TIJORAT BANKLARIDA KIBERXAVFSIZLIK SIYOSATINI TUTGAN O‘RNI

Avezov Mirzabek Komiljonovich
Abu Rayhon Beruniy nomidagi Urganch davlat universiteti Biznes va boshqaruv kafedrasi dotsenti v.b., PhD
https://doi.org/10.5281/zenodo.20748702

Annotatsiya. *Mazkur maqolada tijorat banklarida kiberxavfsizlik siyosatining zarurirati, mavjud imkoniyatlari va tutgan o‘rni yoritilgan. Shuningdek, tijorat banklarida kiberxavfsizlik siyosatini tutgan o‘rnini oshirish yuzasidan xulosalar bayon etilgan.*

Аннотация. *В данной статье рассматриваются необходимость, текущие возможности и роль политики кибербезопасности в коммерческих банках. Также представлены выводы о том, как улучшить роль политики кибербезопасности в коммерческих банках.*

Abstract. *This article discusses the need, current opportunities and role of cybersecurity policy in commercial banks. It also presents conclusions on improving the role of cybersecurity policy in commercial banks.*

Kalit so‘zlar. *Bank, tijorat banki, siyosat, kiberxavfsizlik siyosati, mijoz.*

Ключевые слова. *Банк, коммерческий банк, политика, политика кибербезопасности, клиент.*

Key words. *Bank, commercial bank, policy, cybersecurity policy, client.*

Zamonaviy dunyoda tijorat banklari sektorida eng muhim raqobat omili innovatsiyalarni joriy etish va axborot texnologiyalarini rivojlantirish bo‘lib hisoblanadi. Biroq, ushbu jarayon firibgarlik yangi turlarining paydo bo‘lishi bilan ham birga amalga oshiriladi. Moliyaviy sektor kiberjinoyatchilar uchun yirik qiziqish uyg‘otadi. Kiberjinoyatchilikni rivojlantirish muammosi jahon bo‘ylab kredit tashkilotlari har yili ko‘radigan yo‘qotishlar ko‘lami tufayli dolzarb ahamiyat kasb etadi. Biroq, hozirgi bosqichda tijorat banklarida kiberxavfsizlik siyosati bevosita muammo yangiligi, alohida tashkilotlar darajasida kiberjinoyatlarga qarshi kurashish amaliyoti yo‘qligi alohida ahamiyat kasb etadi. Shuningdek, ushbu turdagi xavfni tahlil qilish va baholashdagi qiyinchilik tufayli kiberxavflarni modellashtirish, jumladan bank sektorida kam rivojlanadi. Bu bevosita kiburhujum imkoniyatlari bilan belgilanadi.

Tijorat banklarida kiberxavfsizlik siyosatini amalga oshirish yuzasidan turli tadqiqotlar olib borilgan. Xususan, kiberhujum iqtisodiy, texnik yoki axborot zararini yetkazishga qaratilgan dasturiy va apparat vositalarini o‘z ichiga olgan qasddan tashkil etilgan harakatlar majmuidir [1]. Kiberhujum oqibatida tijorat banklarida kiberjinoyatlar paydo bo‘lishi mumkin. Chunki, banklarda kiberjinoyatlar keltirib chiqaradigan muammolarni o‘rganib chiqiladi hamda bunda xavfsizlikni kuchaytirish uchun banklar va hukumat tomonidan amalga oshirilayotgan turli choralar ta’kidlanadi [2]. Mavjud muammolarni bartaraf qilish uchun tijorat banklari faoliyati qat’iy tartibga solinishi talab etiladi. Banklar faoliyati qat’iy tartibga solinadi va direktorlar Kengashi aktsiyadorlik jamiyatida yoki mas’uliyati cheklangan jamiyatda yuqori hokimiyat manbaiga aylanadi [3]. Bu borada axborot xavfsizligi siyosatini ishlab chiqish uchun asos bo‘lishi kerak bo‘lgan uning roziligi talab

etiladi. Ushbu loyihalarda turli qarama-qarshiliklar yoki tizim xatolari bo‘lmasligi uchun ushbu bo‘linmalar birgalikda ishlashi kerak. Ba’zan, ular bilan tashqi maslahatchilar va ishlab chiquvchilar keng jalb qilinadi. Shu bois, tijorat banklarida kiberxavfsizlik siyosati mijozlar ma’lumotlari va aktivlarini himoya qilish, shuningdek, kredit tashkiloti obro‘sini saqlab qolishdan iborat bo‘ladi.

Shuningdek, bugungi kunda mamlakatimizda ham kiberxavfsizlik sohasidagi munosabatlarni tartibga solish borasida O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni qabul qilingan [4]. Bu qonun turli kiberjinoyatlarni oldini olishga qaratiladi. Kiberjinoyat kuchli hackerlar tomonidan amalga oshiriladi. Davlatga, jamiyatga xavf tug‘diradigan harakatlarni paydo qiladi. Bunda asosiy maqsad pul undurish va yuqorida aytganimizdek xavfli harakatlarni vujudga keltirishdir [5]. Shunga asosan, kiberxavfsizlik siyosati tijorat banklarida O‘zbekiston Respublikasi Markaziy banki tomonidan tartibga solinadi. 2023-yilda Markaziy bankning kiberxavfsizlik markazi tashkil etildi, uning vazifasi bank axborot tizimlarining kiberxavfsizligini ta’minlash bo‘yicha choralarni muvofiqlashtirishdan iborat. 2024-yilda Markaziy bankka kiberxavflarni aniqlash va oldini olish choralarini ko‘rish bo‘yicha qo‘shimcha vakolatlar berildi. Shuningdek, kiberjinoyatchilikka qarshi kurashish uchun Kaspersky laboratoriyasi bilan hamkorlikdagi o‘quv tadbirlari o‘tkazildi.

Tijorat banklarida kiberxavfsizlik siyosati o‘z maqsad va vazifalariga ega bo‘ladi. Buning uchun bank atrofidagi axborot muhitining doimiy o‘zgarishini hisobga olgan holda tahdidlarni aniqlash va prognozlashtirish, interferentsiya va ruxsatsiz kirishdan himoya qilish hamda tahdidlarga javoblar tezkor bo‘lishi kerak. Zarar oldini olish va kamaytirish uchun sharoit yaratish, himoyaga kompleks yondashuvni amalga oshirish hamda bank axborot tizimining barcha tarkibiy qismlari himoyalangan bo‘lishi kerak. Ularning yo‘nalishlariga elektron hujjat aylanishi, to‘lov tizimlari, kartalarga xizmat ko‘rsatish, bank dasturlari paketlari va ma’lumotlar bazasining zaxira nusxalari kabilar kiradi. Ishonchlilik va nosozliklarga chidamliligini ta’minlash, nosozlik yuz berganda tez tiklanish amalga oshiriladi. Texnik va ma’muriy vositalar yordamida foydalanuvchi ruxsatini ajratish. Bundan tashqari, kiberxavfsizlik siyosati xodimlarni o‘qitishni o‘z ichiga oladi. Chunki, kiberxavfsizlik sohasidagi tahdidlar doimiy ravishda o‘zgarib turadi. Bu esa xodimlarni mumkin bo‘lgan tahdidlarga tayyorlash va tashkilot ichida xavfsizlik madaniyatini yaratishga yordam beradi. Shunga asosan, tijorat banklarida kiberxavfsizlik siyosati quyidagi asosiy yo‘nalishlarga ega bo‘ladi:

- ma’lumotlarni himoya qilish: Banklar mijozlar shaxsiy ma’lumotlari, hisob raqamlari, kredit karta ma’lumotlari va boshqa maxfiy ma’lumotlarni himoya qilishi kerak. Kiberxavfsizlik siyosati ma’lumotlarni ruxsatsiz kirish, o‘g‘irlash, o‘zgartirish yoki yo‘q qilishdan himoya qilish uchun chora-tadbirlarni belgilaydi.

- moliyaviy yo‘qotishlarning oldini olish: Kiberhujumlar banklar uchun katta moliyaviy yo‘qotishlarga olib kelishi mumkin. Kiberxavfsizlik siyosati firibgarlik, pul o‘g‘irlash, ma’lumotlarni buzish va boshqa kiber jinoyatlarning oldini olishga qaratilgan.

- obro‘ni saqlash: Kiberhujum bankning obro‘siga jiddiy zarar yetkazishi mumkin. Kiberxavfsizlik siyosati bankning obro‘sini himoya qilish, mijozlar ishonchini saqlash va kiberhujumlarni oldini olish uchun chora-tadbirlarni o‘z ichiga oladi.

- qonunchilikka rioya qilish: Banklar kiberxavfsizlik bilan bog‘liq qonunlar, qoidalar va standartlarga rioya qilishlari kerak. Kiberxavfsizlik siyosati bankning qonunchilik talablariga muvofiqligini ta’minlaydi.

- biznes uzluksizligini ta’minlash: Kiberhujum bankning operatsiyalarini to‘xtatib qo‘yishi mumkin. Kiberxavfsizlik siyosati biznesning uzluksizligini ta’minlash, kiberhujumdan keyin operatsiyalarni tezda tiklash va xizmatlarni qayta tiklash uchun chora-tadbirlarni belgilaydi.

Shuningdek, tijorat banklarida kiberxavfsizlik siyosatining asosiy unsurlariga quyidagi unsurlar kiradi (1-jadval):

1-jadval

Tijorat banklarida kiberxavfsizlik siyosatining asosiy unsurlari[1]

№	Asosiy unsurlari	Unsurlarning asosiy yo‘nalishlari
1	**Risklarni baholash**	Bank kiberxavfsizlik risklarini muntazam ravishda baholashi va ularni kamaytirish uchun chora-tadbirlar ko‘rishi kerak
2	**Xavfsizlik texnologiyalari**	Bank xavfsizlik devorlari, antivirus dasturlari, kirishni aniqlash tizimlari va boshqa xavfsizlik texnologiyalaridan foydalanishi kerak
3	**Xodimlarni o‘qitish**	Bank xodimlari kiberxavfsizlik bo‘yicha o‘qitilishi va kiberhujumlarni aniqlash va ularga qarshi kurashish bo‘yicha bilim va ko‘nikmalarga ega bo‘lishlari kerak
4	**Voqealarni boshqarish**	Bank kiberxavfsizlik hodisalarini aniqlash, ularga javob berish va ularni bartaraf etish uchun reja tuzishi kerak
5	**Risklarni boshqarish**	Bank yetkazib beruvchilar kiberxavfsizligini baholashi va ular xavfsizligini ta’minlashi kerak
6	**Muntazam tekshiruvlar**	Bank kiberxavfsizlik siyosati va tizimlarini muntazam ravishda tekshirib turishi kerak

Shu bilan birga, tijorat banklari sektorida kiberxavflarni baholash samaradorligi va sifatini oshirishning quyidagi asosiy yo‘nalishlarini qayd etish mumkin:

- risklar bo‘yicha statistik ma’lumotlarni to‘plash va ulardan foydalanish asosida baholash ob’ektivligini oshirish;

- baholash jarayonini optimallashtiradigan eng muhim tizimlar uchun xavf omillarining asosiy ro‘yxatini shakllantirish;

- bank risklarini baholashning boshqa usullaridan foydalangan holda modelni qurish usullarini takomillashtirish;

- xavf omillarini miqdoriy baholashning sifat baholashdan ustunligi va boshqalar.

Xulosa qilib aytganda, kiberxavfsizlik siyosati tijorat banklarining ajralmas qismi sifatida tijorat banklari ma’lumotlarini himoya qilish, moliyaviy yo‘qotishlarning oldini olish, obro‘ni saqlash, qonunchilikka rioya qilish va biznesning uzluksizligini ta’minlash uchun zarur bo‘ladi. Kuchli kiberxavfsizlik siyosati bankning raqamli muhitda muvaffaqiyatli ishlashiga imkon beradi. Shu bois, tijorat banklarida kiberxavfsizlik siyosati muhim ahamiyat kasb etadi. Chunki, tijorat banklari yirik hajmdagi moliyaviy ma’lumotlarni saqlaydi va qayta ishlaydi. Bu esa ularni kiberhujumlar uchun asosiy nishonga aylantiradi. Kiberhujumlar bankning obro‘iga putur yetkazishi, mijozlar ishonchini yo‘qotishiga olib kelishi va katta moliyaviy zararlar keltirishi mumkin. Shu bois, kuchli kiberxavfsizlik siyosati tijorat bank barqarorligi va mijozlar ishonchini saqlash uchun zarur bo‘ladi.

[1] Muallif ishlanmasi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. // Вопросы кибербезопасности, 2014, №5 (8).
2. Kazakov X. O'zbekiston Respublikasi tijorat banklarida mijozlarning bank plastik kartalari mablag'larining xavfsizligi va kiberjinoatchilikka qarshi kurashish va oldini olish. // International journal of scientific researchers (IJSR) INDEXING, Vol. 6, No1 (2024)
3. https://searchinform.ru/products/kib/politiki-informatsionnoj-bezopasnosti/politika-informacionnoj-bezopasnosti-banka/
4. O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni. Manba: https://lex.uz/docs/-5960604
5. Kazakov X. O'zbekiston Respublikasi tijorat banklarida mijozlarning bank plastik kartalari mablag'larining xavfsizligi va kiberjinoatchilikka qarshi kurashish va oldini olish. // International journal of scientific researchers, Vol.6, No.1 (2024).