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 BANKLARIDA KIBERXAVFSIZLIK SIYOSATINI ISHLAB CHIQISH VA BOSHQARISH STRATEGIYALARI

Botirov Fayzullajon Baxtiyarovich
Texnika fanlari doktori (DSc) Muxammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
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. Mazkur maqolada tijorat banklarida kiberxavfsizlik siyosatini ishlab chiqish va boshqarishning dolzarb masalalari kompleks tarzda tahlil qilinadi. Bank tizimlarida yuzaga kelayotgan zamonaviy kiber tahdidlar, jumladan, tarmoq hujumlari, zararli dasturlar, fishing va ma’lumotlar sizib chiqishi kabi xavf omillarining xususiyatlari o‘rganiladi hamda ularning bank infratuzilmasiga ta’siri baholanadi. Shuningdek, amaliyotda qo‘llanilayotgan kiberxavfsizlik siyosatlari va boshqaruv yondashuvlari tahlil qilinib, ularning samaradorligi hamda mavjud kamchiliklari aniqlanadi. Xususan, xavfsizlik siyosatlarining statikligi, tahdidlarga moslashuvchanlik darajasining pastligi va risklarni boshqarish mexanizmlarining yetarli darajada integratsiyalashmaganligi asosiy muammolar sifatida ko‘rib chiqiladi. Tadqiqot jarayonida tizimli tahlil, qiyosiy tahlil hamda risklarni baholash usullaridan foydalanildi. Ushbu takliflar bank tizimlarida axborot xavfsizligini oshirish, kiber tahdidlarning oldini olish va ularning salbiy oqibatlarini minimallashtirishga xizmat qiladi.

Kalit so‘zlar: kiberxavfsizlik, tijorat banklari, axborot xavfsizligi siyosati, kiber tahdidlar, risklarni boshqarish, xavfsizlik strategiyalari, bank tizimlari

Аннотация. В данной статье комплексно анализируются актуальные вопросы разработки и управления политикой кибербезопасности в коммерческих банках. Изучаются современные киберугрозы, возникающие в банковских системах, включая сетевые атаки, вредоносное программное обеспечение, фишинг и утечки данных, а также оценивается их влияние на банковскую инфраструктуру. Кроме того, проводится анализ применяемых на практике политик кибербезопасности и управленческих подходов, выявляются их эффективность и существующие недостатки. В частности, основными проблемами рассматриваются статичность политик безопасности, низкий уровень адаптивности к угрозам и недостаточная интеграция механизмов управления рисками. В ходе исследования использовались методы системного анализа, сравнительного анализа и

ISSN 3030-3907

оценки рисков. Предложенные решения направлены на повышение уровня информационной безопасности банковских систем, предотвращение киберугроз и минимизацию их негативных последствий.

Ключевые слова: кибербезопасность, коммерческие банки, политика информационной безопасности, киберугрозы, управление рисками, стратегии безопасности, банковские системы.

Abstract. This article provides a comprehensive analysis of the актуal issues related to the development and management of cybersecurity policies in commercial banks. It examines modern cyber threats in banking systems, including network attacks, malware, phishing, and data breaches, and evaluates their impact on banking infrastructure. Furthermore, the study analyzes existing cybersecurity policies and management approaches applied in practice, identifying their effectiveness and existing shortcomings. In particular, key issues such as the static nature of security policies, low adaptability to emerging threats, and insufficient integration of risk management mechanisms are highlighted. The research employs system analysis, comparative analysis, and risk assessment methods. The proposed solutions aim to enhance information security in banking systems, prevent cyber threats, and minimize their negative consequences.

Keywords: cybersecurity, commercial banks, information security policy, cyber threats, risk management, security strategies, banking systems

KIRISH.

Zamonaviy raqamli transformatsiya sharoitida tijorat banklari faoliyati axborot-kommunikatsiya texnologiyalari asosida tashkil etilib, bank xizmatlarining aksariyati raqamli platformalar orqali amalga oshirilmoqda. Internet-banking, mobil banking, onlayn to‘lov tizimlari va bulutli texnologiyalarning keng joriy etilishi bank xizmatlarining qulayligini oshirgan bo‘lsa-da, ushbu jarayonlar kiberxavfsizlikka oid yangi xavf va tahdidlarni yuzaga keltirmoqda [1].

Moliyaviy sektor kiberjinoyatchilar uchun eng jozibador yo‘nalishlardan biri hisoblanadi. Xalqaro tahlillarga ko‘ra, bank va moliya tashkilotlariga qaratilgan kiberhujumlar soni yil sayin ortib bormoqda, ayniqsa ma’lumotlar sizib chiqishi, fishing, zararli dasturlar va DDoS hujumlari keng tarqalgan tahdidlar qatoriga kiradi [2]. Ushbu tahdidlar bank infratuzilmasining uzluksiz ishlashiga salbiy ta’sir ko‘rsatib, moliyaviy yo‘qotishlar va mijozlar ishonchining pasayishiga olib keladi [3].

Kiberxavfsizlikni ta’minlash maqsadida xalqaro miqyosda turli standartlar va metodologiyalar ishlab chiqilgan. Jumladan, ISO/IEC 27001 axborot xavfsizligini boshqarish tizimini tashkil etish uchun asosiy talablarni belgilab

ISSN 3030-3907

beradi, COBIT va ITIL yondashuvlari esa axborot texnologiyalarini boshqarish va nazorat qilish mexanizmlarini taklif etadi [4]. Shuningdek, zamonaviy yondashuvlar doirasida “Zero Trust Architecture” konsepsiyasi ham keng qo‘llanilib, har bir foydalanuvchi va tizim komponentini doimiy tekshirish tamoyiliga asoslanadi [5].

Biroq, mavjud yondashuvlar asosan umumiy xarakterga ega bo‘lib, tijorat banklarining o‘ziga xos infratuzilmasi, real vaqt rejimidagi tranzaksiyalar oqimi va yuqori darajadagi xavf muhitini to‘liq hisobga olmaydi [6]. Amaliyot shuni ko‘rsatadiki, ko‘plab banklarda kiberxavfsizlik siyosati statik ko‘rinishda bo‘lib, tez o‘zgaruvchan tahdidlarga moslashish darajasi past [7]. Bundan tashqari, xavfsizlik siyosatlarini ishlab chiqishda risklarni kompleks baholash, tahdidlarni prognozlash va ularni boshqarish mexanizmlari yetarli darajada integratsiyalashmagan [8].

Shu bilan birga, sun’iy intellekt va ma’lumotlar tahliliga asoslangan yondashuvlarning yetarli darajada joriy etilmaganligi ham kiberxavfsizlik tizimlarining samaradorligini pasaytiruvchi omillardan biri hisoblanadi [9]. Zamonaviy kiber tahdidlar dinamik va murakkab xarakterga ega bo‘lganligi sababli, ularni aniqlash va oldini olish uchun moslashuvchan va intellektual boshqaruv strategiyalarini ishlab chiqish zarur.

Yuqoridagi muammolar tijorat banklarida kiberxavfsizlik siyosatini ishlab chiqish va boshqarish strategiyalarini takomillashtirish zaruratini belgilaydi.

Tijorat banklarida kiberxavfsizlik tahdidlari tahlili

Tijorat banklari yuqori darajada axborot texnologiyalariga bog‘liq bo‘lgan murakkab tizimlar hisoblanadi. Bank infratuzilmasining raqamlashtirilishi, moliyaviy operatsiyalarning onlayn muhitga o‘tishi va ma’lumotlar hajmining ortishi kiber tahdidlar spektrining kengayishiga olib kelmoqda [1]. Zamonaviy sharoitda bank tizimlariga tahdidlar nafaqat tashqi manbalardan, balki ichki omillar orqali ham yuzaga kelmoqda [2].

Kiberxavfsizlik tahdidlarini tahlil qilish ularni to‘g‘ri boshqarish va samarali himoya mexanizmlarini ishlab chiqish uchun muhim ahamiyatga ega. Umuman olganda, bank tizimlaridagi tahdidlarni bir nechta asosiy guruhlarga ajratish mumkin.

Birinchi guruh — **tarmoq darajasidagi tahdidlar** bo‘lib, ular orasida DDoS (Distributed Denial of Service) hujumlari alohida o‘rin tutadi. Ushbu hujumlar server va tarmoq resurslarini ortiqcha yuklash orqali xizmat ko‘rsatish jarayonini izdan chiqaradi. Natijada bank xizmatlarining uzluksizligi buziladi va mijozlarga xizmat ko‘rsatishda uzilishlar yuzaga keladi [3]. Bunday hujumlar

ISSN 3030-3907

ko‘pincha moliyaviy tizimlarning zaif nuqtalarini aniqlash va ulardan foydalanish maqsadida amalga oshiriladi.

Ikkinchi guruh — **zararli dasturlar (malware)** bilan bog‘liq tahdidlardir. Ular orqali tizimga ruxsatsiz kirish, ma’lumotlarni o‘g‘irlash yoki tizim faoliyatini izdan chiqarish mumkin. Ayniqsa, bank tizimlarida ransomware va trojan turidagi zararli dasturlar keng tarqalgan bo‘lib, ular moliyaviy ma’lumotlarga bevosita tahdid soladi [4]. Ushbu turdagi hujumlar ko‘pincha foydalanuvchilarni aldash yoki zaifliklardan foydalanish orqali amalga oshiriladi.

Uchinchi guruh — **ijtimoiy muhandislik asosidagi tahdidlar** hisoblanadi. Fishing (phishing), vishing va smishing kabi hujumlar orqali foydalanuvchilarning maxfiy ma’lumotlari qo‘lga kiritiladi [5]. Bank tizimlarida ushbu tahdidlar ayniqsa xavfli bo‘lib, ular texnik himoya tizimlarini chetlab o‘tgan holda bevosita foydalanuvchi orqali amalga oshiriladi.

To‘rtinchi guruh — **ichki tahdidlar (insider threats)** bo‘lib, ular bank xodimlari tomonidan ataylab yoki ehtiyotsizlik natijasida yuzaga keladi. Statistik ma’lumotlarga ko‘ra, ko‘plab kiberinsidentlar inson omili bilan bog‘liq holda sodir bo‘ladi [6]. Bu esa axborot xavfsizligi siyosatini ishlab chiqishda inson omilini hisobga olish zarurligini ko‘rsatadi.

Beshinchi guruh — **zamonaviy texnologiyalar bilan bog‘liq tahdidlar** hisoblanadi. Bulutli texnologiyalar, mobil ilovalar va API asosidagi xizmatlarning keng qo‘llanilishi yangi xavf omillarini yuzaga keltirmoqda. Ushbu muhitlarda ma’lumotlar uzatilishi va saqlanishi jarayonlari murakkablashib, ularni himoyalash masalalari dolzarb ahamiyat kasb etmoqda [7].

Shuningdek, bank tizimlarida **ilg‘or va yashirin (advanced persistent threats — APT)** hujumlar ham kuzatilmoqda. Ushbu hujumlar uzoq muddat davomida tizim ichida yashirin faoliyat yuritib, muhim ma’lumotlarni bosqichma-bosqich yig‘ish va uzatishga qaratilgan bo‘ladi [8]. Bu esa ularni aniqlashni yanada qiyinlashtiradi.

Yuqoridagi tahlillar shuni ko‘rsatadiki, tijorat banklarida kiberxavfsizlik tahdidlari ko‘p darajali va dinamik xarakterga ega bo‘lib, ularni samarali boshqarish uchun kompleks, moslashuvchan va zamonaviy xavfsizlik siyosatini ishlab chiqish zarur. Aynan shu sababli keyingi bosqichda mavjud xavfsizlik siyosatlarini chuqur tahlil qilish va ularning kamchiliklarini aniqlash muhim hisoblanadi.

Mavjud kiberxavfsizlik siyosatlari va ularning kamchiliklari

Tijorat banklarida kiberxavfsizlikni ta’minlash maqsadida turli standartlar va boshqaruv yondashuvlariga asoslangan xavfsizlik siyosatlari qo‘llaniladi. Ushbu siyosatlar bank infratuzilmasini himoya qilish, ma’lumotlar maxfiyligini

ISSN 3030-3907

ta’minlash hamda kiber tahdidlarga qarshi choralarni belgilashga qaratilgan [1]. Amaliyotda keng qo‘llanilayotgan yondashuvlar qatoriga ISO/IEC 27001 asosidagi axborot xavfsizligini boshqarish tizimi, COBIT boshqaruv modeli, ITIL xizmatlarni boshqarish konsepsiyasi hamda NIST Cybersecurity Framework kiradi [2].

Mazkur yondashuvlar asosida ishlab chiqilgan kiberxavfsizlik siyosatlari odatda quyidagi asosiy bosqichlarni o‘z ichiga oladi: aktivlarni aniqlash, tahdid va zaifliklarni baholash, xavfsizlik choralarini belgilash, monitoring va audit jarayonlarini tashkil etish [3]. Ushbu tizimlar banklarda ma’lum darajada himoya darajasini ta’minlasa-da, zamonaviy tahdidlar fonida ularning samaradorligi yetarli emasligi kuzatilmoqda.

Birinchi muhim kamchilik - **siyosatlarning statikligi** hisoblanadi. Ko‘plab banklarda xavfsizlik siyosati muayyan davr uchun ishlab chiqiladi va faqat rejalashtirilgan audit jarayonlarida qayta ko‘rib chiqiladi. Bu esa tez o‘zgaruvchan kiber tahdidlar sharoitida xavfsizlik tizimining moslashuvchanligini pasaytiradi [4].

Ikkinchi muammo - **risklarni baholash jarayonlarining yetarli darajada dinamik emasligi**dir. Ko‘pincha risklar tarixiy ma’lumotlar asosida baholanadi va real vaqt rejimidagi tahdidlar hisobga olinmaydi. Natijada xavfsizlik choralarini tezkor yangilash imkoniyati cheklanadi [5].

Uchinchi kamchilik- **xavfsizlik tizimlarining fragmentatsiyalashganligi**dir. Bank infratuzilmasida turli xavfsizlik vositalari mavjud bo‘lsa-da, ular o‘zaro to‘liq integratsiyalashmagan. Masalan, IDS/IPS tizimlari, SIEM platformalari va tarmoq himoya vositalari alohida ishlashi sababli tahdidlarni kompleks aniqlash va ularni bog‘liq holda tahlil qilish qiyinlashadi [6].

To‘rtinchi muammo - **inson omili bilan bog‘liq zaifliklar**dir. Xodimlarning axborot xavfsizligi bo‘yicha bilim darajasi yetarli bo‘lmagan hollarda yoki xavfsizlik siyosatlariga rioya qilinmaganda kiberinsidentlar yuzaga kelish ehtimoli ortadi [7]. Ijtimoiy muhandislik hujumlari aynan ushbu zaifliklardan foydalanadi.

Bundan tashqari, mavjud xavfsizlik siyosatlarida **proaktiv yondashuv yetishmasligi** ham muhim kamchilik hisoblanadi. Ko‘pgina tizimlar tahdid yuzaga kelgandan keyin javob berishga yo‘naltirilgan bo‘lib, ularni oldindan aniqlash va prognoz qilish imkoniyatlari cheklangan [8].

Yana bir muhim jihat - **zamonaviy texnologiyalar bilan moslashuv muammosi**dir. Bulutli hisoblash, mobil banking va API asosidagi xizmatlarning rivojlanishi mavjud xavfsizlik siyosatlarini qayta ko‘rib chiqishni talab etadi. Ammo ko‘plab banklarda ushbu texnologiyalar uchun alohida xavfsizlik strategiyalari yetarli darajada ishlab chiqilmagan [9].

ISSN 3030-3907

Yuqoridagi kamchiliklar tijorat banklarida kiberxavfsizlik siyosatini takomillashtirish, uni moslashuvchan, integratsiyalashgan va riskga asoslangan yondashuv asosida qayta ishlab chiqish zarurligini ko‘rsatadi. Shu sababli keyingi bosqichda zamonaviy talablar asosida samarali kiberxavfsizlik strategiyalarini ishlab chiqish muhim hisoblanadi.

Tijorat banklarida kiberxavfsizlik siyosatini ishlab chiqish va boshqarish strategiyalari

Tijorat banklarida kiberxavfsizlikni samarali ta’minlash mavjud yondashuvlarni takomillashtirish hamda zamonaviy tahdidlarga moslashuvchan strategiyalarni ishlab chiqishni talab etadi. Ushbu bo‘limda bank tizimlari uchun kiberxavfsizlik siyosatini ishlab chiqish va boshqarishning asosiy strategik yo‘nalishlari taklif etiladi.

Birinchi navbatda, kiberxavfsizlik siyosati **riskga asoslangan yondashuv** asosida shakllantirilishi zarur. Bu yondashuvda bank infratuzilmasidagi barcha aktivlar (ma’lumotlar, tarmoq resurslari, dasturiy tizimlar) aniqlanadi va ular uchun ehtimoliy tahdidlar hamda ularning ta’sir darajasi baholanadi [1]. Natijada xavfsizlik choralarini ustuvorlik asosida joriy etish imkoniyati yaratiladi.

Ikkinchi muhim strategiya - **moslashuvchan (adaptive) kiberxavfsizlik siyosatini joriy etish** hisoblanadi. Ushbu yondashuvda xavfsizlik siyosati doimiy ravishda yangilanib boradi va real vaqt rejimida yuzaga keladigan tahdidlarga moslashadi. Bunda monitoring tizimlari orqali olinadigan ma’lumotlar asosida xavfsizlik siyosati avtomatik ravishda optimallashtiriladi [2].

Uchinchi strategik yo‘nalish - **integratsiyalashgan xavfsizlik boshqaruv tizimini yaratish**dir. Bank tizimlarida mavjud xavfsizlik vositalari (IDS/IPS, SIEM, firewall va boshqalar) yagona platforma doirasida birlashtirilishi zarur. Bu esa turli manbalardan kelayotgan xavfsizlik hodisalarini kompleks tahlil qilish va tezkor qaror qabul qilish imkonini beradi [3].

Shuningdek, kiberxavfsizlikni boshqarishda **sun’iy intellekt va mashinaviy o‘rganish usullaridan foydalanish** muhim ahamiyatga ega. Ushbu usullar yordamida katta hajmdagi tarmoq trafiklarini tahlil qilish, anomal xatti-harakatlarni aniqlash va kiber tahdidlarni oldindan prognoz qilish mumkin [4]. Bu esa an’anaviy xavfsizlik tizimlariga nisbatan yuqori samaradorlikni ta’minlaydi.

Keyingi muhim strategiya - **inson omilini boshqarish** hisoblanadi. Bank xodimlari uchun muntazam ravishda axborot xavfsizligi bo‘yicha treninglar o‘tkazish, xavfsizlik siyosatiga rioya etilishini nazorat qilish hamda ichki audit tizimini kuchaytirish zarur [5]. Bu orqali ijtimoiy muhandislik hujumlari va ichki tahdidlar xavfini kamaytirish mumkin.

ISSN 3030-3907

Bundan tashqari, **ko‘p darajali himoya (defense-in-depth) konsepsiyasini joriy etish** ham muhim hisoblanadi. Ushbu yondashuvda xavfsizlik bir nechta qatlamlarda ta’minlanadi: tarmoq darajasi, tizim darajasi va foydalanuvchi darajasi. Natijada bitta himoya mexanizmi buzilgan taqdirda ham boshqa qatlamlar orqali tizim himoyasi saqlanib qoladi [2].

O‘zbekiston va xorijiy davlatlarda tijorat banklarida kiberxavfsizlik siyosatlari tahlili

Tijorat banklarida kiberxavfsizlik siyosatini shakllantirish jarayoni davlatning raqamli rivojlanish darajasi, normativ-huquqiy bazasi hamda texnologik infratuzilmasiga bevosita bog‘liqdir. Turli mamlakatlarda bank tizimlarida kiberxavfsizlikni ta’minlash uchun qo‘llanilayotgan yondashuvlar o‘zining mazmuni, boshqaruv modeli va texnologik darajasi bilan farqlanadi [10].

O‘zbekiston Respublikasida tijorat banklarida kiberxavfsizlik siyosati asosan milliy normativ hujjatlar va xalqaro standartlar asosida shakllantirilmoqda. Xususan, Markaziy bank tomonidan belgilangan talablar hamda ISO/IEC 27001 standarti asosida axborot xavfsizligini boshqarish tizimlari joriy etilmoqda [11]. Ushbu yondashuv banklarda xavfsizlikni tashkil etishda tizimli asos yaratadi, biroq amaliyotda u ko‘proq audit va nazoratga yo‘naltirilgan bo‘lib, tahdidlarga tezkor moslashish imkoniyati cheklangan [12].

AQSh tijorat banklarida kiberxavfsizlik siyosati yuqori darajada rivojlangan bo‘lib, u NIST Cybersecurity Framework, FFIEC tavsiyalari va Zero Trust konsepsiyasiga asoslanadi [13]. Ushbu tizimda xavfsizlik boshqaruvi proaktiv yondashuv asosida tashkil etilib, real vaqt monitoring, SIEM tizimlari va sun’iy intellekt asosidagi tahdid aniqlash mexanizmlaridan keng foydalaniladi [14].

Yevropa Ittifoqi mamlakatlarida bank tizimlarida kiberxavfsizlik siyosati GDPR va PSD2 direktivalari asosida shakllanadi. Ushbu yondashuvda asosiy e’tibor mijoz ma’lumotlarini himoyalash va xavfsiz tranzaksiyalarni ta’minlashga qaratilgan [15]. Shu bilan birga, Open Banking konsepsiyasi joriy etilishi xavfsizlik siyosatini yanada murakkablashtirib, qo‘shimcha himoya mexanizmlarini talab qiladi [16].

Osiyo davlatlari orasida Singapur tajribasi alohida e’tiborga loyiq bo‘lib, unda Monetary Authority of Singapore tomonidan ishlab chiqilgan Technology Risk Management (TRM) modeli asosida banklarda kiberxavfsizlik siyosati amalga oshiriladi [17]. Ushbu model real vaqt monitoring, kiberrezilyentlik va avtomatlashtirilgan boshqaruv tamoyillariga asoslanadi.

ISSN 3030-3907

1-jadval.

Davlatlar kesimida kiberxavfsizlik siyosatlarining asosiy xususiyatlari

Davlat	Asosiy standart / model	Siyosat yo‘nalishi	Texnologik daraja	Qo‘llaniladigan vositalar
O‘zbekiston	ISO/IEC 27001, MB talablari	Reaktiv, nazoratga yo‘naltirilgan	O‘rta	Firewall, antivirus, audit tizimlari
AQSh	NIST CSF, Zero Trust, FFIEC	Proaktiv, riskga asoslangan	Juda yuqori	SIEM, AI, Big Data, IDS/IPS
Yevropa Ittifoqi	GDPR, PSD2	Maxfiylikka yo‘naltirilgan	Yuqori	IAM, DLP, monitoring tizimlari
Singapur	MAS TRM	Moslashuvchan, real vaqt boshqaruvi	Juda yuqori	AI, real-time monitoring, automation

1-jadvaldan ko‘rinib turibdiki, rivojlangan davlatlarda kiberxavfsizlik siyosati nafaqat normativ talablar asosida, balki zamonaviy texnologiyalar yordamida amalga oshiriladi. Xususan, AQSh va Singapurda real vaqt monitoring va sun’iy intellekt asosidagi tizimlar keng qo‘llanilib, tahdidlarni oldindan aniqlash imkonini beradi. O‘zbekistonda esa asosiy e’tibor standartlarga moslik va nazoratga qaratilgan bo‘lib, texnologik integratsiya darajasi nisbatan past [14], [17].

Davlatlar kesimida olib borilgan chuqur tahlillar asosida kiberxavfsizlik siyosatlarini solishtirish muhim ahamiyatga ega bo‘lib, bu mavjud yondashuvlarning ustun va zaif tomonlarini aniqlash imkonini beradi.

2-jadval.

Kiberxavfsizlik siyosatlarining solishtirma tahlili

Davlat	Yondashuv turi	Ustunliklari	Kamchiliklari
O‘zbekiston	Reaktiv	Tizimli boshqaruv mavjud, standartlarga mos	Moslashuvchanlik past, real vaqt tizimlar kam
AQSh	Proaktiv	Yuqori aniqlik, tezkor javob, AI qo‘llaniladi	Yuqori xarajat, murakkablik

ISSN 3030-3907

Yevropa Ittifoqi	Huquqiy + texnologik	Kuchli ma'lumot himoyasi, standartlashgan tizim	Murakkab tartibga solish
Singapur	Moslashuvchan	Tezkor boshqaruv, yuqori texnologik daraja	Texnologik talab yuqori

2-jadval natijalari shuni ko‘rsatadiki, rivojlangan davlatlarda kiberxavfsizlik siyosati asosan proaktiv va moslashuvchan yondashuvlarga asoslangan. Bunday tizimlarda tahdidlarni oldindan aniqlash va tezkor javob berish imkoniyati yuqori. O‘zbekiston tajribasida esa xavfsizlik siyosati hali to‘liq moslashuvchan emas va ko‘proq an’anaviy himoya choralariga tayanadi. Shu sababli zamonaviy texnologiyalarni joriy etish orqali kiberxavfsizlik siyosatini takomillashtirish zarur hisoblanadi [12], [16].

XULOSA.

Mazkur tadqiqotda tijorat banklarida kiberxavfsizlik siyosatini ishlab chiqish va boshqarish strategiyalari kompleks tarzda tahlil qilindi. Olib borilgan tahlillar shuni ko‘rsatdiki, bank tizimlarida kiberxavfsizlikni ta’minlash zamonaviy raqamli transformatsiya sharoitida dolzarb muammolardan biri hisoblanadi. Bank infratuzilmasining raqamlashtirilishi va xizmatlarning onlayn muhitga o‘tishi kiber tahdidlar ko‘lamining kengayishiga olib kelmoqda.

Tahlil natijalari asosida aniqlanishicha, mavjud kiberxavfsizlik siyosatlari ko‘p hollarda statik va reaktiv xarakterga ega bo‘lib, tez o‘zgaruvchan tahdidlarga moslashishda yetarli darajada samarali emas. Ayniqsa, risklarni baholash va boshqarish jarayonlarida real vaqt monitoring, prognozlash va avtomatlashtirilgan qaror qabul qilish mexanizmlarining yetishmasligi asosiy muammolardan biri sifatida namoyon bo‘lmoqda.

Xorijiy davlatlar tajribasini tahlil qilish shuni ko‘rsatdiki, rivojlangan mamlakatlarda kiberxavfsizlik siyosati asosan proaktiv, moslashuvchan va texnologik yondashuvlarga asoslangan. Xususan, AQSh va Singapur tajribasida sun’iy intellekt, real vaqt monitoring va Zero Trust konsepsiyalariga asoslangan boshqaruv tizimlari yuqori samaradorlikni ta’minlamoqda. Yevropa Ittifoqida esa ma’lumotlar maxfiyligi va huquqiy tartibga solish asosiy o‘rinni egallaydi.

O‘zbekiston bank tizimida kiberxavfsizlik siyosatini takomillashtirish uchun xalqaro tajribani joriy etish, ayniqsa proaktiv va moslashuvchan boshqaruv strategiyalarini ishlab chiqish zarur. Shu bilan birga, sun’iy intellekt va ma’lumotlar tahliliga asoslangan texnologiyalarni joriy etish, xavfsizlik tizimlarini integratsiyalash va inson omilini boshqarish muhim ahamiyat kasb etadi.

ISSN 3030-3907

Tadqiqot natijasida tijorat banklari uchun kiberxavfsizlik siyosatini ishlab chiqishning quyidagi ustuvor yo‘nalishlari asoslandi:

- riskga asoslangan va moslashuvchan xavfsizlik siyosatini joriy etish;
- real vaqt monitoring va tahdidlarni prognozlash tizimlarini rivojlantirish;
- sun’iy intellekt asosidagi xavfsizlik mexanizmlarini qo‘llash;
- kiberrezilyentlikni ta’minlash va tizim barqarorligini oshirish;
- xavfsizlik boshqaruv tizimlarini integratsiyalash.

Ushbu yondashuvlar tijorat banklarida kiberxavfsizlik darajasini oshirish, tahdidlarni samarali boshqarish hamda moliyaviy tizimning barqarorligini ta’minlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. ISO/IEC 27001:2022. *Information Security Management Systems – Requirements*. – Geneva: ISO, 2022.
2. National Institute of Standards and Technology (NIST). *Cybersecurity Framework (CSF 2.0)*. – Gaithersburg, 2024.
3. European Union Agency for Cybersecurity (ENISA). *Threat Landscape for the Financial Sector*. – Athens, 2023.
4. Basel Committee on Banking Supervision. *Principles for Operational Resilience*. – Basel, 2022.
5. Verizon. *Data Breach Investigations Report (DBIR)*. – 2024.
6. Kaspersky Lab. *Financial Cyber Threats Report*. – Moscow, 2023.
7. European Parliament. *General Data Protection Regulation (GDPR)*. – Brussels, 2018.
8. European Commission. *Directive (EU) 2015/2366 (PSD2)*. – Brussels, 2019.
9. Monetary Authority of Singapore (MAS). *Technology Risk Management Guidelines*. – Singapore, 2021.
10. Federal Financial Institutions Examination Council (FFIEC). *Cybersecurity Assessment Tool*. – Washington, 2022.
11. National Cyber Security Centre (NCSC UK). *Cyber Security Guidance for Financial Sector*. – London, 2023.
12. O‘zbekiston Respublikasi Markaziy banki. *Tijorat banklarida axborot xavfsizligini ta’minlash talablari*. – Toshkent, 2023.
13. ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. – 2019.
14. Axelos. *ITIL 4: IT Service Management Framework*. – London, 2019.
15. Gartner. *Top Cybersecurity Trends in Financial Services*. – 2024.
16. Stallings W. *Network Security Essentials: Applications and Standards*. – Pearson, 2021.

ISSN 3030-3907

17. Bishop M. *Computer Security: Art and Science*. – Addison-Wesley, 2020.

ISSN 3030-3907