KIBERXAVFSIZLIK VA BANK AXBOROT TIZIMLARIDA XAVFLARNI BOSHQARISH (XALQARO BANKLAR MISOLIDA)

Isoqjonova Mohinurbonu Doniyor qizi
JIDU, TAshqi qtisodiy faoliyat yo'nalishi 1-kurs magistranti
+99897155474
iiimohinurbonu@gmail.com
Ishmuradov Bahodir Sunnatovich
JIDU, Xalqaro moliya va investitsiyalar kafedrasi o`qituvchisi
+998909863538
ishmuradov@uwed.uz

Annotatsiya. *Ushbu maqolada bank axborot tizimlari kiberxavfsizligining zamonaviy tamoyillari, XXI asr global moliya institutlariga xos bo'lgan asosiy kiberxavf turlari hamda ularga qarshi qo'llaniladigan boshqaruv strategiyalari tahlil qilinadi. DDoS hujumlari, ING va Lloyds Bankdagi uzilishlar, shuningdek, Bangladesh Banking 2016-yilgi SWIFT hodisasi orqali yoritib beriladi. Shuningdek, JPMorgan Chase tomonidan kiberxavfsizlik sohasiga yiliga 600 million dollargacha investitsiya kiritilishi, zero-trust arxitekturasi va real vaqt rejimidagi AI-fraud detection tizimlarini joriy etish natijasida yuzaga kelgan ijobiy o'zgarishlar ham tahlil qilinadi. Maqolada bank tizimlarida kiberxavflarni boshqarishning to'liq sikli - xavflarni aniqlash, baholash, bartaraf qilish, monitoring bosqichlari xalqaro standartlar (NIST Cybersecurity Framework, ISO/IEC 27001) hamda Basel Qo'mitasi tamoyillari asosida izohlanadi. Tadqiqot natijalari bank tizimlari uchun kiberxavfsizlikning nafaqat texnik, balki tashkiliy va strategik jihatdan ham kompleks yondashuvni talab qilishi, global bank amaliyotlari esa O'zbekiston moliya sektori uchun muhim tajriba manbai bo'lib xizmat qilishini ko'rsatadi.*

Kalit so'zlar: *phishing, social engineering, DDoS, ichki firibgarlik, mijoz ma'lumotlarini himoya qilish, kiberxavfsizlik*

Аннотация: *В данной статье анализируются современные принципы кибербезопасности банковских информационных систем, основные виды киберрисков, присущие глобальным финансовым институтам XXI века, и стратегии управления, используемые для борьбы с ними. Особое внимание уделяется DDoS-атакам, сбоям в работе ING и Lloyds Bank, а также инциденту со SWIFT в 2016 году в банковской сфере Бангладеш. Также анализируются позитивные изменения, произошедшие в результате инвестирования JPMorgan Chase до 600 миллионов долларов в год в кибербезопасность, внедрения архитектуры нулевого доверия и систем*

обнаружения мошенничества на основе искусственного интеллекта в режиме реального времени. В статье объясняется полный цикл управления киберрисками в банковских системах – этапы выявления, оценки, минимизации и мониторинга рисков – на основе международных стандартов (NIST Cybersecurity Framework, ISO/IEC 27001) и принципов Базельского комитета. Результаты исследования показывают, что кибербезопасность банковских систем требует комплексного подхода не только в техническом, но и в организационном и стратегическом плане, а мировая банковская практика служит важным источником опыта для финансового сектора Узбекистана.

Abstract. *This article analyzes the modern principles of cybersecurity of banking information systems, the main types of cyber risks inherent in global financial institutions of the 21st century, and the management strategies used to combat them. DDoS attacks, outages at ING and Lloyds Bank, as well as the 2016 SWIFT incident in Bangladesh Banking are highlighted. It also analyzes the positive changes that have occurred as a result of JPMorgan Chase investing up to $600 million per year in cybersecurity, the introduction of zero-trust architecture and real-time AI-fraud detection systems. The article explains the full cycle of cyber risk management in banking systems - the stages of risk identification, assessment, mitigation, monitoring - based on international standards (NIST Cybersecurity Framework, ISO / IEC 27001) and the principles of the Basel Committee. The results of the study show that cybersecurity for banking systems requires a comprehensive approach not only technically, but also organizationally and strategically, and global banking practices serve as an important source of experience for the financial sector of Uzbekistan.*

KIRISH

XXI asrning rivojlanib borayotgan raqamli muhiti har bir foydalanuvchiga nafaqat bir qancha qulaylikar berdi, balki uning shaxsiy ma'lumotlariga qaratilgan moliyaviy xavflarni ham paydo qildi. Shu bilan birgalikda banklar bosqichma-bosqich raqamlashib bormoqda. Bu raqamlashuv jarayoni onlayn bank xizmatlari va o'tkazmalari, mobil banking, infratuzilmaning bulutli tizimga asoslanganligi, sun'iy intellekt yordamida yaratilgan va ishlayotgan moliyaviy mahsulotlar misolida namoyon bo'ladi.

Kiberxavfsizlik va risklarni samarali baholash banklar faoliyatidagi barqarorlik hamda foydalanuvchilardagi ishonchni ta'minlaydi. Masalaning dolzarbligi shundaki, banklar o'z mijozlaring ma'lumotlari, jumladan, identifikatsion raqamlar, kredit tarixi, mijozning moliyaviy holati bo'yicha

barcha ma’lumotlarni yig’adi, saqlaydi va uzatadi – ushbu ma’lumotlar xavfsizligi ta’minlanmagan

holatda bank, birinchidan, katta moliyaviy yo’qotishlar va inqirozga uchraydi, bank faoliyatidagi barqarorlikka putur yetadi. Ikkinchidan, kibertahdidlar va zarali viruslar (troyanlar) hujumi natijasida raqamli infratuzilmaning zaifligi sababli, mijoz ma’lumotlariga buzib kirilish holatlari, bank operatsiyalaridagi uzilishlar bo’lish ehtimoli yuqori[9]. Xususan, O’rta Osiyo hududida keng tarqalgan SpyMax va Godfather kabi bank troyanlari foydalanuvchi shaxsiy ma’lumotlariga buzib kirishda ishlatilayotgan viruslarga misol bo’ladi.

Real banking muhitidan kelib chiqib aytish mumkinki, jahon banklari bugungi kuda duch kelayotgan ken tarqalgan kiberxavf turlari phishing va ‘social engineering’ hujumlari, shuningdek, DDoS hujumlari va ichki firibgarlik (insider threat)dan iborat. Bular orasida birinchi sanalgan ikki kiberhujum to’g’ridan-to’g’ri mijozning ishtirokida amalga oshirilsa, DDoS hujumi bank tizimini xavf ostiga qo’yadi, ‘insider’ xavflar banking troyanlari va ma’lumotlar o’g’irlanish holatlarini qamrab oladi. Yuqorida sanab o’tilgan barcha holatlar bank mijozlari moliyaviy maxfiyligiga zarar yetkazadi. Shu sababli jahon moliyaviy institutlari kiberxavfsizlik strategiyalarini ishlab chiqishda, shuningdek, hodisalarga javob berish va operatsion tiklanish rejalarini yaratishda katta e'tibor qaratmoqda.[10]

ADABIYOTLAR TAHLILI

Ushbu tadqiqotda foydalanilgan adabiyotlar bank kiberxavfsizligi, raqamli banking xavflari va xalqaro standartlar bo'yicha keng qamrovli ilmiy hamda amaliy manbalardan iborat. Kiwia va hammualliflarning (2017) tadqiqoti banklarga qarshi qo'llaniladigan zararli dasturlar va ularning ishlash mexanizmini chuqur tahlil qilib, phishing va malware hujumlarining ilmiy asosini mustahkamlaydi. Waliullah va hammualliflari (2025) tomonidan olib borilgan tizimli adabiyot sharhi esa kiberxavfsizlik tahdidlarining raqamli bank xizmatlari rivojiga ta'sirini yoritib, mijoz ishonchi va xavfsizlik o'rtasidagi bog'liqlikni tushuntiradi. Maqolaning metodologik asosini NIST Cybersecurity Framework va Basel Qo'mitasining “Operational Resilience Principles” hujjatlari tashkil etadi. Ushbu standartlar kiberxavflarni aniqlash, baholash va boshqarish jarayonlarini aniq ko'rsatib berish bilan birgalikda banklar uchun xalqaro talablarga mos yondashuvni ham belgilab beradi. Moliya sanoatidagi

[9] Dennis Kiwia , Ali Dehghantanha , Kim-Kwang Raymond Choo , Jim Slaughter ; 2017, Journal of Computational Science - A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence, https://doi.org/10.1016/j.jocs.2017.10.020

kiber tahdidlar bo'yicha Pat Antonacci (2018)ning ishlari global miqyosda uchraydigan asosiy hujum turlari, ularning oqibatlari va sohadagi tendensiyalarni amaliy misollar bilan tushuntiradi. JPMorgan Chase'ning rasmiy hisobotlari va SecurityWeek kabi sanoat manbalari esa banking yillik 600 million dollarlik kiberxavfsizlik investitsiyalari, AI asosidagi fraud detection tizimlari va zero-trust arxitekturasining joriy etilishi haqidagi ishonchli ma'lumotlarni taqdim etadi. Umumlashtirib aytganda, tanlangan adabiyotlar bank tizimlaridagi kiberxavflarni o'rganish, xalqaro tajribani tahlil qilish va samarali boshqaruv yondashuvlarini shakllantirish uchun mustahkam ilmiy-amaliy baza vazifasini o'taydi.

ASOSIY QISM

Bank sohasidagi kiberxavfsizlik - bu moliyaviy institutlar o'z tizimlari, ma'lumotlari vamijozlarini kiberhujumlardan himoya qilish uchun foydalanadigan amaliyotlar,texnologiyalar va strategiyalardir. Uning asosiy uch tamoyili maxfiylik, yaxlitlik va mavjudlik(CIA triad – confidentiality, integrity, availability) dan iborat. Maxfiylik ma’lumotlarning ruxsatsiz shaxslarga oshkor etilmasligini ta’minlasa, yaxlitlik ma’lumotlarning noto‘g‘ri o‘zgartirilmasligi va yo‘qolmasligini kafolatlaydi. Mavjudlik esa tizim va xizmatlarning foydalanuvchilarga doimiy ravishda ochiq bo‘lishini nazorat qiladi. Ushbu tamoyillar bankning barqarorligi va mijoz ishonchi uchun asosiy shart hisoblanadi.

Kiberxavfsizlikning markaziy elementi bank axborot tizimlari hisoblanadi hamda bankning barcha mijoz hisoblarini markazlashtirilgan holda boshqarish Core Banking System (CBS) tizimi yordamida bajariladi. Bugungi kunda onlayn banking va mobil ilovalar mijozlarga qulaylik yaratadi, ammo ular phishing, malware va DDoS hujumlariga duch kelishiga ham sabab bo'ladi. Shu bilan birga, SWIFT tizimi xalqaro pul o‘tkazmalarini xavfsiz amalga oshirish uchun yuqori darajadagi shifrlash va autentifikatsiya talab qiladi.

Xorij tajribasidan kelib chiqib aytadigan bo'lsak, banklar kiberxavfsizlikni xalqaro standartlar va regulyator qo‘llanmalari asosida tashkil qiladi. Axborot xavfsizligini boshqarish tizimlari ISO/IEC 27001 yordamida belgilanadi, NIST Cybersecurity framework[11] xavflarni aniqlash, himoya qilish, aniqlash, javob berish va tiklash bosqichlarini ko‘rsatadi. Shuningdek, Basel Qo’mitasi banklarga global moliya tizimidagi xavflarni kamaytirish va operatsion barqarorlikni ta’minlashda tavsiyalar va yo‘l-yo‘riqlar beradi.[12]

ASOSIY TAHDIDLAR

[10] Md. Waliullah; Md Zahin Hossain George; Md Tarek Hasan; Md Khorshed Alam; Mosa Sumaiya Khatun Munira;Noor Alam Siddiqui; 2025, American Journal of Advanced Technology and Engineering Solutions - Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review, https://doi.org/10.63125/fh49gz18
[11] Cybersecurity Framework I NIST - https://www.nist.gov/cyberframework
[12] Basel Committee “Principles for Operational Resilience” - https://www.bis.org/bcbs/publ/d516.htm

Phishing va social engineering — bank mijozlarini aldash orqali ularning shaxsiy ma'lumotlarini, mazfiylik parollarini yoki bank kartasi ma'lumotlarini qo'lga kiritishga qaratilgan eng keng tarqalgan kiberxavf turlari sanaladi. Bu hujumlar har qanday bank mijoziga nisbatan amalda qo'llanishi mumkin va ular ko'pincha e-mail, SMS yoki soxta login sahifalari orqali sodir etiladi. Hattoki yirik xalqaro banklar faoliyatida ham phishing hujum holatlari qayd etilgan, masalan, xalqaro HSBC banki aldov yo'li orqali mijoz login va parollarini olishga qaratilgan urinishlarni aniqlagan. Joriy holatdan mijozlarni ogohlantirish maqsadida bank rasmiy saytida va SMS xabarnomalar orqali ogohlantirishlar e'lon qilgan, shubhali havolalarga kirmaslik bo'yicha o'z foydalanuvchilariga eslatmalar yuborgan. Texnik himoya choralarini kuchaytirgan (2FA, OTP) va kiberhujumga bog'liq IP manzillarni qo'ra ro'yxatga kiritgan hamda domen registratoridan phishing domenlarini bloklashda yordam olgan.

Bunday hujumlardan himoyalanish uchun banklar turli xavfsizlik choralarini joriy qiladilar:

- ikki bosqichli autentifikatsiya (2FA). Foydalanuvchi login qilayotganda faqat parol emas, qo'shimcha tasdiqlash kodi ham talab qilinadi, bu identifikatsion tasdiqlash yoki mijozning shaxsiy ikkilamchi paroli bo'lishi mumkin;
- anti-phishing gateways. Bank texnik himoya xodimlari elektron pochta va veb-trafikni tahlil qilib, shubhali xabarlarni bloklaydi;
- mijozlarni o'qitish va ogohlantirish. Banklar o'z mijozlarini phishing va aldov usullarini tushuntiruvchi ma'lumotlar, video va treninglar bilan xabardor qiladi.

DDoS (Distributed Denial of Service) hujumlari deb banklarning onlayn xizmatlarini vaqtincha ishdan chiqarish yoki kuchli sekinlashtirishga qaratilgan kiberharakatlarga aytiladi. Ularning ishlash tamoyili minglab zararli qurilmalar bir vaqtning o'zida bank serveriga so'rov yuborish, natijada server ortiqcha yuklama ostida qoldirgan holatda real mijozlarni tizimga kirishdan cheklashdan iborat. Bank xizmatlarining to'xtashi mijoz ishonchi, obro' va operatsion barqarorlikka eng katta zarba beradigan xavflardan biri sanaladi. So'nggi yillarda sodir bo'lgan real vaziyatlardan misol keltirsak, global bank tizimi bir nechta yirik DDoS hujumlariga guvoh bo'lgan. Masalan 2012–2016 yillarda AQShdagi yirik banklarga (Bank of America, JPMorgan, Wells Fargo va boshqalar) uyushtirilgan "Izz ad-Din al-Qassam Cyber Fighters" guruhi hujumlari eng mashhurlaridan biri bo'lib, u paytda ko'plab banklarning onlayn banking tizimlari bir necha soatlab ishlamay qolgan. Shu kabi holat Yevropa ING Bankida 2018-yilda kuzatilgan va bank hujum davomida ketma-

ket DDoS hujumlaridan zarar ko‘rgan. Lloyds Bank esa 2017-yilda ikki kun davom etgan kuchli trafik oqimi tufayli xizmatlarda uzilish qayd etgan. Yuqoridagi kabi holatlarda banklar bunday hujumlardan himoyalanish uchun bir nechta zamonaviy texnologiyalarni qo‘llaydi. WAF (Web Application Firewall) zararli trafikni ilova darajasida aniqlaydi va bloklaydi. "Traffic filtering" orqali serverga faqat qonuniy so‘rovlar kirishiga ruxsat beriladi. CDN (Content Delivery Network) esa trafikni global serverlar bo‘ylab tarqatib, yuklamani kamaytiradi va xizmatlarning uzluksiz ishlashini ta’minlaydi. Real-time monitoring ushbu jarayondagi eng muhimi hisoblanadi, ya’ni trafik oqimini doimiy kuzatib borish kerak, bunda banklar shubhali faollikni soniyalar ichida aniqlab, tezkor choralar ko‘ra oladi. DDoS hujumlari tobora murakkablashib borayotgan bir paytda, banklar nafaqat texnik himoya, balki tezkor javob berish jamoalari va uzluksiz monitoring tizimlari orqali o‘z mustahkamligini oshirmoqda.

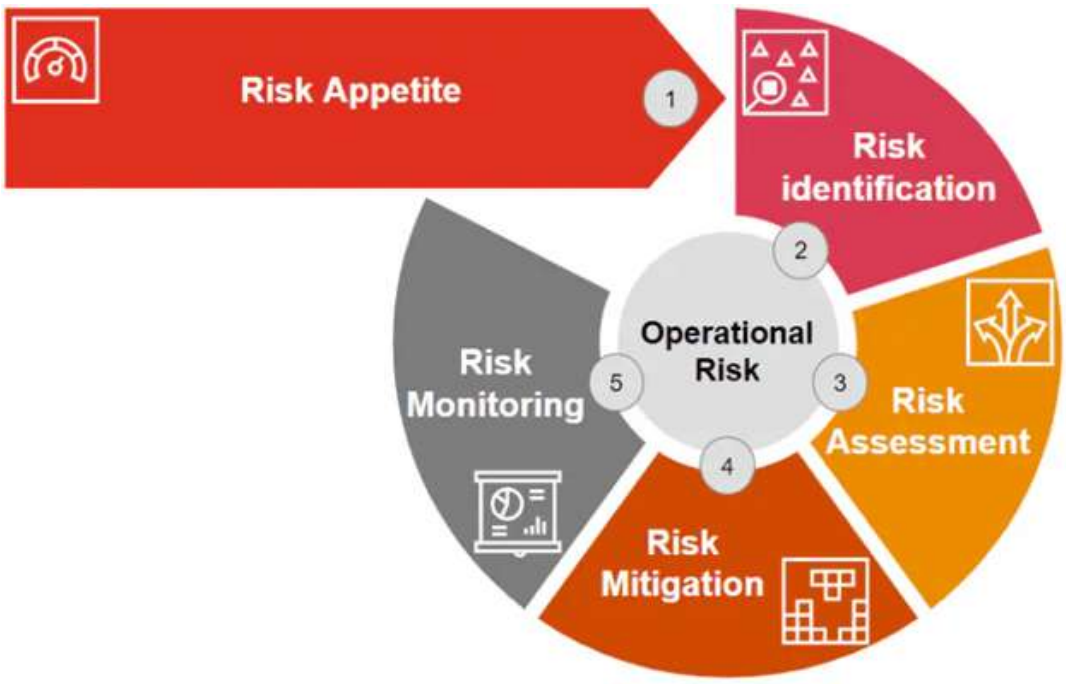
Banklar faoliyatiga tahdid soluvchi xavflar nafaqat tashqi, balki ichki omillar natijasi bo'ladi. Shu sababli bank ximoya tizimi tashqi kiberhujumlarga bardoshli bo'lish bilan bir qatorda, ichki xavflardan - xodimlarning noto'g'ri xatti-harakatlari yoki ularning bank mijozlari hisob raqamlari orqali firibgarlik qilish ehtimolidan ham xavfsiz bo'lishi kerak. Bunday tahdidlar “insider threat” deb yuritiladi va ular ko'pincha bank mijozlarining ma'lumotlar bazasiga ruhsati bor xodimlar tomonidan ma'lumotlardan noto'g'ri foydalanish, hujjatlarni soxtalashtirish yoki maxfiy ma'lumotlarni uchinchi shaxslarga sotish ko'rinishida amalga oshiriladi. Ichki xavflarni aniqlash tashqi hujumlarga qaraganda ancha murakkab, chunki xodim tizimga qonuniy kirish huquqiga ega va uning harakati odatiy operatsiyalar bilan aralashib ketadi. Bank tarixidagi eng mashhur ichki xavf bilan bog'liq hodisalarga 2016-yil Bangladesh Bankida SWIFT tizimiga qilingan hujumi yaqqol misol bo'ladi. Bank xodimlari tomonidan rasmiy xavfsizlik protokollariga rioya qilinmagani, tizimning yetarli darajada kuzatilmagani va SWIFT terminalidagi zaifliklar hujumning muvaffaqiyatli amalga oshirilishida asosiy omil sifatida ko'rsatilgan. Hujumda bank hisobidan $1 mlrd o’g’irlashga urinishgan, natijada kiberjinoyatchilar reja qilingan summaning ma’lum miqdorini noqonuniy o'tkazishga muvaffaq bo'lgan.[13]

Ushbu voqea global banklar uchun ichki xavflarni jiddiy nazorat qilishning qanday dolzarbligini yana bir bor namoyon qildi. Bugungi kunda ichki firibgarlikni kamaytirish va xodimlarning xavfli faoliyatini erta aniqlash uchun zamonaviy banklar AI/ML asosidagi fraud detection tizimlaridan foydalanmoqda. Mazkur tizimlar real vaqt rejimida tranzaksiyalarni kuzatadi,

[13] The cyberthreat facing the financial services industry, Pat Antonacci, Cyber Security: A Peer-Reviewed Journal, 2 (2), 106-113 (2018) - https://doi.org/10.69554/TXMH8697

noodatiy xatti-harakatlarni aniqlaydi va firibgarlik ehtimoli bo'lgan holatlar haqida avtomatik ravishda signal beradi. Sun'iy intellekt modellari xodimlarning tizimga kirish vaqtini, ularning bajaradigan amaliyotlar sonini va odatdagidan farq qiladigan harakatlarni tahlil qilib, xavfni oldindan bashorat qilish imkonini beradi. Bu nafaqat ichki firibgarlikni kamaytiradi, balki bankning umumiy xavfsizlik madaniyatini mustahkamlaydi. Umuman olganda, bank ichidagi firibgarlik va xodimlar tomonidan amalga oshiriladigan risklarini boshqarish nafaqat texnik vositalar, balki axloqiy standartlar, ichki nazorat siyosatlari va doimiy monitoringni talab qiladigan kompleks jarayon hisoblanadi.

Kiberxavflarni boshqarish (cyber risk management) banklar uchun strategik va doimiy jarayon bo'lib, u xavflarni aniqlashdan tortib, hodisalarga javob berish va tiklanishgacha bo'lgan sikldan iborat. 1-rasmda ushbu boshqaruv tizimining besh bosqichi keltirib o'tilgan:



1-rasm. Kiberxavflarni boshqarish siklining besh bosqichi

Yuqoridagi rasmda tasvirlangan xavflarni aniqlash(identification) bosqichida bank aktivlari (masalan, ma'lumotlar bazalari, tarmoq infratuzilmasi, uchinchi tomon xizmatlari), potentsial tahdid manbalari va ehtimoliy zaifliklar aniqlanadi. FDIC kiberxavfsizlik ramkasida, "Identify" funksiyasi alohida e'tibor qaratilgan bo'lib, u korporativ boshqaruv, tahdid monitoringi va resurs egaligi (asset ownership)ni o'z ichiga oladi. Keyingi bosqichda aniqlangan xavflar baholanadi – ehtimollik darajasi, ta'sir kuchi va xavf og'irligi o'lchanadi. Basel Committee "Principles for Operational Resilience" hujjatida banklar bank faoliyatining asosiy operatsion

bo'g'inlari(critical operations) uchun zaifliklarni doimiy baholashi va o'zaro bog'langan risklar (interdependent)ni xaritalashi kerakligi aytilgan. 4-bosqichda baholangan xavflar bo'yicha banklar xavfni kamaytirish strategiyasini ishlab chiqadi hamda bu jarayon mitigatsiyalash deyiladi. Bu strategiya turli choralarni o'z ichiga olishi mumkin, jumladan, xavfsizlik nazoratlarini mustahkamlash, ichki siyosatlarni takomillashtirish, tashqi xavf manbalarini kamaytirish va texnologik yechimlar joriy etish bunga misol bo'la oladi. Basel Qo'mitasi operation chidamlilik tamoyillarida banklar ICT va kiberxavfsizlik nazoratlari (masalan, kirish nazorati, identifikatsiya, autentifikatsiya)ni doimiy ravishda baholashni talab qiladi. Mitigatsiya bosqichidan so'ng, banklar xavflarning yangi shakllarini kuzatib borishi va nazoratni muntazam yangilashi kerak. Bu “real-time monitoring” va nazorat mexanizmlari orqali amalga oshiriladi. Shuningdek, Basel Qo’mitasining operatsion risk hujjatida banklar monitoring natijalarini vaqti-vaqti bilan qayta ko'rib chiqishi va nazorat mexanizmlarini takomillashtirishi doimiy jarayon bo'lishi kerakligi ta'kidlagan.

Risk boshqaruvi bo’yicha jahon tajribasini JPMorgan Chase misolida ko’rib chiqamiz, ushbu tashkilot yirik texnologik va xavfsizlik sarmoyalari bilan tanilgan moliya giganti hisoblanadi. Bir necha yil avval bank rahbariyati kiberxavflarga qarshi kurashni kuchaytirish maqsadida katta hajmdagi investitsiyalar kiritilishini e'lon qilgan. Ommaviy manbalarda qayd etilishicha, bank har yili kiberxavfsizlik yo'nalishiga taxminan 600 million dollar atrofida mablag' ajratadi.[14] Ushbu mablag' 24/7 rejimida ishlaydigan xavfsizlik operatsiyalari markazi (SOC), hodisalarga tezkor javob berish, zaifliklarni aniqlash va bartaraf etish, ijtimoiy muhandislikka qarshi choralar ko'rish hamda uchinchi tomon servislarini nazorat qilish kabi jarayonlarni qo'llab-quvvatlashga sarflanadi.

JPMorgan tomonidan amalga oshirilayotgan texnologik yangilanishlar ichida ikki asosiy strategik yo'nalish yaqqol ko'zga tashlanadi: 'zero-trust arxitekturasi'ni joriy etish va AI asosidagi real vaqt rejimidagi firibgarlikni aniqlash tizimlarini kengaytirish. Bankning o'z nashrlari hamda soha bo'yicha chop etilgan maqolalarda ta'kidlanishicha, SI (sun'iy intellekt)ga asoslangan tekshiruv mexanizmlari va hisob ma'lumotlarini avtomatik tasdiqlash (account/payment validation) xizmatlari ishga tushirilganidan so'ng, rad etilgan transzaksiyalar ulushi 15–20 foizga kamaygan. Bu esa mijozlar uchun keraksiz rad javoblarining kamayishi va operatsiyalar o'tkazilishining yaxshilanishini anglatadi. Zero-trust arxitekturasi esa ko'proq tizim sifati va xavfsizlik dizayniga taalluqli o'zgarish bo'lib, banking ichki tarmoqlariga avtomatik

[14] https://am.jpmorgan.com/ie/en/asset-management/institutional/about-us/trusted-asset-manager/oversight/

ishonchni kamaytiradi, har bir sessiya va so'rovni alohida tekshiradi hamda “eng kam imtiyoz” (least-privilege) tamoyilini qo'llaydi. JPMorgan va boshqa yetakchi moliyaviy institutlar ushbu yondashuv orqali ichki tizim zaifliklarini, xodimlar faoliyati bilan bog'liq xavflarni va uchinchi tomon integratsiyalaridan kelib chiqadigan tahdidlarni sezilarli darajada kamaytirish mumkinligini ta'kidlamoqda. Shunga qaramay, bank xavfsizlik siyosatining maxfiyligi bilan bog'liq holatda zero-trust natijalarining aniq raqamlarda e'lon qilinishi kam uchraydi. Umuman olganda, JPMorgan tomonidan amalga oshirilgan yirik va maqsadli investitsiyalar - yillik kiberxavfsizlik byudjeti, SI asosidagi fraud detection tizimlari va zero-trust arxitekturasi - bank faoliyati barqarorligi va mijozlar tajribasini sezilarli darajada yaxshilagan. Buni rad etilgan tranzaksiyalar kamayishi, hodisalarni tezroq aniqlash va firibgarlik bo'yicha noto'g'ri ogohlantirishlar (false positives) qisqarishi kabi bir qator statistik ko'rsatkichlar ham tasdiqlaydi.

Quyidagi jadvalda JPMorgan Chase tomonidan amalga oshirilgan kiberxavfsizlik islohotlari natijasida erishilgan ijobiy natijalar keltirib o’tilgan. Kompaniya rasmiy yillik hisobotlari[15] va turli rasmiy nashrlardagi hisobotlar[16]dan jamlangan ma’lumotlar jadvalda islohotlar kiberxavfsizlikka ajratilgan yilli budjet miqdori, kiberhimoya xodimlari soni kabi turli ko’rsatkichlarda keltirib o’tilgan va islohotlardan avvalgi va keyingi ochiq manbalardagi raqamli ko’rsatkichlar o’zaro taqqoslangan:

[15] https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/JPMC-2012-AR.pdf
[16] https://www.securityweek.com/600-million-cybersecurity-budget-jpmorgan-chief-endorses-ai-and-cloud/

Ko'rsatkich	Avval	Keyin
Kiberxavfsizlik yillik budjeti	$200 mln (2012-yil)	$600 mln
Kiberxavfsizlik xodimlari o'rtacha soni	600 nafar (2012-yil)	3000 nafar
Account validation rad etish darajasi	-	15-20%ga kamaygan

JPMorgan kabi yirik moliya tashkilotlari o'zlarining xavfsizlik strategiyasining ko'p detallari va investitsiya natijalarini ommaga to'liq oshkor qilmaganligi sababli yuqoridagi jadvalni yanada chuqurroq solishtirish imkoniyati cheklangan. Ammo islohotlar yuzasidan umumiy holat ijobiy o'zgargan. Firibgarlik bo'yicha noto'g'ri signallar keskin qisqargan, kiber hodisalarni aniqlash va ularga javob berish jarayoni sezilarli darajada tezlashgan , ichki tizimlar va uchinchi tomon integratsiyalari bilan bog'liq xavflar zero-trust yondashuvi sabab ancha pasaytirilgan.

XULOSA

Tadqiqot natijalari shuni ko'rsatadiki, zamonaviy bank tizimlari va moliyaviy institutlar kiberxavfsizlik sohasida turli tahdidlarga duch kelmoqda. Phishing, social engineering va banking trojanlari kabi hujumlar mijozlarning shaxsiy ma'lumotlari va moliyaviy mablag'larini xavf ostiga qo'yadi. Ushbu tahdidlar nafaqat texnologik zaifliklardan, balki inson omilidan ham kelib chiqadi. Shu bois, kiberxavfsizlikni ta'minlashda texnologik yechimlar bilan bir qatorda xodimlar va mijozlarning bilim va ongini oshirish muhim ahamiyatga ega. Adabiyotlar tahlili shuni ko'rsatadiki, xalqaro tajribada banking trojanlarini aniqlash va oldini olish uchun kiber kill chain, evolyutsion kompyutatsion yondashuvlar va xavf monitoring tizimlari qo'llaniladi. Shu bilan birga, fintech va bank sektorida ma'lumotlarni himoya qilish, ikki faktorli autentifikatsiya va xavfsiz parol siyosati kabi standartlar muvaffaqiyatli amaliyot sifatida tasdiqlangan. Bu tajribalarni O'zbekiston sharoitida ham moslashtirish zarur. O'zbekiston muhitida banklar va moliya tashkilotlarida phishing va social engineering hujumlarini real vaqt rejimida aniqlashga qaratilgan monitoring va signal tizimlarini joriy etish samarali ish berishi mumkin. Xodimlar va mijozlar uchun ikki faktorli autentifikatsiya va xavfsiz parol siyosatini majburiy qilish orqali shaxsiy ma'lumotlarni himoyalashni kuchaytirish, milliy kiberxavfsizlik platformasi va normativ-huquqiy bazani takomillashtirish orqali fintech va bank sektorida xavfsizlikni milliy darajada mustahkamlashga erishish mumkin. Xulosa qilib aytganda, O'zbekiston bank tizimi va fintech sohasida kiberxavfsizlikni oshirish nafaqat texnologik chora-tadbirlar, balki inson omili va normativ-huquqiy bazani birlashtirish orqali

amalga oshirilishi mumkin. Bu esa moliyaviy institutlarning barqarorligini ta'minlash, mijozlar ishonchini oshirish va mamlakat moliyaviy xavfsizligini mustahkamlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Dennis Kiwia , Ali Dehghantanha , Kim-Kwang Raymond Choo , Jim Slaughter ; 2017, Journal of Computational Science - A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence, https://doi.org/10.1016/j.jocs.2017.10.020

2. Md. Waliullah; Md Zahin Hossain George; Md Tarek Hasan; Md Khorshed Alam; Mosa Sumaiya Khatun Munira;Noor Alam Siddiqui; 2025, American Journal of Advanced Technology and Engineering Solutions - Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review, https://doi.org/10.63125/fh49gz18

3. Cybersecurity Framework I NIST - https://www.nist.gov/cyberframework

4. Basel Committee "Principles for Operational Resilience" - https://www.bis.org/bcbs/publ/d516.htm

5. The cyberthreat facing the financial services industry, Pat Antonacci, Cyber Security: A Peer-Reviewed Journal, 2 (2), 106-113 (2018) - https://doi.org/10.69554/TXMH8697

6. https://am.jpmorgan.com/ie/en/asset-management/institutional/about-us/trusted-asset-manager/oversight/

7. https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/JPMC-2012-AR.pdf

8. https://www.securityweek.com/600-million-cybersecurity-budget-jpmorgan-chief-endorses-ai-and-cloud/