ISNN 3030-3907

2026/4
VOLUME 2

DEVELOPMENT OF SCIENCE

ILMIY JURNAL



Development of science

Ilmiy jurnal

2026/4 VOLUME 2

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Асадова Раъно Дилмуратовна
Тошкент Давлат техника университети доценти

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

TIJORAT BANKLARI AXBOROT RESURSLARINI HIMOYALASH SIYOSATINI SHAKLLANTIRISH VA BOSHQARISHNING ZAMONAVIY YONDASHUVLARI

Botirov Fayzullajon Baxtiyarovich
Muxammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Texnika fanlari doktori (DSc)
Email: botirov_fz@mail.ru
Mahmudov Humoyun Turdimahammad o‘g‘li
Muxammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Axborot xavfsizligi yo‘nalishi magistranti (2-bosqich)
Email: humoyunmirzomahmudov99@gmail.com

Annotatsiya. Maqolada tijorat banklarida axborot resurslarini himoyalash siyosatini shakllantirish va boshqarishning zamonaviy yondashuvlari tahlil qilinadi. Bank sektori raqamli transformatsiya, masofaviy xizmatlar, mobil banking, API-integratsiyalar va uchinchi tomon IT-provayderlariga bog‘liqlik kuchayib borayotgan sharoitda kiberxavflarga nisbatan yanada sezgir bo‘lib bormoqda. Xalqaro tashkilotlar ma’lumotlariga ko‘ra, moliyaviy sektor kiberhujumlar ta’siriga eng ko‘p uchraydigan tarmoqlardan biri bo‘lib, kiberinsidentlar soni pandemiyagacha bo‘lgan davrga nisbatan deyarli ikki baravar oshgan, moliyaviy kompaniyalar esa kuzatilgan insidentlarning qariyb beshdan bir qismini tashkil etgan [1]. Shu bilan birga, banklar uchun ma’lumotlar buzilishi qiymati boshqa ko‘plab tarmoqlarga nisbatan yuqoriroq bo‘lib, 2024 yilda moliyaviy sektor uchun o‘rtacha zarar 6,08 mln AQSh dollariga yetgan [2]. Maqolada ISO/IEC 27001, NIST CSF 2.0, DORA va SWIFT CSP kabi xalqaro yondashuvlar asosida banklar uchun kompleks siyosat modeli taklif etiladi.

Kalit so‘zlar: tijorat banki, axborot resurslari, axborot xavfsizligi siyosati, kiberxavfsizlik, risklarni boshqarish, ISO/IEC 27001, NIST CSF 2.0, DORA, SWIFT CSP.

Аннотация. В статье анализируются современные подходы к формированию и управлению политикой защиты информационных ресурсов в коммерческих банках. В условиях цифровой трансформации банковского сектора, расширения дистанционных услуг, мобильного банкинга, API-интеграций и роста зависимости от сторонних IT-провайдеров банки становятся более уязвимыми к киберугрозам. Согласно данным международных организаций, финансовый сектор является одной из наиболее подверженных кибератакам отраслей: количество киберинцидентов увеличилось почти в два раза по сравнению с допандемийным периодом, при этом на финансовые компании приходится около одной пятой всех зафиксированных инцидентов [1]. Кроме

ISSN 3030-3907

того, стоимость утечек данных для банков превышает показатели большинства других отраслей и в 2024 году составила в среднем 6,08 млн долларов США [2]. В статье на основе международных подходов, таких как ISO/IEC 27001, NIST CSF 2.0, DORA и SWIFT CSP, обосновывается необходимость интегрированного подхода к формированию политики защиты информационных ресурсов в коммерческих банках.

Ключевые слова: коммерческий банк, информационные ресурсы, политика информационной безопасности, кибербезопасность, управление рисками, ISO/IEC 27001, NIST CSF 2.0, DORA, SWIFT CSP.

Abstract. This paper analyzes modern approaches to the development and management of information resource protection policies in commercial banks. In the context of digital transformation, the expansion of remote services, mobile banking, API integrations, and increasing reliance on third-party IT providers, banks are becoming more vulnerable to cyber threats. According to international organizations, the financial sector is among the most targeted industries for cyberattacks, with the number of cyber incidents nearly doubling compared to the pre-pandemic period, while financial institutions account for approximately one-fifth of all recorded incidents [1]. Furthermore, the cost of data breaches in the banking sector exceeds that of many other industries, reaching an average of USD 6.08 million in 2024 [2]. Based on international frameworks such as ISO/IEC 27001, NIST CSF 2.0, DORA, and SWIFT CSP, the paper substantiates the need for an integrated approach to developing information security policies in commercial banks.

Keywords: commercial bank, information resources, information security policy, cybersecurity, risk management, ISO/IEC 27001, NIST CSF 2.0, DORA, SWIFT CSP.

KIRISH.

Tijorat banklari zamonaviy iqtisodiyotning eng muhim axborot-intensiv institutlaridan biri hisoblanadi. Ularning faoliyati nafaqat an’anaviy moliyaviy operatsiyalarni bajarish, balki katta hajmdagi axborot resurslarini yig‘ish, saqlash, qayta ishlash va uzatish bilan ham chambarchas bog‘liq. Banklarda mijozlarning shaxsiy identifikatsiya ma’lumotlari, depozit va kredit hisobvaraqlari, to‘lov kartalari rekvizitlari, tranzaksiya tarixlari, biometrik ma’lumotlar, autentifikatsiya vositalari, ichki korporativ hujjatlar, audit loglari va banklararo hisob-kitob ma’lumotlari kabi yuqori qiymatli resurslar jamlangan bo‘ladi. Shu sababli tijorat banklari axborot resurslari kiberjinoyatchilar, firibgar guruhlar va boshqa tahdid manbalari uchun eng jozibador nishonlardan biri hisoblanadi [3][4]. ISO/IEC 27001 axborot xavfsizligini boshqarish tizimi uchun talablarni belgilab, maxfiylik,

ISSN 3030-3907

yaxlitlik va mavjudlik tamoyillarini markaziy o‘ringa qo‘yadi, NIST CSF 2.0 esa xavfsizlikni tashkilot boshqaruvi, himoya, aniqlash, javob va tiklanish bilan bog‘liq uzluksiz jarayon sifatida ko‘radi [3][4].

Bank sektorida raqamli transformatsiya jarayonlarining jadallashuvi ushbu masalani yanada dolzarb qilmoqda. Internet-banking, mobil banking, masofaviy identifikatsiya, API orqali uchinchi tomon xizmatlari bilan integratsiya, ochiq bank tizimlari va bulutli infratuzilmadan foydalanish bank xizmatlarini tezkor va qulay qilgan bo‘lsa-da, bir vaqtning o‘zida hujum yuzasini ham sezilarli darajada kengaytirdi [3][4]. Endilikda bank axborot resurslari faqat ichki serverlar yoki mahalliy tarmoqlar bilan cheklanib qolmay, ko‘p qatlamli raqamli ekotizimda faoliyat yuritmoqda. Bu esa xavfsizlik siyosatini faqat texnik himoya vositalari majmui sifatida emas, balki tashkiliy boshqaruv, risklarni tahlil qilish, uchinchi tomonlar bilan ishlash, hodisalarga javob qaytarish va operatsion barqarorlikni ta’minlash tizimi sifatida ko‘rib chiqishni talab etadi [4][6]. Jahon banki moliyaviy sektorda kiberxavfsizlikni tartibga solish va nazorat qilish bo‘yicha materiallarida ham aynan shu yondashuvga urg‘u berib, banklarda kiberxavfsizlik boshqaruvi korporativ boshqaruv va nazorat mexanizmlari bilan uyg‘unlashtirilishi zarurligini ko‘rsatadi [6].

Xalqaro Valyuta Jamg‘armasi ma’lumotlariga ko‘ra, kiberhujumlar soni COVID-19 pandemiyasidan oldingi davrga nisbatan deyarli ikki baravar oshgan, moliyaviy sektor esa barcha qayd etilgan kiberinsidentlarning qariyb beshdan bir qismini tashkil etgan [1]. Bu ko‘rsatkich moliya tizimi, xususan tijorat banklari, global kiberxavf makonida eng yuqori xavf ostidagi subyektlardan biri ekanini ko‘rsatadi. IMF baholashiga ko‘ra, ayrim yirik kiberhodisalar natijasida yuzaga keladigan ekstremal yo‘qotishlar kamida 2,5 milliard AQSh dollariga yetishi mumkin, bu esa banklar uchun axborot xavfsizligi siyosatini faqat himoya chorasi sifatida emas, balki makroiqtisodiy barqarorlikka ham ta’sir qiluvchi strategik boshqaruv vositasi sifatida shakllantirish lozimligini anglatadi [1].

Moliya sektori bo‘yicha Yevropa kiberxavf manzarasi ham ushbu fikrni tasdiqlaydi. ENISA tomonidan e’lon qilingan moliya sektori tahdidlar tahliliga ko‘ra, 2023 yil yanvaridan 2024 yil iyunigacha bo‘lgan davrda Yevropa Ittifoqi va unga qo‘shni hududlarga taalluqli moliyaviy sektorda 488 ta ommaga ma’lum bo‘lgan insident ko‘rib chiqilgan [5]. Mazkur ma’lumotlar banklar, to‘lov xizmatlari va boshqa moliyaviy institutlar faoliyati raqamlashtirilgan sari tahdidlar soni va murakkabligi ortib borayotganini ko‘rsatadi. Ayniqsa, fishing, credential compromise, ransomware, DDoS, uchinchi tomon provayderlari bilan bog‘liq risklar va xizmatlar uzluksizligiga tahdid soluvchi hujumlar bank infratuzilmasining zaif nuqtalarini namoyon etmoqda [5]. Shu sababli banklarda

ISSN 3030-3907

axborot resurslarini himoyalash siyosatini ishlab chiqish an’anaviy antivirus, firewall yoki kirishni cheklash bilan kifoyalanmasdan, tahdidlarni oldindan baholash, monitoring qilish va barqaror tiklanish choralarini ham o‘z ichiga olishi kerak [4][5].

Bugungi sharoitda tijorat banklarida axborot resurslarini himoyalash siyosatini shakllantirish va boshqarish nafaqat IT bo‘linmasining texnik vazifasi, balki butun bank boshqaruv tizimining strategik funksiyasi sifatida qaralmoqda [3][4][6]. Bunday siyosat bankning axborot aktivlarini identifikatsiya qilish, ularni kritik darajasiga ko‘ra tasniflash, tahdid va zaifliklarni baholash, nazorat choralarini tanlash, insidentlarga javob qaytarish hamda uzluksiz audit va takomillashtirish mexanizmlarini o‘z ichiga olishi lozim [3][4]. Demak, tijorat banklarida axborot resurslarini himoyalash siyosatini zamonaviy yondashuvlar asosida shakllantirish masalasi ilmiy va amaliy jihatdan dolzarb bo‘lib, bank tizimining ishonchliligi, mijozlar ishonchi va moliyaviy barqarorlikni ta’minlashning asosiy omillaridan biri hisoblanadi [1][5][6].

Muammoning dolzarbligi va tadqiqot zarurati

Tijorat banklari faoliyatida axborot resurslari strategik ahamiyatga ega bo‘lib, ular nafaqat operatsion jarayonlarning texnologik asosi, balki bankning umumiy barqarorligi, mijozlar ishonchi, bozordagi obro‘si va regulyativ talablarga muvofiqligining muhim omili hisoblanadi. Bank tizimida qayta ishlanadigan ma’lumotlar hajmining ortishi, xizmatlarning to‘liq raqamlashtirilishi hamda moliyaviy operatsiyalarning global integratsiyalashuvi sharoitida axborot resurslarini himoyalash masalasi yanada dolzarb tus olmoqda. Shu sababli bank infratuzilmasida yuzaga keladigan har qanday kiberinsidentlar nafaqat texnik nosozlik yoki lokal muammo sifatida, balki kompleks iqtisodiy, huquqiy va reputatsion oqibatlarga olib keluvchi hodisa sifatida baholanadi [1][2].

Xususan, kiberxavfsizlik bilan bog‘liq insidentlar natijasida bank xizmatlarining vaqtincha yoki uzoq muddatga to‘xtashi, mijozlarga xizmat ko‘rsatish sifatining pasayishi, moliyaviy operatsiyalarning buzilishi, shaxsiy ma’lumotlarning oshkor bo‘lishi va firibgarlik holatlarining ortishi kuzatiladi. Bundan tashqari, bunday hodisalar bankning regulyatorlar oldidagi majburiyatlarini buzishiga, moliyaviy jarimalar va sanksiyalarga duch kelishiga ham sabab bo‘ladi. Natijada bankning bozordagi ishonchliligi pasayadi va uzoq muddatli iqtisodiy zarar yuzaga keladi [1][2].

Zamonaviy statistik tahlillar ham ushbu muammoning dolzarbligini tasdiqlaydi. IBM’ning 2024 yilgi hisobotiga ko‘ra, global miqyosda ma’lumotlar sizib chiqishining o‘rtacha qiymati 4,88 mln AQSh dollarini tashkil etgan bo‘lsa, aynan moliyaviy sektor tashkilotlari uchun bu ko‘rsatkich 6,08 mln dollarga yetgan

ISSN 3030-3907

[2]. Bu esa bank tizimida axborot xavfsizligi buzilishining iqtisodiy zarari boshqa tarmoqlarga nisbatan ancha yuqori ekanini ko‘rsatadi. Xalqaro Valyuta Jamg‘armasi esa kiberinsidentlar natijasida yuzaga keladigan ekstremal yo‘qotishlar hajmi 2017 yildan buyon keskin oshib, to‘rt baravardan ko‘proqqa ortganini hamda ayrim hollarda 2,5 milliard AQSh dollariga yetishi mumkinligini qayd etadi [1][7]. Bu esa muammoning nafaqat mikroiqtisodiy, balki makroiqtisodiy darajada ham muhim ekanligini anglatadi.

Shu bilan birga, banklarda axborot xavfsizligini ta’minlash bo‘yicha mavjud amaliyotlar ko‘pincha fragmentar xarakterga ega. Ya’ni, ko‘plab tijorat banklarida axborot xavfsizligi siyosati mavjud bo‘lsa-da, u ko‘pincha formal hujjat sifatida ishlab chiqilgan bo‘lib, real boshqaruv jarayonlariga to‘liq integratsiyalanmagan bo‘ladi. Xususan, quyidagi muammolar kuzatiladi:

- xavfsizlik siyosatining real vaqt monitoring tizimlari bilan bog‘lanmaganligi;
- uchinchi tomon (third-party) xizmat ko‘rsatuvchilar ustidan yetarli nazoratning mavjud emasligi;
- insidentlarga tezkor javob berish mexanizmlarining sustligi;
- biznes uzluksizligini ta’minlash (BCP/DRP) rejalarining yetarli darajada ishlab chiqilmaganligi;
- xavfsizlik siyosatining bank boshqaruv tizimi va risk-menejment bilan integratsiyalanmaganligi [3][8].

Bundan tashqari, zamonaviy bank infratuzilmasining murakkablashuvi, ya’ni bulutli texnologiyalar, API-ekotizimlar, fintech integratsiyalari va masofaviy xizmatlarning kengayishi mavjud xavfsizlik siyosatlarini qayta ko‘rib chiqishni talab etmoqda. An’anaviy yondashuvlar zamonaviy kiberxavflarning dinamik tabiati, murakkab hujum ssenariylari va ko‘p bosqichli tahdidlarga qarshi yetarli darajada samarali emasligi kuzatilmoqda [3][8].

Shu munosabat bilan, maqolaning ilmiy muammosi quyidagicha shakllantiriladi:

tijorat banklarida axborot resurslarini himoyalash siyosatini zamonaviy kiberxavflar, xalqaro regulyativ talablar va raqamli bank infratuzilmasining o‘ziga xos xususiyatlarini hisobga olgan holda qanday shakllantirish va samarali boshqarish mumkin?

Mazkur muammoni hal etish bank tizimida axborot xavfsizligini yangi bosqichga olib chiqish, risklarni kamaytirish, xizmatlar uzluksizligini ta’minlash va moliyaviy tizim barqarorligini mustahkamlashga xizmat qiladi [1][3][7].

TADQIQOT METODOLOGIYASI.

Mazkur tadqiqot tijorat banklarida axborot resurslarini himoyalash siyosatini shakllantirish va boshqarishning zamonaviy yondashuvlarini asoslashga qaratilgan

ISSN 3030-3907

bo‘lib, u yuqorida ko‘rib chiqilgan dolzarblik hamda adabiyotlar tahlili natijalari bilan uzviy bog‘liq holda ishlab chiqildi. Tadqiqot metodologiyasi xalqaro standartlar va amaliy yondashuvlarga tayangan holda kompleks tarzda shakllantirildi hamda bank axborot tizimlarining o‘ziga xos xususiyatlarini hisobga oldi.

Birinchidan, tadqiqotda **kontent-tahlil usuli** qo‘llanildi. Ushbu usul orqali axborot xavfsizligini boshqarish sohasidagi yetakchi xalqaro standartlar va rasmiy hisobotlar tizimli ravishda o‘rganildi. Xususan, ISO/IEC 27001 standarti, NIST Cybersecurity Framework 2.0, Yevropa Ittifoqining DORA reglamenti, SWIFT Customer Security Programme (CSP), ENISA tahdidlar tahlili hamda IMF hisobotlari tahlil qilindi [1][3][4][5][9][10]. Kontent-tahlil natijasida tijorat banklarida xavfsizlik siyosatini shakllantirishda asosiy e’tibor risklarni boshqarish, nazorat mexanizmlarini joriy etish, insidentlarga javob berish va operatsion barqarorlikni ta’minlashga qaratilishi zarurligi aniqlashtirildi. Shu bilan birga, mazkur manbalar bank tizimida xavfsizlik siyosatini ishlab chiqishda xalqaro standartlarga moslik muhim omil ekanligini ko‘rsatdi.

Ikkinchidan, tadqiqotda **tizimli yondashuv (system approach)** qo‘llanildi. Ushbu yondashuvga ko‘ra, axborot xavfsizligi siyosati alohida choralar yoki texnik vositalar yig‘indisi sifatida emas, balki o‘zaro bog‘langan va bir-birini to‘ldiruvchi komponentlardan iborat yagona tizim sifatida ko‘rib chiqildi. Xususan, xavfsizlik siyosati boshqaruv (governance), texnologik infratuzilma, inson omili, operatsion jarayonlar va audit mexanizmlarining o‘zaro integratsiyasi asosida tahlil qilindi [3][4]. Ushbu yondashuv banklarda xavfsizlik siyosatini amaliy boshqaruv tizimi bilan bog‘lash, uning samaradorligini oshirish va qaror qabul qilish jarayonlariga integratsiyalash imkonini beradi.

Uchinchidan, tadqiqotda **riskga asoslangan yondashuv (risk-based approach)** asosiy metod sifatida tanlandi. Ushbu yondashuv ISO va NIST standartlarida belgilangan tamoyillarga mos ravishda xavfsizlik siyosatini shakllantirishda ustuvor yo‘nalishlarni aniqlash imkonini beradi [3][4]. Risk tahdid ehtimoli va uning ta’sir darajasi asosida baholanadi. Soddalashtirilgan ko‘rinishda risk quyidagi model orqali ifodalanadi:

$$R = P \times I$$

bu yerda: R — risk darajasi, P — tahdid ro‘y berish ehtimoli,
I — tahdidning zarar darajasi.

Mazkur model bank axborot tizimlarida ustuvor himoya obyektlarini aniqlashda qo‘llaniladi. Jumladan, yuqori risk darajasiga ega bo‘lgan resurslar — mijoz ma’lumotlari bazasi, to‘lov tizimlari, autentifikatsiya serverlari hamda tranzaksiya monitoringi platformalari — alohida himoya choralarini talab qiladi.

ISSN 3030-3907

To‘rtinchidan, tadqiqot metodologiyasida xavfsizlik siyosatini shakllantirish jarayonida uning amaliy qo‘llanish imkoniyatlari ham hisobga olindi. Bunda xavfsizlik siyosati nafaqat nazariy hujjat, balki bank infratuzilmasida real ishlaydigan boshqaruv mexanizmi sifatida ko‘rib chiqildi. Shu nuqtayi nazardan, siyosatni ishlab chiqishda monitoring, nazorat, audit va uzluksiz takomillashtirish elementlari ham muhim tarkibiy qism sifatida qaraldi [4][9]. Bu esa xavfsizlik siyosatini bank faoliyatining ajralmas qismiga aylantirishga xizmat qiladi.

Beshinchidan, metodologiya doirasida banklarda axborot resurslarini himoyalash siyosatini shakllantirish jarayoni bosqichma-bosqich amalga oshiriladigan tizim sifatida qaraldi. Ya’ni, resurslarni aniqlash, tahdidlarni baholash, risklarni hisoblash, nazorat choralarini tanlash va ularni joriy etish bosqichlari o‘zaro bog‘langan holda tahlil qilindi [3][4][10]. Ushbu yondashuv xavfsizlik siyosatini doimiy ravishda yangilab borish va uni zamonaviy kiberxavflarga moslashtirish imkonini beradi.

Shunday qilib, mazkur metodologiya tijorat banklarida axborot resurslarini himoyalash siyosatini shakllantirish va boshqarishda kompleks, tizimli va riskga asoslangan yondashuvni ta’minlaydi. Ushbu yondashuv bank tizimida axborot xavfsizligini oshirish, risklarni kamaytirish hamda xizmatlar uzluksizligini ta’minlashga xizmat qiladi [1][3][4][9].

Tijorat banklarida himoyalanishi lozim bo‘lgan asosiy axborot resurslari

Tijorat banklarida axborot resurslarini himoyalash siyosatini samarali shakllantirish uchun, avvalo, himoyalanishi lozim bo‘lgan resurslarni to‘g‘ri aniqlash va ularni tizimli ravishda tasniflash muhim ahamiyat kasb etadi. Yuqorida ko‘rib chiqilgan metodologik yondashuvlar asosida bank axborot resurslari funksional jihatdan bir nechta asosiy qatlamlarga ajratildi. Bunday tasniflash xavfsizlik siyosatini ishlab chiqishda ustuvor yo‘nalishlarni belgilash hamda risklarni boshqarish jarayonini samarali tashkil etishga xizmat qiladi [3][4].

Birinchi qatlam — **mijozlarga oid ma’lumotlar** bo‘lib, ular bank faoliyatining eng muhim va eng yuqori darajada himoyalanishi zarur bo‘lgan axborot resurslari hisoblanadi. Ushbu qatlamga shaxsiy identifikatsiya ma’lumotlari, biometrik ma’lumotlar, bank hisobvaraqlari, to‘lov kartalari rekvizitlari, kredit tarixi, shartnomaviy hujjatlar va boshqa maxfiy ma’lumotlar kiradi. Mazkur ma’lumotlarning noqonuniy oshkor bo‘lishi yoki buzilishi mijozlar xavfsizligiga bevosita tahdid soladi hamda bankning obro‘siga jiddiy zarar yetkazadi. Shu bilan birga, bunday holatlar regulyativ talablarning buzilishiga va moliyaviy sanksiyalarga olib kelishi mumkin [2][8]. Shuning uchun ushbu qatlam uchun maxfiylik va kirishni qat’iy nazorat qilish mexanizmlari ustuvor ahamiyat kasb etadi.

ISSN 3030-3907

Ikkinchi qatlam — **tranzaksion resurslar** bo‘lib, ular bank tizimining operatsion faoliyatini ta’minlaydi. Ushbu resurslarga to‘lov topshiriqlari, banklararo hisob-kitoblar, SWIFT xabarlari, valyuta operatsiyalari hamda antifrod tizimlarida qayd etiladigan ma’lumotlar kiradi. Tranzaksion resurslarning buzilishi moliyaviy operatsiyalarning noto‘g‘ri bajarilishiga yoki firibgarlik holatlarining yuzaga kelishiga olib kelishi mumkin. SWIFT tomonidan joriy etilgan Customer Security Programme (CSP) va Customer Security Controls Framework (CSCF) ushbu qatlamni himoyalash uchun minimal xavfsizlik talablarini belgilaydi, bu esa tranzaksion tizimlarning global moliyaviy infratuzilmadagi muhim o‘rnini ko‘rsatadi [10][11].

Uchinchi qatlam — **infratuzilmaviy resurslar** bo‘lib, ular bankning texnologik asosini tashkil etadi. Ushbu qatlamga serverlar, tarmoq qurilmalari, ma’lumotlar markazlari, bulutli xizmatlar, zaxira tizimlari hamda autentifikatsiya va avtorizatsiya servislar kiradi. Mazkur resurslar bank xizmatlarining uzluksiz ishlashini ta’minlaydi. Ularning ishdan chiqishi yoki buzilishi bank xizmatlarining to‘xtashiga, mijozlarga xizmat ko‘rsatishning izdan chiqishiga olib kelishi mumkin. Yevropa Markaziy Banki tomonidan o‘tkazilgan kiberbarqarorlik testlari ham aynan infratuzilmaviy resurslarning barqaror ishlashi va tiklanish imkoniyatlari banklar uchun muhim ekanligini ko‘rsatgan [12][13].

To‘rtinchi qatlam — **boshqaruv va audit axboroti** bo‘lib, ushbu qatlam bankda xavfsizlik siyosatini monitoring qilish va boshqarish uchun zarur bo‘lgan ma’lumotlarni o‘z ichiga oladi. Bu yerga tizim loglari, SIEM hodisalari, audit yozuvlari, insidentlar reyestri, risk baholash hujjatlari hamda muvofiqlik materiallari kiradi. Ushbu ma’lumotlar bankda xavfsizlik darajasini baholash, tahdidlarni aniqlash va boshqaruv qarorlarini qabul qilishda muhim ahamiyatga ega. NIST va DORA yondashuvlarida monitoring va audit mexanizmlari xavfsizlik siyosatining ajralmas elementi sifatida ko‘riladi [4][9].

Shunday qilib, tijorat banklarida axborot resurslarini himoyalash siyosatini samarali tashkil etish uchun barcha resurslarni kompleks tarzda tahlil qilish, ularni qatlamlar bo‘yicha tasniflash va har bir qatlam uchun mos himoya choralarini belgilash zarur hisoblanadi. Bunday yondashuv risklarni kamaytirish, xizmatlar uzluksizligini ta’minlash hamda bank tizimining umumiy xavfsizlik darajasini oshirishga xizmat qiladi [3][4][10].

Tijorat banklarida axborot xavfsizligini ta’minlash yondashuvlarining taqqoslama tahlili

Yuqorida ko‘rib chiqilgan xalqaro standartlar va amaliy yondashuvlar tijorat banklarida axborot resurslarini himoyalash siyosatini shakllantirishda muhim metodologik asos bo‘lib xizmat qiladi. Biroq ushbu yondashuvlarning har biri turli

ISSN 3030-3907

maqsad va vazifalarga yo‘naltirilgan bo‘lib, ularni amaliy jihatdan solishtirish zarur hisoblanadi.

ISO/IEC 27001 standarti axborot xavfsizligini boshqarish tizimini tashkil etish uchun eng keng tarqalgan yondashuvlardan biri bo‘lib, u xavfsizlik siyosatini tizimli ravishda ishlab chiqish, joriy etish va nazorat qilish imkonini beradi [3]. Ushbu yondashuvning asosiy afzalligi uning universalligi va standartlashtirilganligi bo‘lsa, kamchiligi sifatida uning nisbatan statik xarakterga ega ekanligi va tez o‘zgaruvchan kiberxavflarga moslashuvchanligi cheklanganligini ko‘rsatish mumkin.

NIST Cybersecurity Framework 2.0 esa xavfsizlikni boshqarishning moslashuvchan modelini taklif etadi. Ushbu yondashuv tashkilotlarga xavfsizlik jarayonlarini boshqaruv, aniqlash, himoya qilish, aniqlash, javob berish va tiklanish bosqichlari asosida tashkil etish imkonini beradi [4]. NIST modelining ustunligi uning dinamikligi va riskga asoslangan yondashuvga tayanganligidadir. Biroq, ushbu yondashuv umumiy xarakterga ega bo‘lib, uni aniq tashkilotga moslashtirish qo‘shimcha metodik ishlanmalarni talab qiladi.

DORA reglamenti esa moliyaviy sektor uchun maxsus ishlab chiqilgan bo‘lib, banklar faoliyatida axborot xavfsizligini ta’minlashda regulyativ yondashuvni kuchaytiradi [9]. Ushbu yondashuvning afzalligi shundaki, u operatsion barqarorlik, insidentlarga javob berish va uchinchi tomon xizmat ko‘rsatuvchilar ustidan nazoratni majburiy talab sifatida belgilaydi. Shu bilan birga, uning qo‘llanilishi asosan Yevropa Ittifoqi hududi bilan chegaralangan.

SWIFT Customer Security Programme (CSP) va uning Customer Security Controls Framework (CSCF) banklar uchun amaliy xavfsizlik choralarini belgilaydi [10][11]. Ushbu yondashuv ayniqsa xalqaro to‘lov tizimlari bilan ishlovchi banklar uchun muhim hisoblanadi. Uning ustunligi aniq texnik va tashkiliy nazorat choralarini belgilashidadir, ammo u faqat SWIFT infratuzilmasi doirasida qo‘llaniladi.

Yuqoridagi yondashuvlarni umumlashtirgan holda, ularni quyidagi 1-jadval orqali taqqoslash mumkin:

1-jadval

Yondashuv	**Afzalliklari**	**Kamchiliklari**
ISO/IEC 27001	tizimli va standartlashgan	moslashuvchanligi past
NIST CSF 2.0	moslashuvchan, riskga asoslangan	umumiy xarakterga ega
DORA	regulyativ va majburiy talablar	hududiy cheklangan
SWIFT CSP	amaliy va aniq nazoratlar	tor yo‘nalishga ega

Taqqoslama tahlil shuni ko‘rsatadiki, yuqoridagi yondashuvlarning hech biri alohida holda tijorat banklarida axborot xavfsizligini to‘liq ta’minlay olmaydi. Har

ISSN 3030-3907

bir yondashuv ma’lum bir jihatni qamrab oladi: ISO — tizimlilikni, NIST — moslashuvchanlikni, DORA — regulyativ barqarorlikni, SWIFT esa amaliy xavfsizlik nazoratlarini ta’minlaydi.

Shu sababli tijorat banklarida axborot resurslarini himoyalash siyosatini shakllantirishda ushbu yondashuvlarni integratsiyalashgan holda qo‘llash maqsadga muvofiq hisoblanadi. Bunday yondashuv banklarda xavfsizlik siyosatini yanada samarali boshqarish, risklarni kamaytirish va xizmatlar uzluksizligini ta’minlash imkonini beradi [3][4][9][10].

XULOSA.

Mazkur maqolada tijorat banklarida axborot resurslarini himoyalash siyosatini shakllantirish va boshqarishning zamonaviy yondashuvlari tahlil qilindi. Tadqiqot natijalari shuni ko‘rsatdiki, bank tizimida axborot xavfsizligi masalasi nafaqat texnik, balki strategik boshqaruv darajasida hal etilishi zarur.

Tahlillar asosida aniqlanishicha, zamonaviy bank infratuzilmasining murakkablashuvi, raqamli xizmatlar kengayishi va kiberxavflarning ortib borishi xavfsizlik siyosatini yangi yondashuvlar asosida qayta ko‘rib chiqishni talab etadi. ISO/IEC 27001, NIST CSF 2.0, DORA va SWIFT CSP kabi yondashuvlar banklarda xavfsizlikni ta’minlashda muhim rol o‘ynaydi, biroq ularning har biri alohida holda yetarli darajada samarali emas.

Shu asosda, tijorat banklarida axborot resurslarini himoyalash siyosatini shakllantirishda integratsiyalashgan yondashuvni qo‘llash zarurligi asoslandi. Bunday yondashuv turli standartlar va amaliy choralarni birlashtirish orqali xavfsizlik tizimining samaradorligini oshirish, risklarni kamaytirish hamda xizmatlar uzluksizligini ta’minlash imkonini beradi.

Natijada, taklif etilgan yondashuv bank tizimida axborot xavfsizligini mustahkamlash, mijozlar ishonchini oshirish va moliyaviy barqarorlikni ta’minlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. International Monetary Fund. *Global Financial Stability Report: Cyber Risk – A Growing Concern for Macro-Financial Stability*. – Washington, DC: IMF, 2024.
2. IBM Security. *Cost of a Data Breach Report 2024*. – IBM Corporation, 2024.
3. International Organization for Standardization. *ISO/IEC 27001:2022 Information Security Management Systems – Requirements*. – Geneva: ISO, 2022.
4. National Institute of Standards and Technology. *Cybersecurity Framework (CSF) 2.0*. – Gaithersburg, MD: NIST, 2024.
5. European Union Agency for Cybersecurity. *ENISA Threat Landscape for the Finance Sector 2024*. – ENISA, 2025.

ISSN 3030-3907

6. World Bank. *Financial Sector's Cybersecurity: Regulations and Supervision*. – Washington, DC: World Bank, 2018.
7. International Monetary Fund. *Cyber Risk, Financial Stability and Monetary Policy*. – IMF Departmental Paper, 2023.
8. World Bank. *Cybersecurity and Financial Sector Development: Challenges and Solutions*. – Washington, DC: World Bank, 2020.
9. European Union. *Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554*. – Official Journal of the European Union, 2022.
10. SWIFT. *Customer Security Programme (CSP)*. – SWIFT, 2024.
11. SWIFT. *Customer Security Controls Framework (CSCF)*. – SWIFT, 2024.
12. European Central Bank. *Cyber Resilience Stress Test for Banks 2024*. – ECB, 2024.
13. European Central Bank. *Supervisory Priorities for 2024–2026*. – ECB, 2023.

ISSN 3030-3907