ISSN:3030-332X
Impact factor: 9,493
International journal of scientific researchers

KIBER TAHDIDLAR VA RAQAMLI BANK TIZIMLARINI HIMOYA QILISH USULLARI

Shokirov Javohir Xurshid o'g'li
Samarqand iqtisodiyot va servis instituti talabasi

Tursunov Faridun Mustafoyevich
Samarqand iqtisodiyot va servis instituti
Bank ishi kafedrasi assistenti
Doi: https://doi.org/10.5281/zenodo.20428652

Annotatsiya: Bugungi raqamli iqtisodiyot sharoitida bank tizimlarining axborot texnologiyalariga chuqur integratsiyalashuvi moliyaviy xizmatlar samaradorligini oshirgan bo‘lsa-da, shu bilan birga kiber tahdidlar ko‘lamining kengayishiga ham olib keldi. Raqamli bank tizimlari — mobil banking, internet banking va avtomatlashtirilgan to‘lov platformalari — foydalanuvchilarga qulaylik yaratishi bilan bir qatorda, ma’lumotlar xavfsizligi, autentifikatsiya jarayonlari va tarmoq infratuzilmasi zaifliklari kabi muammolarni yuzaga chiqarmoqda. Mazkur maqolada bank sektoriga yo‘naltirilgan asosiy kiber tahdidlar turlari tahlil qilinadi hamda ularni kamaytirish va oldini olishga qaratilgan zamonaviy himoya usullari o‘rganiladi. Xususan, ko‘p bosqichli autentifikatsiya tizimlari, kriptografik himoya algoritmlari, sun’iy intellekt asosida ishlovchi monitoring tizimlari hamda kiberxavfsizlik siyosatining institutsional darajadagi ahamiyati yoritiladi. Shuningdek, raqamli bank tizimlarida inson omili bilan bog‘liq xavflar va ularni minimallashtirish strategiyalari ham tahlil qilinadi. Tadqiqot natijalari bank infratuzilmasining barqarorligini oshirish va moliyaviy axborot xavfsizligini ta’minlash bo‘yicha amaliy tavsiyalar ishlab chiqishga xizmat qiladi.

Kalit so‘zlar: kiber tahdidlar, raqamli bank tizimlari, axborot xavfsizligi, autentifikatsiya, kriptografiya, fintech, kiberxavfsizlik siyosati, moliyaviy texnologiyalar, tarmoq xavfsizligi, sun’iy intellekt monitoringi.

KIRISH

Raqamli transformatsiya bank sektorining ishlash modelini tubdan o‘zgartirdi. Bugungi kunda mobil banking, internet banking va elektron to‘lov tizimlari moliyaviy xizmatlardan foydalanishni sezilarli darajada osonlashtirdi hamda operatsion samaradorlikni oshirdi. Biroq ushbu jarayon bilan parallel ravishda kiber tahdidlarning murakkablashuvi va son jihatdan ortib borishi bank infratuzilmasi uchun jiddiy xavf omiliga aylandi. Kiberjinoyatchilar tomonidan qo‘llanilayotgan usullar — phishing, zararli dasturlar, ijtimoiy muhandislik va tizimlarga ruxsatsiz kirish urinishlari — nafaqat moliyaviy yo‘qotishlarga, balki mijozlarning shaxsiy ma’lumotlari xavfsizligiga ham tahdid solmoqda.

Shu sharoitda raqamli bank tizimlarining barqaror ishlashini ta’minlash faqat texnologik yechimlar bilan cheklanib qolmay, balki kompleks yondashuvni talab etadi. Xususan, axborot xavfsizligi siyosatini takomillashtirish, ko‘p darajali autentifikatsiya tizimlarini joriy etish, kriptografik himoya vositalarini kuchaytirish hamda real vaqt rejimida monitoring qilish mexanizmlarini rivojlantirish dolzarb ahamiyat kasb etadi. Bundan tashqari, inson omili bilan bog‘liq xatoliklar ham kiberxavfsizlik zanjirining eng zaif bo‘g‘inlaridan biri bo‘lib qolmoqda.

Ushbu maqolada raqamli bank tizimlariga yo‘naltirilgan asosiy kiber tahdidlar tahlil qilinadi va ularning iqtisodiy hamda texnologik oqibatlari yoritiladi. Shuningdek, zamonaviy himoya usullari va ularni amaliyotga tatbiq etish imkoniyatlari ko‘rib chiqiladi. Tadqiqotning asosiy maqsadi bank tizimlarida axborot xavfsizligini oshirishga xizmat qiluvchi samarali yondashuvlarni aniqlash va ularni amaliy jihatdan asoslashdan iborat.

ASOSIY QISM

Raqamli bank tizimlarining rivojlanishi moliyaviy xizmatlar arxitekturasini sezilarli darajada o‘zgartirdi. An’anaviy filialga asoslangan model o‘rnini real vaqt rejimida ishlovchi platformalar, mobil

ilovalar va bulutli infratuzilmalarga tayangan tizimlar egallamoqda. Bunday transformatsiya bank xizmatlarining tezligi va qulayligini oshirgan bo‘lsa-da, tizimning hujum yuzasini ham kengaytirdi. Endilikda bank infratuzilmasi faqat ichki tarmoqlar bilan cheklanmay, mijoz qurilmalari, uchinchi tomon API’lari va global internet muhitiga ham bog‘liq murakkab ekotizimga aylandi. Shu sababli har bir yangi integratsiya nuqtasi potentsial zaiflik sifatida baholanadi.

Raqamli bank tizimlariga yo‘naltirilgan kiber tahdidlar ko‘lami va murakkabligi jihatidan turlicha xususiyatga ega. Eng ko‘p uchraydigan tahdidlar qatoriga fishing hujumlari, zararli dasturlar (malware), DDoS hujumlari hamda hisob raqamlariga ruxsatsiz kirish urinishlari kiradi. Fishing hujumlari orqali foydalanuvchilarni aldash va ularning autentifikatsiya ma’lumotlarini qo‘lga kiritish amaliyoti keng tarqalgan. Malware esa bank tizimlariga yashirin kirib, ma’lumotlarni o‘g‘irlash yoki operatsion jarayonlarni izdan chiqarishga xizmat qiladi. Bundan tashqari, “man-in-the-middle” hujumlari orqali uzatilayotgan ma’lumotlar tutib olinishi yoki o‘zgartirilishi mumkin. Yana bir muhim xavf manbai sifatida ichki tahdidlar, ya’ni xodimlar yoki tizimga ruxsatga ega shaxslarning noto‘g‘ri yoki ataylab zararli harakatlari ham qayd etiladi. Ushbu tahdidlar bir-biri bilan kombinatsiyalashgan holda yanada murakkab hujum ssenariylarini shakllantirmoqda.

Mazkur xavflarga qarshi samarali himoya tizimini shakllantirish ko‘p qatlamli yondashuvni talab etadi. Birinchi navbatda, autentifikatsiya va identifikatsiya jarayonlarini kuchaytirish muhim ahamiyatga ega. Ko‘p bosqichli autentifikatsiya (MFA) tizimlari foydalanuvchini tasdiqlash jarayonida bir nechta mustaqil omillardan foydalanib, ruxsatsiz kirish ehtimolini sezilarli darajada kamaytiradi. Shuningdek, kriptografik himoya mexanizmlari, jumladan ma’lumotlarni shifrlash va raqamli imzo texnologiyalari, uzatilayotgan va saqlanayotgan ma’lumotlarning yaxlitligini ta’minlaydi. Zamonaviy yondashuv sifatida sun’iy intellekt va mashinaviy o‘qitish asosida ishlovchi monitoring tizimlari real vaqt rejimida shubhali faoliyatni aniqlash va unga tezkor javob berish imkonini yaratadi. Zero Trust arxitekturasi esa “ishonch yo‘q, har doim tekshir” tamoyiliga asoslanib, tizim ichidagi va tashqarisidagi barcha so‘rovlarni doimiy nazorat ostida ushlab turadi.

Bundan tashqari, bank tizimlarida kiberxavfsizlikni ta’minlash faqat texnik yechimlar bilan cheklanib qolmasligi kerak. Institutsional darajada aniq xavfsizlik siyosatlari ishlab chiqilishi, xodimlar uchun muntazam trening va kiberxavfsizlik bo‘yicha malaka oshirish dasturlari joriy etilishi zarur. Chunki amaliyot shuni ko‘rsatadiki, ko‘plab xavfsizlik buzilishlari texnik nosozlikdan ko‘ra inson omili bilan bog‘liq xatoliklar natijasida yuzaga keladi. Shu nuqtai nazardan, foydalanuvchilar va xodimlarda kiber gigiyena madaniyatini shakllantirish tizim xavfsizligining ajralmas qismi hisoblanadi. Shuningdek, banklar va regulyator organlar o‘rtasida axborot almashinuvi va hamkorlik mexanizmlarini kuchaytirish kiber tahdidlarga qarshi umumiy barqarorlikni oshirishga xizmat qiladi. Natijada, texnologik va tashkiliy choralar uyg‘unligi raqamli bank tizimlarining ishonchliligi va barqarorligini ta’minlashda hal qiluvchi omil bo‘lib qoladi.

XULOSA

Raqamli bank tizimlarining rivojlanishi moliyaviy xizmatlar samaradorligini oshirgan bo‘lsa-da, ularni kiber tahdidlarga nisbatan yanada sezgir holatga keltirdi. Tadqiqot natijalari shuni ko‘rsatadiki, zamonaviy bank infratuzilmasida xavfsizlik masalasi faqat texnik himoya vositalari bilan emas, balki kompleks yondashuv asosida hal etilishi kerak. Chunki hujumlarning murakkablashuvi, ularning avtomatlashtirilgan va ko‘p qatlamli shaklga o‘tishi an’anaviy himoya mexanizmlarining yetarli emasligini ko‘rsatmoqda. Shu sababli bank tizimlarida xavfsizlikni ta’minlashda birinchi navbatda ko‘p darajali autentifikatsiya va doimiy identifikatsiya nazorati tizimlarini to‘liq joriy etish zarur, chunki bu ruxsatsiz kirish xavfini keskin kamaytiradi va foydalanuvchi identifikatsiyasini yanada ishonchli qiladi. Ikkinchidan, barcha ma’lumotlar oqimini shifrlash standartlarini kuchaytirish va kriptografik algoritmlarni muntazam yangilab borish talab etiladi, chunki eskirgan algoritmlar hujumchilar uchun zaif nuqtaga aylanishi mumkin. Uchinchi muhim yo‘nalish sifatida sun’iy intellekt asosida ishlovchi real vaqt monitoring tizimlarini keng joriy etish taklif etiladi, chunki bunday tizimlar odatiy bo‘lmagan xatti-harakatlarni tez aniqlab, hujumning erta bosqichida uni to‘xtatish imkonini beradi. Bundan tashqari, banklar ichida kiberxavfsizlik madaniyatini shakllantirish strategik ahamiyatga ega bo‘lib, xodimlarning xatolari ko‘pincha eng zaif bo‘g‘in bo‘lib qolayotganini hisobga olgan holda muntazam o‘quv dasturlari

va amaliy treninglar joriy etilishi lozim. Shuningdek, regulyator organlar va banklar o‘rtasida kiber tahdidlar bo‘yicha tezkor axborot almashinuvi tizimini yo‘lga qo‘yish umumiy xavfsizlik darajasini oshiradi, chunki bir tashkilotda aniqlangan hujum modeli boshqalar uchun ham erta ogohlantirish vazifasini bajarishi mumkin. Yakuniy xulosa sifatida aytish mumkinki, raqamli bank tizimlarining barqarorligi faqat texnologik yechimlarga emas, balki tashkiliy intizom, inson omili va doimiy yangilanib boruvchi xavfsizlik strategiyalarining uyg‘unligiga bog‘liq bo‘lib, aynan shu integratsiyalashgan yondashuv kelajakda kiber tahdidlar ta’sirini minimal darajaga tushirish imkonini beradi.

Foydalanilgan adabiyotlar

1. Sanayev, M. E. (2024). Kiberxavfsizlik tushunchasi va uning vazifalari. Samarqand iqtisodiyot va servis instituti.
2. G‘aniyev, S. K., G‘aniyev, A. A., & Xodoyqulov, Z. T. (2020). Kiberxavfsizlik asoslari. Toshkent: Aloqachi nashriyoti.
3. Qodirov, F. E., O‘ktamov, M. O‘., & Musirmanov, Sh. U. (2024). Kiberxavfsizlik asoslari. Samarqand: Shahrisabz nashriyoti.
4. Raxmonov, Q. S., & Bekkamov, F. A. (2023). Kiberxavfsizlik siyosati. Toshkent: Zamon poligraf.
5. Jurayev, Q. (2023). Axborot va kiberxavfsizlik asoslari: O‘quv qo‘llanma. Toshkent: Oliy va o‘rta maxsus ta’lim vazirligi tavsiyasiga muvofiq nashr.
6. Oblomuradov, N. N., Ochilov, I. S., & Saidova, D. N. (2022). Iqtisodiy xavfsizlik. Toshkent: Metodist nashriyoti.