BANK FAOLIYATIDA AXBOROT TEXNOLOGIYALARI XAVFSIZLIGIGA TAHDIDLAR VA ULARNI BAHOLASH

Ibragimova Mashhura Yusufboy qizi

Berdaq nomidagi Qoraqalpoq davlat universiteti 2-bosqich magistranti

Annotatsiya. Mazkur maqolada bank faoliyatida axborot texnologiyalari xavfsizligiga tahdidlar va ularni baholash masalalari ilmiy-tahliliy jihatdan o‘rganilgan. Tadqiqotda bank axborot tizimlarining raqamlashtirilishi sharoitida yuzaga kelayotgan tashqi va ichki kiberxavflar, ularning kelib chiqish sabablari hamda bank faoliyatiga ta’siri tahlil qilingan. Shuningdek, axborot xavfsizligi tahdidlarini aniqlash va baholashda qo‘llaniladigan zamonaviy yondashuvlar, risklarni boshqarish metodlari va xalqaro standartlarning ahamiyati yoritilgan. Tadqiqot natijalari bank axborot tizimlarining ishonchliligi va barqarorligini oshirishga qaratilgan ilmiy-amaliy tavsiyalar ishlab chiqish imkonini beradi.

Kalit so‘zlar: bank axborot tizimlari, axborot xavfsizligi, kiberxavfsizlik, tahdidlar, risklarni baholash, kiberhujumlar, raqamli bank xizmatlari, axborotni muhofaza qilish, xavfsizlik siyosati, inson omili.

Аннотация. В данной статье проведён научно-аналитический анализ угроз информационной безопасности в банковской деятельности и методов их оценки. В условиях цифровизации банковских услуг рассмотрены основные внешние и внутренние киберугрозы, причины их возникновения и влияние на устойчивость банковских информационных систем. Особое внимание уделено современным подходам к выявлению и оценке угроз, методам управления рисками, а также роли международных стандартов в обеспечении информационной безопасности. Результаты исследования могут быть использованы для повышения надёжности и безопасности банковских информационных систем.

Ключевые слова: банковские информационные системы, информационная безопасность, кибербезопасность, угрозы, оценка рисков, кибератаки, цифровые банковские услуги, защита информации, политика безопасности, человеческий фактор.

Abstract. This article presents a scientific and analytical study of information technology security threats in banking activities and methods for their assessment. In the context of digitalization of banking services, the main external and internal cyber threats, their causes, and their impact on the stability of banking information systems are analyzed. Particular attention is paid to modern approaches to threat identification and assessment, risk management methods, and the role of international standards in ensuring information security. The research findings

ISSN 3030-3907

provide a basis for developing practical recommendations aimed at enhancing the reliability and security of banking information systems.

Key words: banking information systems, information security, cybersecurity, threats, risk assessment, cyberattacks, digital banking services, information protection, security policy, human factor.

KIRISH.

Bugungi globallashuv va raqamli transformatsiya sharoitida bank tizimi iqtisodiyotning eng muhim va strategik tarmoqlaridan biri sifatida axborot texnologiyalariga bevosita bog‘liq holda faoliyat yuritmoqda. Jahon moliya bozorlarining integratsiyalashuvi, raqamli iqtisodiyotning jadal rivojlanishi hamda moliyaviy xizmatlar ko‘rsatish jarayonlarining avtomatlashtirilishi bank faoliyatining barcha bosqichlarida zamonaviy axborot texnologiyalaridan keng foydalanishni taqozo etmoqda. Natijada banklar nafaqat moliyaviy institut sifatida, balki murakkab axborot tizimlariga ega bo‘lgan texnologik tuzilma sifatida ham faoliyat olib bormoqda. Zamonaviy bank xizmatlari, xususan masofaviy bank xizmatlari, internet va mobil banking, elektron to‘lov tizimlari, banklararo axborot almashinuvi, real vaqt rejimida ishlovchi tranzaksion platformalar hamda avtomatlashtirilgan boshqaruv tizimlari yuqori darajadagi axborot texnologiyalariga asoslangan. Ushbu texnologiyalar bank operatsiyalarining tezkorligi, aniqligi va qulayligini oshirish bilan bir qatorda, mijozlarga xizmat ko‘rsatish sifatini sezilarli darajada yaxshilash imkonini bermoqda. Biroq, raqamli texnologiyalarning keng joriy etilishi bilan birga, axborot xavfsizligi bilan bog‘liq tahdidlar ko‘lami va murakkabligi ham ortib bormoqda.

Bank axborot tizimlarida qayta ishlanadigan ma’lumotlarning yuqori darajadagi maxfiyligi, yaxlitligi va mavjudligi ularni kiberjinoyatchilar uchun eng jozibador nishonlardan biriga aylantiradi. Mijozlarning shaxsiy ma’lumotlari, moliyaviy tranzaksiyalar tafsilotlari, hisobvaraqlar holati, kredit va depozit shartnomalari, autentifikatsiya ma’lumotlari kabi axborot resurslari har qanday noqonuniy aralashuv natijasida jiddiy moliyaviy yo‘qotishlarga olib kelishi mumkin. Bundan tashqari, bunday hodisalar bankning obro‘-e’tiboriga putur yetkazib, mijozlar ishonchining pasayishiga hamda huquqiy va moliyaviy javobgarlikning kuchayishiga sabab bo‘ladi. Shu sababli bank faoliyatida axborot texnologiyalari xavfsizligini ta’minlash masalasi faqat texnik muammo sifatida emas, balki iqtisodiy, tashkiliy va huquqiy jihatlarni o‘z ichiga olgan kompleks masala sifatida qaralmoqda. Bank axborot xavfsizligi nafaqat texnik himoya vositalari, balki xavfsizlik

ISSN 3030-3907

siyosati, xodimlarning axborot madaniyati, normativ-huquqiy bazaning mukammalligi va boshqaruv mexanizmlarining samaradorligi bilan ham bevosita bog‘liqdir.

So‘nggi yillarda kiberhujumlarning murakkablashuvi va xilma-xilligi bank sektorida xavfsizlikni baholash va boshqarish usullarini takomillashtirish zaruratini yuzaga keltirdi. Fishing hujumlari orqali foydalanuvchilarning maxfiy ma’lumotlarini qo‘lga kiritish, zararli dasturlar yordamida bank axborot tizimlariga yashirin kirish, xizmatni rad etish (DDoS) hujumlari orqali bank xizmatlarining uzluksizligini izdan chiqarish, ichki xodimlar tomonidan sodir etiladigan qasddan yoki ehtiyotsizlik bilan bog‘liq tahdidlar, shuningdek axborot tizimlaridagi texnik va dasturiy zaifliklardan foydalanish holatlari bank axborot infratuzilmasiga jiddiy xavf tug‘dirmoqda. Ushbu tahdidlar banklarning barqaror faoliyatiga bevosita ta’sir ko‘rsatib, moliyaviy xavfsizlikka putur yetkazishi mumkin. Bundan tashqari, sun’iy intellekt, avtomatlashtirilgan hujum vositalari va murakkab algoritmlarga asoslangan kiberhujumlarning rivojlanishi axborot xavfsizligi tahdidlarini aniqlash va ularning oldini olish jarayonini yanada murakkablashtirmoqda. An’anaviy himoya usullari ko‘pincha zamonaviy kiberxavflarga nisbatan yetarli darajada samarali bo‘lmay qolmoqda, bu esa banklardan xavfsizlikni ta’minlashning yangi yondashuvlarini joriy etishni talab etadi.

Axborot texnologiyalari xavfsizligiga tahdidlarni samarali boshqarish uchun ularni tizimli ravishda aniqlash, tasniflash va baholash muhim ahamiyatga ega. Tahdidlarni baholash jarayoni bank axborot tizimlarining zaif tomonlarini aniqlash, ehtimoliy xavflarni prognoz qilish va xavfsizlik choralarini rejalashtirish imkonini beradi. Ushbu jarayonda risklarni boshqarish konsepsiyasi, xavfsizlik darajasini baholash modellari, xalqaro standartlar hamda ilg‘or xorijiy va mahalliy amaliyotlardan foydalanish muhim hisoblanadi.

O‘zbekiston bank tizimida ham raqamli bank xizmatlarining keng joriy etilishi axborot xavfsizligi masalalariga bo‘lgan e’tiborni yanada kuchaytirdi. Mamlakatda elektron to‘lovlar ulushining oshishi, masofaviy bank xizmatlarining ommalashuvi, banklararo integratsiya va axborot almashinuvi jarayonlarining faollashuvi bank axborot tizimlarining ishonchliligini ta’minlash bo‘yicha ilmiy va amaliy tadqiqotlarga bo‘lgan ehtiyojni oshirmoqda. Shu nuqtai nazardan, bank faoliyatida mavjud axborot xavfsizligi tahdidlarini chuqur tahlil qilish va ularni baholashning samarali usullarini ishlab chiqish dolzarb ilmiy masala hisoblanadi. Mazkur maqolada bank faoliyatida axborot texnologiyalari xavfsizligiga tahdidlarning asosiy turlari, ularning kelib chiqish sabablari hamda bank axborot tizimlariga ko‘rsatadigan salbiy ta’siri ilmiy-tahliliy jihatdan keng yoritiladi. Shuningdek, tahdidlarni baholash usullari, risklarni boshqarish mexanizmlari va

ISSN 3030-3907

ularning bank xavfsizlik siyosatini shakllantirishdagi o‘rni tahlil qilinib, mavjud muammolar va ularni bartaraf etishning ustuvor yo‘nalishlari asoslab beriladi.

Adabiyotlar tahlili. Axborot texnologiyalari xavfsizligi masalalari bank tizimining raqamlashtirilishi bilan bevosita bog‘liq holda ko‘plab xorijiy va mahalliy tadqiqotchilar tomonidan keng o‘rganilgan. Ilmiy adabiyotlarda bank axborot tizimlarining himoyasi, kiberxavfsizlik tahdidlari, risklarni baholash metodlari hamda xavfsizlikni boshqarish mexanizmlariga alohida e’tibor qaratilgan. Ushbu tadqiqotlar bank sektorida axborot xavfsizligini ta’minlashning nazariy va amaliy asoslarini shakllantirishga xizmat qiladi. Xorijiy tadqiqotlarda bank axborot xavfsizligining asosiy tahdidlari sifatida kiberhujumlar, ichki xodimlar faoliyati bilan bog‘liq xavflar, texnik va dasturiy zaifliklar hamda tashkiliy omillar ko‘rsatiladi. Masalan, Anderson va Moore tomonidan olib borilgan tadqiqotlarda bank tizimlarida axborot xavfsizligi muammolari iqtisodiy nuqtai nazardan tahlil qilinib, kiberjinoyatchilikning moliyaviy oqibatlari va xavfsizlikka yetarli sarmoya kiritilmasligi asosiy muammo sifatida ta’kidlangan. Ularning fikricha, banklar xavfsizlikka xarajatlarni ko‘pincha zarar yuzaga kelgandan keyingina oshiradilar, bu esa risklarni oldindan baholash zaruratini kuchaytiradi.

Stallings, Whitman va Mattord kabi olimlarning ishlarida axborot xavfsizligi uch asosiy tamoyil — maxfiylik, yaxlitlik va mavjudlik (CIA triadasi) asosida ko‘rib chiqilgan. Ushbu yondashuv bank axborot tizimlari uchun ham dolzarb bo‘lib, har bir tamoyilning buzilishi alohida turdagi tahdidlarni keltirib chiqarishi ilmiy jihatdan asoslab berilgan. Mualliflar bank axborot infratuzilmasida ushbu tamoyillarni ta’minlash uchun texnik va tashkiliy choralarni kompleks qo‘llash zarurligini ta’kidlaydilar. Bank sektorida kiberxavfsizlik tahdidlarini tasniflash masalasi ham ko‘plab tadqiqotlarda yoritilgan. Von Solms va Van Niekerk axborot xavfsizligi tahdidlarini tashqi va ichki tahdidlarga ajratgan holda, ichki tahdidlarning ko‘pincha e’tibordan chetda qolishini qayd etadi. Ularning tadqiqotlariga ko‘ra, bank xodimlarining beparvoligi, malaka yetishmasligi yoki ataylab sodir etiladigan harakatlar bank axborot tizimlariga katta zarar yetkazishi mumkin. Shu sababli, xavfsizlik siyosatini shakllantirishda inson omilini hisobga olish muhim hisoblanadi.

Risklarni baholash va boshqarish masalalari bo‘yicha ISO/IEC 27001 va ISO/IEC 27005 standartlari ilmiy adabiyotlarda keng qo‘llaniladigan metodologik asos sifatida ko‘rsatiladi. Ushbu standartlar bank axborot xavfsizligini boshqarish tizimini yaratish, tahdidlarni aniqlash va ularning ehtimoli hamda ta’sir darajasini baholash imkonini beradi. Humphreys va Siponen tomonidan olib borilgan

ISSN 3030-3907

tadqiqotlarda ISO standartlariga asoslangan risklarni baholash banklarda axborot xavfsizligini tizimli ravishda ta’minlashda samarali vosita ekanligi ilmiy jihatdan asoslangan. So‘nggi yillarda sun’iy intellekt va mashinaviy o‘rganish texnologiyalarining bank axborot xavfsizligida qo‘llanilishi bo‘yicha ham ilmiy tadqiqotlar soni ortib bormoqda. Sommer va Paxson o‘z ishlarida an’anaviy xavfsizlik tizimlarining murakkab kiberhujumlarni aniqlashda yetarli emasligini ko‘rsatib, intellektual monitoring va tahdidlarni avtomatik aniqlash tizimlarining afzalliklarini tahlil qilgan. Ushbu yondashuv bank tizimlarida real vaqt rejimida xavfsizlikni baholash imkonini beradi.

MDH davlatlari va O‘zbekiston olimlarining tadqiqotlarida bank axborot xavfsizligi masalalari milliy qonunchilik, iqtisodiy xavfsizlik va raqamli iqtisodiyot bilan uzviy bog‘liq holda o‘rganilgan. Mahalliy tadqiqotchilar bank axborot tizimlarida axborotni muhofaza qilish masalalarini ko‘pincha tashkiliy va huquqiy jihatdan tahlil qiladilar. Ularning ishlarida bank axborot xavfsizligini ta’minlashda normativ-huquqiy hujjatlar, ichki reglamentlar va davlat nazoratining o‘rni alohida ta’kidlanadi. Shuningdek, O‘zbekiston Respublikasi Markaziy banki va tegishli davlat organlari tomonidan qabul qilingan me’yoriy hujjatlar ham ilmiy adabiyotlarda muhim manba sifatida ko‘rsatiladi. Ushbu hujjatlarda banklarda axborot xavfsizligini ta’minlash bo‘yicha minimal talablar, xavfsizlik siyosatini ishlab chiqish va risklarni baholash mexanizmlari belgilangan. Tadqiqotchilar ushbu hujjatlarning amaliyotga joriy etilishi bank axborot tizimlarining barqarorligini oshirishga xizmat qilishini qayd etadilar.

Adabiyotlar tahlili shuni ko‘rsatadiki, bank faoliyatida axborot texnologiyalari xavfsizligiga tahdidlar murakkab va ko‘p omilli xarakterga ega. Mavjud tadqiqotlar asosan tahdidlarni aniqlash va umumiy baholash masalalariga qaratilgan bo‘lsa-da, ularni bank faoliyatining aniq jarayonlari bilan bog‘lab tahlil qilish yetarli darajada yoritilmagan. Shu bois, bank axborot tizimlarida tahdidlarni kompleks baholash va ularni boshqarish mexanizmlarini takomillashtirish bo‘yicha ilmiy izlanishlar dolzarb bo‘lib qolmoqda.

Tadqiqot muhokamasi. O‘tkazilgan ilmiy tahlil va adabiyotlar sharhi bank faoliyatida axborot texnologiyalari xavfsizligiga tahdidlar tizimli va ko‘p qatlamli xarakterga ega ekanligini ko‘rsatdi. Tadqiqot natijalariga ko‘ra, bank axborot tizimlariga tahdidlar nafaqat tashqi kiberhujumlar bilan, balki ichki tashkiliy va inson omiliga bog‘liq xavflar bilan ham chambarchas bog‘liqdir. Ushbu holat bank axborot xavfsizligini faqat texnik vositalar orqali ta’minlash yetarli emasligini, balki kompleks yondashuv zarurligini tasdiqlaydi. Tadqiqot davomida aniqlanganki, zamonaviy bank axborot infratuzilmasida eng ko‘p uchraydigan tahdidlar qatoriga fishing hujumlari, zararli dasturlar orqali ma’lumotlarni

ISSN 3030-3907

o‘g‘irlash, xizmatni rad etish (DDoS) hujumlari hamda autentifikatsiya mexanizmlaridagi zaifliklardan foydalanish holatlari kiradi. Ushbu tahdidlar bank xizmatlarining uzluksizligi va ishonchliligiga bevosita salbiy ta’sir ko‘rsatadi. Ayniqsa, masofaviy bank xizmatlarining kengayishi kiberjinoyatchilar uchun yangi imkoniyatlar yaratmoqda.

Muhokama jarayonida ichki tahdidlarning ahamiyati alohida e’tiborga loyiq ekanligi aniqlandi. Bank xodimlarining axborot xavfsizligi bo‘yicha yetarli bilim va malakaga ega emasligi, xavfsizlik qoidalariga beparvolik bilan munosabatda bo‘lishi yoki ataylab sodir etiladigan noqonuniy harakatlar tashqi hujumlar bilan teng darajada xavf tug‘dirishi mumkin. Bu holat adabiyotlarda ta’kidlangan inson omilining bank axborot xavfsizligidagi hal qiluvchi rolini yana bir bor tasdiqlaydi. Tadqiqot natijalari shuni ko‘rsatadiki, banklarda axborot xavfsizligi tahdidlarini baholash ko‘pincha fragmentar tarzda amalga oshiriladi. Ayrim banklar texnik xavflarni baholashga e’tibor qaratgan bo‘lsa, boshqalari tashkiliy va huquqiy jihatlarni ustuvor deb biladi. Biroq, axborot xavfsizligi tahdidlarining o‘zaro bog‘liqligi ularni yagona tizim sifatida baholash zaruratini yuzaga keltiradi. ISO/IEC 27005 standarti asosida risklarni kompleks baholash yondashuvi ushbu muammoni hal etishda samarali vosita bo‘lishi mumkin.

Muhokama jarayonida aniqlangan muhim jihatlardan biri — xavfsizlik choralarining bank faoliyatiga iqtisodiy ta’siridir. Tadqiqot shuni ko‘rsatadiki, axborot xavfsizligiga yetarli sarmoya kiritilmasligi qisqa muddatda xarajatlarni kamaytirgandek ko‘rinsa-da, uzoq muddatda katta moliyaviy yo‘qotishlarga olib kelishi mumkin. Kiberhujum natijasida yuzaga keladigan to‘xtalishlar, mijozlar ishonchining pasayishi va huquqiy jarimalar bank barqarorligiga jiddiy xavf tug‘diradi. Shu sababli, xavfsizlikni baholash jarayoni strategik rejalashtirish bilan uzviy bog‘lanishi lozim. Tadqiqot doirasida O‘zbekiston bank tizimiga xos jihatlar ham muhokama qilindi. Raqamli bank xizmatlarining jadal rivojlanishi fonida axborot xavfsizligini ta’minlash bo‘yicha normativ-huquqiy bazaning mavjudligi muhim ijobiy omil hisoblanadi. Biroq, amaliyotda ushbu talablarning bajarilishi banklar kesimida bir xil emasligi kuzatildi. Ayrim banklarda xavfsizlik siyosati formal xarakterga ega bo‘lib, real tahdidlarni baholash va monitoring qilish mexanizmlari yetarli darajada rivojlanmagan. Shuningdek, tadqiqot natijalari zamonaviy intellektual texnologiyalarni axborot xavfsizligi tizimlariga joriy etish zaruratini ko‘rsatmoqda. An’anaviy himoya vositalari murakkab va moslashuvchan kiberhujumlarni aniqlashda cheklangan imkoniyatlarga ega. Sun’iy intellekt va mashinaviy o‘rganish asosidagi monitoring tizimlari tahdidlarni real vaqt rejimida aniqlash va baholash imkonini berib, bank axborot tizimlarining barqarorligini oshirishi mumkin.

ISSN 3030-3907

Umuman olganda, tadqiqot muhokamasi bank faoliyatida axborot texnologiyalari xavfsizligiga tahdidlarni baholash masalasi ko‘p qirrali va doimiy takomillashtirishni talab etuvchi jarayon ekanligini ko‘rsatdi. Tahdidlarni samarali boshqarish uchun texnik, tashkiliy, huquqiy va inson omillarini yagona tizimda ko‘rib chiqish zarur. Ushbu yondashuv bank axborot tizimlarining ishonchliligi va barqarorligini ta’minlashda muhim ilmiy va amaliy ahamiyatga ega.

Xulosa. O‘tkazilgan ilmiy-tahliliy tadqiqot natijalari bank faoliyatida axborot texnologiyalari xavfsizligi masalasi bugungi kunda muhim strategik ahamiyatga ega ekanligini ko‘rsatdi. Bank axborot tizimlarining raqamlashtirilishi va masofaviy xizmatlarning kengayishi axborot resurslarini samarali himoyalash zaruratini yanada kuchaytirmoqda. Tadqiqot davomida aniqlanganki, bank axborot tizimlariga tahdidlar tashqi kiberhujumlar, ichki inson omiliga bog‘liq xavflar hamda texnik va tashkiliy zaifliklar bilan uzviy bog‘liqdir. Tahlil natijalariga ko‘ra, axborot texnologiyalari xavfsizligini ta’minlash faqat texnik vositalar bilan cheklanmasligi, balki kompleks yondashuv asosida amalga oshirilishi lozim. Tahdidlarni tizimli ravishda aniqlash va baholash bank faoliyatida yuzaga kelishi mumkin bo‘lgan risklarni kamaytirish, moliyaviy barqarorlikni ta’minlash hamda mijozlar ishonchini mustahkamlashga xizmat qiladi. Shuningdek, xalqaro standartlarga asoslangan risklarni baholash metodlarini joriy etish bank axborot xavfsizligi boshqaruv tizimini takomillashtirish imkonini beradi. Umuman olganda, bank faoliyatida axborot texnologiyalari xavfsizligiga tahdidlarni baholash va ularni boshqarish doimiy monitoring va yangilanishni talab etuvchi jarayon bo‘lib, u bank tizimining ishonchliligi va raqobatbardoshligini oshirishda muhim omil hisoblanadi.

FOYDALANILGAN ADABIYOTLAR

1. Stallings W. Cryptography and Network Security: Principles and Practice. – 7th Edition. – Pearson Education, 2017.
2. Whitman M.E., Mattord H.J. Principles of Information Security. – 6th Edition. – Cengage Learning, 2018.
3. Von Solms R., Van Niekerk J. From Information Security to Cyber Security. – Computers & Security, 2013. – Vol. 38. – P. 97–102.
4. Siponen M., Oinas-Kukkonen H. A Review of Information Security Issues and Respective Research Contributions. – ACM SIGMIS Database, 2007. – Vol. 38(1). – P. 60–80.
5. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. – IEEE Symposium on Security and Privacy, 2010. – P. 305–316.

ISSN 3030-3907

6. Karimov A.A., Islomov B.Sh. Bank axborot tizimlarida axborot xavfsizligini ta’minlash masalalari. – Toshkent: Iqtisodiyot, 2020.
7. Xolmatov D.M. Axborot xavfsizligi asoslari. – Toshkent: Fan va texnologiya, 2019.
8. Ashurov S.S. Raqamli bank xizmatlari va kiberxavfsizlik muammolari. – “Iqtisodiyot va innovatsion texnologiyalar” jurnali, 2021. – №4.

ISSN 3030-3907