yuqori darajadagi boshqaruv boshqaruvi bank xizmatlariga nisbatan ishonchni va bank mustahkamlaydi.

Kamchiliklari:

Xush kelibsiz – zamonaviylar– Zamonaviy yordam tizimlarini joriy etish va qo‘-quvvatlash katta mablag‘ talab qiladi.

samaralilar uchun murakkablik – Ba’zi usullar (masalan, ikki bosqichli) foydalanuvchilarga zararlik tug‘dirishi mumkin.

Doimiy yangilanib turuvchi loyihalar –asosiy doimiy rashish – Kiberxavf-xatarlar tez-tez o‘zgarib turadi, bu asosiy muammolarni doimiy ravishda yangilab borishni talab qiladi.

Inson omili – foydalarning za– kasalliklarning zaif parollardan yurishi yoki yordam berishning e’tiborsizligidan surilishi mumkin.

Texnik nosozliklar Ba’zan biometrik yoki tizim tizimlarining ishlamay qolishiga xizmat ko‘rsatishda uzilishlarga olib keladi.

XULOSA: Bank tizimi muayam vazfani bajaruvchi tizim. Ya’ni insonlarni mablag‘ini saqlash va ularga foiz o‘rniga mablag‘ beruvchi joy. Lekin bank tizimi sizga chet el va yurtimiz bo‘ylab to‘lovlar va ximoyalangan tizim. Bu dunyoda ko‘plab insonlar bank tizimidan foidalanadi. Bunga sabab bank tizimidagi shifirlar va sifatli ximoyalar. Eng asosiysi sizda vertual pulingiz bor va bu sizni

cho‘ntagizga ko‘p joy egalamaydi, balki ko‘p miqdordagi pul sig‘imiga ega bo‘lgan kichik bir chip.

Masalan: siz ko‘chaga chiqdingiz va taksi chaqirdingiz u sizni ayilgan manzilga olib bordi va sizning karta(kichik chip)ingizdan pul yechib oldi. Bu bilan siz ko‘chada yursangiz uyda tursangiz ham karta sizga juda katta foida beradi. Qanday yordan beradi uy sharoitida deb o‘ylagan bo‘lsangiz qisqacha shuntirish beraman : “ siz yashab turgan joy yoki kamunal xizmatlar uchun pul to‘laysiz. Tolov qilish uchun malum bir joylarga borishingizga to‘g‘ri keladi, lekin sizda karta bor demak siz bank ilovasi yoki *880# orqali clik tizimiga ulab olganizdan keyin siz harqanday hizmatlarga uydan turib to‘lov qila olasiz” ya’ni 21-asrdagi xavsizlik usularidan ancha farq qiladi. Hozirgi kunda biometrik quluf va bir qancha shifirlar sizning pulingiz va dunyoning tinchligini asrab kelmoqda.

FOIDANILGAN ADABYOTLAR:

1. Sattarov B. X. Bankovskaya sistema i informatsionnaya bezopasnost – Toshkent: “Fan va texnologiya”, 2021. B. 45–58.
2. G‘ulomov S. S., Karimov B. B. Axborot xavfsizligi asoslari – Toshkent: “Iqtisodiyot”, 2020. B. 112–125.
3. Stallings W. Cryptography and Network Security – 7th Edition, Pearson Education, 2020. P. 234–265.
4. ISO/IEC 27001 Information Security Management Systems Requirements – International Organization for Standardization, 2013. – Clause 6–10.
5. O‘zbekiston Respublikasi Prezidenti qarori PQ–4699-son 2020-yil 15-aprel, “Bank tizimini raqamlashtirish chora-tadbirlari to‘g‘risida”.
6. Markaziy bank rasmiy sayti – https://cbu.uz (O‘zbekiston bank tizimining umumiy tuzilmasi va statistik ma’lumotlari uchun – murojaat qilingan sana: 2026-yil 27-aprel)
7. OWASP Foundation – https://owasp.org (Veb-xavfsizlik va autentifikatsiya choralari bo‘yicha amaliy tavsiyalar – murojaat qilingan sana: 2026-yil 27-aprel)
8. “O‘zinfokom” markazi – https://uzinfocom.uz (Biometrik autentifikatsiya va kiberxavfsizlik bo‘yicha tavsiyalar – murojaat qilingan sana: 2026-yil 28-aprel)