BANK SEKTORIDA RAQAMLASHTIRISH JARAYONIDA KIBERXAVFSIZLIK XATARLARINI ANIQLASH VA BAHOLASH USULLARI.

Asemova Rano Japbarbergenovna
Uzsanoatqurilishbank ATB Qo'ng'irot BXM
Service manager bosh mutaxasisi

МЕТОДЫ ВЫЯВЛЕНИЯ И ОЦЕНКИ РИСКОВ КИБЕРБЕЗОПАСНОСТИ В ПРОЦЕССЕ ЦИФРОВИЗАЦИИ БАНКОВСКОГО СЕКТОРА.

Асемову Рано Жапбарбергеновну
АКБ "Узсаноаткурилишбанк" Кунградский БХЦ
Главный специалист сервисного менеджера

Methods for identifying and assessing cybersecurity risks in the process of digitalization in the banking sector.

Asemova Rano Zhapparbergenovna
JSCB "Uzpromstroybank" Kungrad BKM
Chief Specialist of Service Manager

Annotatsiya: Ushbu maqolada bank sektorida raqamlashtirishning jadallashuvi natijasida yuzaga kelayotgan kiberxavfsizlik xatarlarini aniqlash, monitoring qilish va samarali baholash usullari tahlil qilinadi. Raqamli to‘lov tizimlarining kengayishi, elektron bank xizmatlaridan foydalanishning ko‘payishi, mijoz ma’lumotlarining katta hajmda qayta ishlanishi kiberhujumlarning xavfini oshirmoqda. Maqolada ushbu xatarlarni erta aniqlash, xavfni mezonlar asosida baholash, ilg‘or texnologiyalar (SIEM, AI, ML) yordamida real vaqt rejimida monitoring qilishning afzalliklari ochib berilgan. Natijada bank tizimida axborot xavfsizligini ta’minlashda kompleks yondashuv, zamonaviy himoya modellari hamda xatarlarni baholash algoritmlarining ahamiyati asoslab berilgan.

Kalit so’zlar: raqamlashtirish, bank sektori, kiberxavfsizlik, xatarlarni baholash, SIEM, sun’iy intellekt, monitoring, moliyaviy xavflar, ma’lumotlarni himoyalash, raqamli bank xizmatlari.

Abstract: This article analyzes methods for detecting, monitoring, and effectively evaluating cybersecurity risks emerging as a result of the accelerated digitization in the banking sector. The expansion of digital payment systems, the increase in the use of electronic banking services, and the large-scale processing of customer data are heightening the risk of cyberattacks. The article reveals the advantages of early detection of these risks, evaluating risks based on criteria, and real-time monitoring using advanced technologies (SIEM, AI, ML). As a result, the importance of a comprehensive approach, modern protection models, and risk assessment algorithms in ensuring information security in the banking system is substantiated.

Keywords: digitization, banking sector, cybersecurity, risk assessment, SIEM, artificial intelligence, monitoring, financial risks, data protection, digital banking services.

Аннотация: В данной статье анализируются методы выявления, мониторинга и эффективной оценки рисков кибербезопасности, возникающих в результате ускорения цифровизации в банковском секторе. Расширение цифровых платежных систем, увеличение использования услуг электронного банкинга, обработка больших объемов данных клиентов повышают риск кибератак. В статье раскрываются преимущества раннего выявления этих рисков, критериальной оценки риска, мониторинга в режиме реального времени с использованием передовых технологий (SIEM, AI, ML). В результате обоснована важность комплексного подхода, современных моделей защиты и алгоритмов оценки рисков в обеспечении информационной безопасности в банковской системе.

Ключевые слова: цифровизация, банковский сектор, кибербезопасность, оценка рисков, SIEM, искусственный интеллект, мониторинг, финансовые риски, защита данных, цифровые банковские услуги.

Kirish: So‘nggi yillarda global moliya tizimida raqamlashtirish jarayonlari keng ko‘lamda rivojlanib, bank sektorida xizmat ko‘rsatishning elektron shakllari ustuvor yo‘nalishga aylanmoqda. Internet-banking, mobil ilovalar orqali hisob-kitoblar, masofaviy kreditlash, raqamli identifikatsiya tizimlari va bulutli texnologiyalar asosida ma’lumotlar almashinuvi bank faoliyatining ajralmas qismiga aylandi. Ushbu jarayon mijozlarga tezkor, qulay va kam xarajatli xizmatlarni taklif etish imkonini bergan bo‘lsa-da, axborot xavfsizligi masalalarini dolzarb qilmoqda.

Raqamli bank tizimlari murakkablashgani sari ularga nisbatan kiberhujumlar soni ham ortib bormoqda. Xususan, fishing, DDoS hujumlari, zararli dasturlar orqali tizimlarni izdan chiqarish, mijoz ma’lumotlarini o‘g‘irlash, firibgarlik bilan tranzaksiyalarni o‘zgartirish kabi xavf omillari tez-tez uchramoqda. Kiberjinoyatchilar texnologiyalarning yangi imkoniyatlaridan foydalangan holda bank infratuzilmalariga kirish yo‘llarini izlaydi, bu esa moliyaviy barqarorlikka, mijozlar ishonchiga hamda milliy iqtisodiy xavfsizlikka jiddiy tahdid tug‘diradi.

Shu nuqtai nazardan, bank sektorida yuzaga kelishi mumkin bo‘lgan kiberxatarlarni aniqlash va ularni baholashning ilmiy-nazariy asoslarini ishlab chiqish, xavfsizlik monitoringi hamda himoya mexanizmlarini takomillashtirish strategik ahamiyat kasb etadi. Mazkur maqolada raqamlashtirilgan bank tizimlarida kiberxavfsizlik tahdidlarini aniqlash va baholash bo‘yicha qo‘llaniladigan metodlar, zamonaviy texnologik yechimlar hamda ularning samaradorligini oshirishga doir takliflar yoritib beriladi.

Asosiy qism: Raqamli iqtisodiyot sharoitida bank sektorining faoliyati tubdan o‘zgarib, elektron to‘lovlar, masofaviy xizmatlar va mobil banking tizimlari mijozlar hayotining odatiy qismiga aylandi. Bugungi kunda milliy va xalqaro moliya bozori raqobati kuchaygani sari banklarning texnologik modernizatsiya darajasi ularning barqarorligi va ishonchliligini belgilovchi asosiy mezonga aylangan. Aynan shu jarayonda kiberxavfsizlik masalasi strategik ahamiyat kasb etadi.

Statistik ma’lumotlarga ko‘ra, so‘nggi yillarda moliyaviy sektor global miqyosda eng ko‘p kiberhujumga uchrayotgan sohaga aylangan. Xavf darajasining oshishi, fishing, DDoS, ransonware, ma’lumotlar bazasiga noqonuniy kirish kabi hujumlarning soni ortib borayotgani bank infratuzilmasini himoyalashni yanada murakkablashtiradi. Birgina tizimdagi kichik zaiflik ham katta miqdorda moliyaviy yo‘qotishlarga, mijozlar ishonchi pasayishiga, kredit-moliya bozori barqarorligining izdan chiqishiga sabab bo‘lishi mumkin.

Shuningdek, raqamli tranzaksiyalarning ko‘payishi, to‘lov tizimlarining integratsiyalashuvi, bulutli hisoblash, API va ochiq bank xizmatlarining kengayishi nafaqat qulaylik yaratmoqda, balki yangi turdagi kiberxatarlar paydo bo‘lishiga ham zamin yaratmoqda. Shu bois bank tizimida xatarlarni oldindan aniqlash, ularni baholash va boshqarishning ilmiy asoslangan metodologiyasini ishlab chiqish va amaliyotga joriy etish bugunning dolzarb vazifalaridan biridir.

Banklar uchun samarali kiberxavfsizlik tizimini yaratish — faqat texnik zarurat emas, balki iqtisodiy bardoshlilik, moliyaviy xizmatlar sifati, milliy to‘lov

infratuzilmasining xavfsizligini ta’minlashning muhim omilidir. Mazkur mavzuning ahamiyati aynan shu omillar bilan belgilanadi.

Bank sektorida kiberxavfsizlik tahdidlarining shakllanish omillari

Raqamli texnologiyalarni keng tatbiq etish banklar faoliyatini tezkor va samarali qilgani bilan birga axborot tahdidlarini ham kuchaytirmoqda. Tahdidlarning asosiy shakllanish omillari quyidagilardan iborat:

- **Axborot tizimlarining murakkablashuvi** — tizimlar kengaygan sari ulardagi zaifliklar soni ham ortadi.
- **Masofaviy xizmatlar ulushi oshishi** — mijozlar internet va mobil bankingdan foydalanar ekan, fishing, MITM (man-in-the-middle) kabi hujumlar uchun imkon kengayadi.
- **Ichki xodimlar omili** — xodimlarning bexabar yoki qasddan sodir etgan xatolari tizimga zarar yetkazishi mumkin.
- **Ma’lumotlar hajmining keskin oshishi** — katta hajmdagi mijoz ma’lumotlarini saqlash va uzatish ularni himoya qilish talabini kuchaytiradi.
- **Integratsiya va API tizimlarining ko‘payishi** — uchinchi tomon xizmatlariga ulanish xavfsizlikni zaiflashtirishi mumkin.

Mazkur omillar bank raqamlashtirish jarayonida tizimli xavf baholashning zarurligini ko‘rsatadi.

2. Kiberxatarlarni aniqlash usullari

Bank tizimida tahdidlarni erta aniqlash real vaqt rejimida ishlovchi texnologiyalar va diagnostika mexanizmlariga tayanadi. Quyida asosiy aniqlash usullari keltiriladi:

2.1. SIEM tizimlari (Security Information and Event Management)

SIEM platformalari turli manbalardan kelgan xavfsizlik signallarini yig‘adi, ularni tahlil qiladi va potentsial hujumlar haqida signal beradi. Bu usul yordamida:

- loglar real vaqt rejimida ko‘rib chiqiladi;
- anomaliyalar avtomatik aniqlanadi;
- hujum ssenariylari bo‘yicha tahdidlar bashorat qilinadi.

2.2. IDS va IPS tarmoqlarini qo‘llash

Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) tarmoqqa kiruvchi harakatlarni kuzatadi va zarur bo‘lsa bloklaydi. Ushbu tizimlar:

- zararli trafikni aniqlaydi;
- kirish urinishlarini to‘xtatadi;
- trafikni statistik tahlil asosida monitoring qiladi.

2.3. Penetratsion testlar (Pentesting)

Bank infratuzilmasida zaifliklarni aniqlash uchun real hujumga o‘xshash model sinovlari o‘tkaziladi. Pentest natijasida:

- zaif serverlar aniqlanadi;
- mavjud parollar mustahkamligi tekshiriladi;
- tizimga kirish yo‘llari simulyatsiya qilinadi.

2.4. Anomaliya aniqlash algoritmlari

Sun’iy intellekt va mashinaviy o‘qitish asosida ishlovchi algoritmlar noodatiy tranzaksiyalar yoki tizim harakatlarini aniqlashi mumkin. Misol sifatida:

- bir mijozning odatiy faoliyatidan keskin farqlanadigan tranzaksiyalar;
- shubhali IP-manzillardan takror kirish urinishlari;
- katta hajmdagi ma’lumotlarni yuklab olish harakatlari.

Ushbu yondashuvlar hujumlarni oldindan bashorat qilish imkonini beradi.

3. Kiberxavfsizlik xatarlarini baholash metodlari

Baholash jarayoni mavjud tahdidlarni miqdoriy va sifat tahlili orqali o‘lchashni o‘z ichiga oladi.

Baholash metodi	**Tavsifi**	**Afzalligi**
Risk Matrix	Xavflarni yuzaga kelish ehtimoli va zarari asosida baholash	Vizual, sodda va tezkor
FAIR modeli (Factor Analysis of Information Risk)	Moliyaviy yo‘qotish qiymatini aniq hisoblaydi	Aniq moliyaviy baho beradi
CVSS reytingi	Zaiflik darajasini 0–10 ball oralig‘ida aniqlaydi	Zaifliklarni ustuvorlashtirish oson
Quantitative Risk Assessment	Statistika va matematik model asosida hisoblaydi	Ehtimollik asosida real prognoz beradi

Baholash natijalari asosida bank xavfsizlik protokollari optimallashtiriladi.

4. Xatarlarni boshqarish va himoya strategiyalari

- Ko‘p bosqichli autentifikatsiya (MFA) joriy etish
- Ma’lumotlarni shifrlash va rezerv nusxalash (backup)
- Xodimlar uchun muntazam kiberhavsizlik treninglari
- Bulutli himoya texnologiyalaridan foydalanish
- Zero-Trust Arxitekturasi asosida xavfsizlik muhitini yaratish

Bu yondashuvlar bank tizimida barqaror, himoyalangan raqamli ekotizim shakllantirishga xizmat qiladi.

Muhokama: Bank sektorida raqamli texnologiyalarni keng joriy etish bilan bog‘liq kiberxavfsizlik xatarlarini boshqarish nafaqat texnik choralarni, balki xavflarni tizimli ravishda aniqlash, baholash va minimallashtirishga qaratilgan kompleks yondashuvni talab qiladi. Yuqorida ko‘rib o‘tilgan tahlillar shuni ko‘rsatadiki, raqamli bank xizmatlarining qulayligi oshgani sayin ularga qaratilgan tajovuzlar ham murakkablashmoqda. Shu sababli, bank infratuzilmasida xavfsizlikni ta’minlash uchun an'anaviy usullar yetarli emas, balki zamonaviy texnologiyalar asosida real vaqt monitoring mexanizmlarini kuchaytirish zarur.

Tadqiqot davomida aniqlangan SIEM tizimlari, IDS/IPS himoya modullari, pentesting va sun’iy intellektga asoslangan anomaliya aniqlash modellari tahdidlarni erta qayd etishda va ularning oqibatlarini kamaytirishda muhim o‘rin tutishi qayd etildi. Ayniqsa mashinaviy o‘qitish algoritmlari tranzaksiyalarni avtomatik tahlil qilish, noodatiy xatti-harakatlarni aniqlash, statistik og‘ishlarni kuzatish orqali xavflarni bashorat qilishda yuqori samaradorlik ko‘rsatmoqda. Bu esa kelgusida kiberxavfsizlikni prognozlash imkoniyatlarini yanada kengaytiradi.

Shuningdek, xavflarni baholashning miqdoriy va sifat asosidagi modellari (Risk Matrix, FAIR, CVSS va boshqalar) bank tizimida ustuvor tahdidlarni aniqlash va ularni kamaytirish strategiyasini shakllantirishda amaliy ahamiyatga ega. Ularning qo‘llanilishi risklarni minimal darajaga tushirish, moliyaviy yo‘qotishlarning oldini olish hamda mijozlar ishonchini mustahkamlashga xizmat qiladi. Ushbu jarayonni muvaffaqiyatli olib borish uchun faqat texnologik emas, balki tashkiliy choralar — xodimlar uchun muntazam treninglar, ma’lumotlar zaxiralash siyosati, ko‘p bosqichli autentifikatsiya, Zero-Trust modeli kabi elementlar ham zarur.

Muhokamalardan kelib chiqadiki, bank sektorida kiberxavfsizlikning samarali boshqaruvi bir necha omilning uyg‘unligini talab etadi: texnik himoya vositalari, xavf tahlili metodologiyasi, inson omili bo‘yicha profilaktika choralari va yuqori darajadagi axborot madaniyati. Faqat shu holda raqamlashtirish jarayonidagi kiberxatarlar ustidan nazorat kuchayadi va moliya tizimining barqarorligi ta’minlanadi.

Xulosa va takliflar: Yuqoridagi tahlillar va muhokamalar shuni ko‘rsatadiki, bank sektorida raqamlashtirish jarayonining jadallashuvi kiberxavfsizlik xatarlarini ham shunga mos ravishda oshirmoqda. Elektron to‘lov tizimlari, mobil banking, bulutli texnologiyalar, ochiq API platformalari imkoniyatlari kengaygani sari tizimga

kirish nuqtalari ko‘payadi va ular orqali hujum ehtimoli ham kuchayadi. Shuning uchun zamonaviy bank tizimi xavfsizlikni faqat himoya vositalari bilan emas, balki xatarlarni aniqlash, baholash va boshqarishning kompleks mexanizmlari bilan ta’minlashi zarur.

O‘tkazilgan tahlillar quyidagi xulosalarni chiqarishga asos bo‘ladi:

- Banklarda kiberxatarlar manbalari ko‘p qirrali bo‘lib, tarmoq infratuzilmasi, inson omili, dasturiy nosozliklar va tashqi tajovuzlar bilan bog‘liq.
- Tahdidlarni erta aniqlash uchun SIEM, IDS/IPS tizimlari, penetratsion testlar va sun’iy intellekt asosidagi anomaliya aniqlash usullari eng samarali vositalardan hisoblanadi.
- Risklarni baholashning sifat va miqdoriy modellari (Risk Matrix, FAIR, CVSS) tahdidlar ustuvorligini belgilash va ularga nisbatan choralar ko‘rishda muhim o‘rin tutadi.
- Kiberxavfsizlikni ta’minlash jarayoni faqat texnik vositalarga emas, balki inson omilini to‘g‘ri boshqarishga ham bog‘liq bo‘lib, xodimlar malakasi bu borada keskin ta’sir qiladi.

Takliflar

Banklarda kiberxavfsizlik darajasini yaxshilash va xatarlarni minimallashtirish uchun quyidagi takliflar ilgari suriladi:

1. **Real vaqt monitoring tizimlarini kengaytirish** SIEM, SOC (Security Operation Center) va AI asosidagi kuzatuv platformalarini joriy etish orqali hujumlarni aniqlash tezligini oshirish.
2. **Xodimlar uchun uzluksiz kiberxavfsizlik treninglarini yo‘lga qo‘yish** Phishing, zararli havolalar va firibgarlik sxemalarini tanish bo‘yicha muntazam o‘qitish inson omili bilan bog‘liq xatarlarni sezilarli kamaytiradi.
3. **Ko‘p bosqichli autentifikatsiya (MFA) tizimini majburiy joriy etish** Bu mijoz profillariga noqonuniy kirish ehtimolini minimal darajaga tushiradi.
4. **Ma’lumotlarni shifrlash, rezerv nusxalarni yaratish va Zero-Trust modeliga o‘tish**: Har bir kirish talabini tekshirish, foydalanuvchi vakolatini doimiy baholash xavfsizlik mexanizmini mustahkamlaydi.
5. **Penetratsion testlarni rejalashtirilgan ravishda o‘tkazish** Tizimdagi zaifliklarni oldindan aniqlash va ularni bartaraf etish moliyaviy yo‘qotishlarning oldini oladi.
6. **Kiberxavfsizlik standartlari asosida ichki normativlarni kuchaytirish**

ISO/IEC 27001, PCI DSS kabi xalqaro standartlar bo‘yicha siyosat yuritish bank tizimining barqarorligini ta’minlaydi.

Umuman olganda, raqamlashtirish jarayonini xavfsiz yuritish banklarning uzoq muddatli rivojlanishi, mijozlar ishonchi va moliyaviy tizimning barqarorligini saqlashning eng muhim kafolatidir. Maqolada taklif etilgan texnik va tashkiliy yechimlar ushbu maqsadga erishishda samarali vosita bo‘lib xizmat qiladi.

Foydalanilgan adabiyotlar

- Karimov A. *Bank tizimida axborot xavfsizligini ta’minlash masalalari*. – Toshkent: Iqtisodiyot nashriyoti, 2021. – 256 b.
- Niyozov B. Raqamli bank xizmatlarida kiberxavfsizlik va tahdidlarni boshqarish. // *Axborot texnologiyalari va tizimlar* jurnali. – 2022. – №4. – B. 33–41.
- To‘raqulov M. *Bank faoliyatida raqamli texnologiyalar: nazariya va amaliyot*. – Toshkent: Innovatsiya ziyo, 2023. – 310 b.
- Abdug‘aniyev S., Xolmirzayev J. Kiberxavf omillari va ularning moliyaviy tizimga ta’siri haqida. // *Moliya va bank ishi* ilmiy jurnali. – 2020. – №2. – B. 45–52.
- Davronov F. *Axborot xavfsizligi asoslari: ta’lim qo‘llanma*. – Toshkent: Fan va texnologiya, 2019. – 198 b.
- Shodmonov Q., Matkarimova S. Bank tizimida raqamlashtirish jarayoni va xavfsizlik muammolari. // *O‘zbekiston iqtisodiy axboroti*. – 2021. – №10. – B. 67–75.
- Valixo‘jayev A. *Kiberjinoyatchilik va uni oldini olish usullari*. – Urganch: Xorazm universiteti nashriyoti, 2022. – 144 b.
- Rasulov E. Raqamli to‘lov tizimlarida xatarlarni minimallashtirish texnologiyalari. // *Innovatsion texnologiyalar review*. – 2023. – №1. – B. 59–66.
- Yo‘ldoshev U. *Banklarda axborot xavfsizligi boshqaruvi: o‘quv qo‘llanma*. – Toshkent: TDIU, 2020. – 224 b.
- Mamatqulov D., Beknazarov O. Sun’iy intellekt asosida kiberxavflarni aniqlash mexanizmlari. // *Axborot havfsizligi va raqamli iqtisodiyot* ilmiy jurnali. – 2023. – №3. – B. 12–21.