KIBERXAVFSIZLIK VA RAQAMLI MOLIYAVIY XIZMATLARDA XAVFLARNI BOSHQARISH

Muallif: **Radjabov Azimjon**
Ilmiy yo'nalish: **Moliya va moliyaviy texnologiya**

Annotatsiya. Ushbu maqolada raqamli moliyaviy xizmatlar sohasidagi kiberxavflarning tasnifi, ularni boshqarishning zamonaviy metodologiyalari va xalqaro tartibga solish amaliyoti tahlil qilinadi. Tadqiqotning maqsadi — moliya muassasalari uchun kiberxavflarni boshqarishning tizimli yondashuvini asoslash va uni operatsion risklarni boshqarish tizimi bilan bog'lashdan iborat. Tahlil ENISA, NIST, ISO va Basel bank nazorati qo'mitasi hujjatlari hamda sohadagi empirik tadqiqotlar natijalariga tayanadi. Maqolada raqamli moliyaviy xizmatlarga xos asosiy kiberxavflar — fishing va sotsial injeneriya, ransomware hujumlari, DDoS hujumlari hamda ma'lumotlar oqishi tasniflangan; NIST va ISO 27001 doiralari asosida kiberxavflarni boshqarishning besh bosqichli sikli taklif etilgan. Tahlil natijalari kiberxavflarga qarshi kurashishda texnik vositalar bilan bir qatorda boshqaruv, tashkiliy va tartibga soluvchi vositalar majmuasining hal qiluvchi ahamiyatga ega ekanligini ko'rsatadi. Xulosalarda kiberxavfsizlikni muassasa miqyosidagi risklarni boshqarish tizimiga integratsiya qilish va kiberbarqarorlikni ta'minlash bo'yicha tavsiyalar bayon etilgan.

Kalit so'zlar: kiberxavfsizlik; raqamli moliyaviy xizmatlar; kiberxavflar; operatsion risklar; risklarni boshqarish; kiberbarqarorlik.

Аннотация. В статье анализируются классификация киберугроз в сфере цифровых финансовых услуг, современные методологии управления киберрисками и международная практика регулирования. Цель исследования — обосновать системный подход к управлению киберрисками для финансовых учреждений и интегрировать его в систему управления операционными рисками. Анализ опирается на документы ENISA, NIST, ISO и Базельского комитета по банковскому надзору, а также на результаты эмпирических исследований. В работе классифицируются основные киберугрозы, характерные для цифровых финансовых услуг — фишинг и социальная инженерия, атаки программ-вымогателей (ransomware), DDoS-атаки и утечки данных; на основе рамок NIST и ISO 27001 предлагается пятиэтапный цикл управления киберрисками. Результаты показывают, что наряду с техническими средствами решающее значение в противодействии киберугрозам имеют управленческие, организационные и регуляторные инструменты. В заключении сформулированы рекомендации по интеграции кибербезопасности в систему управления рисками учреждения и обеспечению киберустойчивости.

Ключевые слова: кибербезопасность; цифровые финансовые услуги; киберриски; операционные риски; управление рисками; киберустойчивость.

Abstract. The paper analyzes the classification of cyber threats in digital financial services, modern methodologies for managing cyber risks, and international regulatory practice. The purpose of the study

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

is to substantiate a systematic approach to cyber risk management for financial institutions and to integrate it into the operational risk management framework. The analysis draws on the documents of ENISA, NIST, ISO and the Basel Committee on Banking Supervision, as well as on empirical research findings. The study classifies the main cyber threats specific to digital financial services — phishing and social engineering, ransomware attacks, DDoS attacks and data breaches; based on the NIST and ISO 27001 frameworks, a five-stage cyber risk management cycle is proposed. The results indicate that, alongside technical measures, managerial, organizational and regulatory instruments play a decisive role in countering cyber threats. The conclusion outlines recommendations for integrating cybersecurity into the institution-wide risk management system and ensuring cyber resilience.

Keywords: cybersecurity; digital financial services; cyber risks; operational risks; risk management; cyber resilience.

1. Kirish

So'nggi o'n yillikda moliyaviy xizmatlarni yetkazish shakllari tubdan o'zgardi: mobil banking, onlayn to'lov platformalari va raqamli kreditlash xizmatlari keng tarqaldi. Raqamlashtirish mijozlar uchun qulaylik, muassasalar uchun samaradorlik yaratgan bo'lsa-da, bir yo'la, hujumlar yuzasi ham keskin kengaydi. Ilmiy adabiyotlarda kiber risk moliyaviy tizim uchun tizimli xavf manbai sifatida talqin etilmoqda: kiberhodisalar individual muassasa zararidan tashqari, bozorlararo bog'liqlik orqali butun sektorga tarqalishi mumkin [1].

O'zbekistonda «Raqamli O'zbekiston — 2030» strategiyasi doirasida moliya sohasini raqamlashtirish davlat siyosatining ustuvor yo'nalishi etib belgilangan [2]. To'lov tizimlarining rivojlanishi, elektron hukumat xizmatlari bilan integratsiya va fintech kompaniyalarning faollashuvi kiberxavfsizlikni ta'minlash muammosini keskin dolzarblashtirdi. Shu bois tijorat banklari va fintech tashkilotlari uchun kiberxavflarni tizimli boshqarish nafaqat texnik, balki iqtisodiy va tashkiliy muammo sifatida maydonga chiqdi.

Tadqiqotning maqsadi — raqamli moliyaviy xizmatlarda kiberxavflarni boshqarishning tizimli yondashuvini asoslashdan iborat. Ushbu maqsadga erishish uchun quyidagi vazifalar belgilangan: kiberxavflarni tasniflash; xalqaro boshqaruv metodologiyalarini tahlil qilish; ularni moliya muassasalari amaliyotiga moslashtirish bo'yicha tavsiyalar ishlab chiqish.

2. Raqamli moliyaviy xizmatlarda kiberxavflarning tasnifi

Kiber risk — axborot tizimlari va tarmoqlar orqali amalga oshiriladigan hujumlar natijasida muassasa ma'lumotlari, moliyaviy resurslari yoki obro'sining zarar ko'rish ehtimolidir. Xalqaro miqyosda kiber tahdidlar landshafti muntazam monitoring qilib boriladi: ENISA hisobotlariga ko'ra, so'nggi yillarda ransomware eng keng tarqalgan tahdidlardan biri bo'lib qolmoqda, sotsial injeneriya hujumlarining murakkablashuvi esa alohida tashvish uyg'otadi [3]. Ma'lumotlar oqishining o'rtacha global zarari 2023-yilda 4,45 mln AQSH dollarini tashkil etgan bo'lib, moliya sohasi ushbu ko'rsatkich bo'yicha yetakchi tarmoqlardan biri sifatida qolmoqda [4].

Kiberxavfsizlik faqat texnologiya masalasi emasligi adabiyotlarda alohida ta'kidlanadi: samarali himoya boshqaruv, tashkiliy madaniyat va odam omili bilan uzviy bog'liq [5]. Shu nuqtai nazardan raqamli moliyaviy xizmatlardagi asosiy kiberxavflar tasnifini shakllantirish mumkin (1-jadval).

1-jadval. Raqamli moliyaviy xizmatlardagi asosiy kiberxavflar tasnifi

Xavf turi	Mohiyati	Mumkin bo'lgan oqibatlar	Boshqaruv vositalari

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

Xavf turi	Mohiyati	Mumkin bo'lgan oqibatlar	Boshqaruv vositalari
Fishing va sotsial injeneriya	Mijoz yoki xodimni firibgarlik yo'li bilan maxfiy ma'lumotlarni oshkor qilishga undash	Mijoz vositalarining o'g'irlanishi, reputatsion zarar	Xabardorlikni oshirish, ikki faktorli autentifikatsiya
Ransomware hujumlari	Tizimlarni shifrlab, tovon puli talab qilish	Xizmatlarning uzilishi, ma'lumotlar yo'qolishi	Zaxira nusxalar, tarmoq segmentatsiyasi, EDR vositalari
DDoS hujumlari	Serverlarga ommaviy so'rovlar orqali hujum uyushtirish	Onlayn xizmatlarning ishdan chiqishi	Trafikni filtrlash, bulutli himoya xizmatlari
Ma'lumotlar oqishi	Shaxsiy va moliyaviy ma'lumotlarning oshkor bo'lishi	Jarimalar, sud da'volari, ishonch pasayishi	Ma'lumotlarni shifrlash, kirishni nazorat qilish
API va mobil ilovalar zaifliklari	Ilovalararo o'zaro ta'sir qatlamidagi nuqsonlar	Operatsiyalarga ruxsatsiz kirish	Xavfsiz dasturlash, muntazam pen-test
Ichki xavflar	Xodimlar yoki hamkorlar tomonidan suiiste'mol	Maxfiylik buzilishi, firibgarlik	Kirish huquqlarini cheklash, audit

Manba: [3, 8] asosida muallif tuzishi.

3. Kiberxavflarni boshqarish metodologiyasi

Xalqaro amaliyotda kiberxavflarni boshqarish uchun bir necha yetakchi doiralar qo'llaniladi. NIST kibermakon doirasi (CSF) 2.0 boshqaruv (Govern), aniqlash (Identify), himoya (Protect), hodisalarni detektlash (Detect), javob berish (Respond) va tiklanish (Recover) funksiyalaridan iborat siklni taklif etadi [6]. ISO/IEC 27001 standarti esa axborot xavfsizligini boshqarish tizimini doimiy takomillashtiruvchi (Plan–Do–Check–Act) sikliga tayanadi [7]. Ikkala doira ham kiberxavfni faqat texnik muammo emas, balki boshqaruv jarayoni sifatida ko'radi.

Bank sektorida kiber risk operatsion risklarning tarkibiy qismi sifatida qaraladi: Basel qo'mitasi operatsion risklarni ovoz chiqarib boshqarish tamoyillarida axborot xavfsizligi va kiber barqarorlikka alohida urg'u bag'ishlaydi [8]. Tartibga soluvchi amaliyot esa nazorat organlari bilan axborot almashinuvi, kiberhodisalarni hisobot qilish va milliy javob rejalari talablarini o'z ichiga oladi [9]. Ushbu yondashuvlarni umumlashtirgan holda, kiberxavflarni boshqarish siklini besh bosqichga ajratish mumkin (2-jadval).

2-jadval. Kiberxavflarni boshqarish siklining bosqichlari

Bosqich	Mazmuni	Asosiy vositalar
1. Xavflarni aniqlash	Aktivlar ro'yxati, zaifliklar va tahdid manbalarini belgilash	Vulnerability assessment, aktivlar auditi

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

Bosqich	Mazmuni	Asosiy vositalar
2. Xavflarni baholash	Ehtimollik va zarar darajasini baholash, xavflarni reytinglash	Risk matritsasi, szenariy tahlili, stress-test
3. Boshqaruv choralari	Texnik, tashkiliy va yuridik vositalarni tanlash	Kirish nazorati, shifrlash, ichki siyosatlar
4. Javob berish	Hodisalarga tezkor munosabat va lokalizatsiya	Incident response reja, SOC xizmati
5. Monitoring va tiklanish	Doimiy nazorat, sabablarni tahlil qilish va tiklash	SIEM tizimlari, zaxira nusxalar, trenajyorlar

Manba: [6, 7] asosida muallif tuzishi.

Tadqiqotda taqqoslama tahlil, mazmun tahlili va tizimli yondashuv usullaridan foydalanildi. Empirik bazani xalqaro tashkilotlar (ENISA, BIS, NIST) rasmiy hisobotlari, milliy tartibga solish hujjatlari hamda sohadagi ilmiy nashrlar tashkil etdi. Ushbu manbalar majmui kiberxavflarni boshqarishning xalqaro tajribasini yaxlit tasvirlash imkonini berdi.

4. Tahlil natijalari va ularning muhokamasi

O'tkazilgan tahlil kiber riskning uchta o'ziga xos xususiyatini ko'rsatadi. Birinchidan, uning o'lchovi an'anaviy moliyaviy risklardan farq qiladi: hodisalar statistikasi chekli, ma'lumotlar notekis va tahdidlar tez mutatsiyaga uchraydi, shuning uchun ehtimollik modellariga tayanish bilan birga szenariy va stress-test yondashuvlarini qo'llash maqsadga muvofiq [1]. Ikkinchidan, zarar miqyosi muassasa o'lchami bilan emas, uning raqamli integratsiyalashganlik darajasi bilan ortib boradi: qanchalik ko'p xizmatlar onlayn rejimga o'tgansa, potensial zarar shunchalik yuqori bo'ladi [4]. Uchinchidan, boshqaruv samaradorligi texnik vositalardan ko'ra boshqaruv tuzilmalariga — mas'uliyat taqsimoti, budjet ajratish va xodimlar malakasiga bog'liq bo'lmoqda [5].

Moliya muassasalari uchun amaliy jihatdan uchta muammo alohida e'tibor talab qiladi. Birinchisi, eskirgan tizimlar bilan zamonaviy raqamli xizmatlarni parallel yuritish zaiflik zanjirlarini ko'paytiradi. Ikkinchisi, autsorsing va hamkorlik aloqalari kengaygan sari uchinchi tomon xavflari kuchayadi: hamkor provayderlarning xavfsizlik darajasi muassasa o'zining darajasi bilan barobar bo'lib qolmoqda. Uchinchisi, kiberxavfsizlik mutaxassislari tanqisligi soha miqyosidagi umumiy muammo bo'lib qolmoqda. Bularga qarshi javob sifatida kiberbarqarorlik — ya'ni hodisaga uchraganda ham muhim funksiyalarni saqlab qolish va tez tiklanish salohiyati — tamoyilini qabul qilish taklif etiladi [6, 8].

Zarar effektlarini yumshatishning qo'shimcha vositasi sifatida kiber sug'urtasi maydonga chiqmoqda. Biroq xalqaro tajriba shuni ko'rsatadiki, sug'urta preventiv choralarni almashtira olmaydi; aksincha, sug'urtashuv shartlari sifatida ma'lum darajadagi xavfsizlik standartlariga rioya qilish talab etiladi. Shu ma'noda kiber sug'urtasi himoya sarmoyalarining qo'shimcha rag'batlantiruvchisi vazifasini bajarishi mumkin [9].

5. Xulosa

Tadqiqot natijalari asosida quyidagi xulosalarga kelindi. Raqamli moliyaviy xizmatlarda kiberxavflar operatsion risklarning eng dinamik va tizimli xavfli yo'nalishi bo'lib, ularni boshqarish aniqlash, baholash, himoya, javob berish va tiklanish bosqichlaridan iborat yagona siklda tashkil etilishi lozim. NIST va ISO 27001 doiralari ushbu siklning amaliy shakllari sifatida xalqaro e'tirofga ega; bank sektorida esa ular Basel operatsion risk tamoyillari bilan uyg'unlashtirilishi zarur.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

Amaliy tavsiyalar sifatida quyidagilar taklif etiladi: kiberxavfsizlikni muassasa miqyosidagi risklarni boshqarish tizimiga integratsiya qilish va mas'uliyatni rahbariyat darajasida belgilash; xodimlar va mijozlarning kiber savodxonligini oshirish bo'yicha muntazam tadbirlarni amalga oshirish; hodisalarga javob rejalari va zaxira nusxalarni muntazam sinovdan o'tkazish; milliy nazorat organi bilan axborot almashinuvi mexanizmlarini yo'lga qo'yish. Umuman olganda, kiberxavfsizlikni raqamli moliyaviy xizmatlarni rivojlantirish strategiyasining ajralmas qismi sifatida ko'rish uzoq muddatda mijozlar ishonchini va moliyaviy barqarorlikni mustahkamlashning muhim sharti bo'lib xizmat qiladi.

Foydalanilgan adabiyotlar

1. Aldasoro I., Gambacorta L., Giudici P., Leach T. The drivers of cyber risk // Journal of Financial Stability. – 2022. – Vol. 60. – Article 100989.
2. O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni: «Raqamli O'zbekiston — 2030» strategiyasi to'g'risida.
3. ENISA Threat Landscape 2023. – Athens: European Union Agency for Cybersecurity, 2023.
4. IBM Security. Cost of a Data Breach Report 2023. – Armonk, NY: IBM Corporation, 2023.
5. Dhillon G., Backhouse J. Information system security management in the new millennium // Communications of the ACM. – 2001. – Vol. 44, No. 7. – P. 125–128.
6. NIST. The NIST Cybersecurity Framework (CSF) 2.0. – Gaithersburg, MD: National Institute of Standards and Technology, 2024.
7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva: ISO, 2022.
8. Basel Committee on Banking Supervision. Revisions to the Principles for the Sound Management of Operational Risk. – Basel: Bank for International Settlements, 2021.
9. Crisanto J. C., Prenio J. Regulatory frameworks for cybersecurity. – FSI Insights No. 15. – Basel: Bank for International Settlements, 2017.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.