3
5
(№09-07)
iyul

MOLIYA TIZIMIDA KIBERXAVFSIZLIK MASALALARI

Sabirova Dildor Arifovna
Xalqaro Nordik universiteti “Sanoatni boshqarish
va raqamli texnologiyalar” kafedrasi dotsenti
Email: dildorsabirova11@gmail.com

Azizov Olim Maxmudovich
Toshkent xalqaro moliyaviy boshqaruv va texnologiyalar universiteti
“Moliya, bank ishi va buxgalteriya hisobi” kafedrasi dotsenti
Email: olimmaxmud@gmail.com
DOI: *https://doi.org/10.55439/EIT/vol13_iss3/678*

Moliya tizimida raqamli kanallar orqali millionlab tranzaksiyalar amalga oshirilayotgan bugungi kunda, ularning xavfsizligini ta’minlash moliyaviy tizimlarga bo‘lgan ishonch va barqarorlikni kiberxavflar – fishing, ijtimoiy muhandislik, zararli dasturlar, DDoS hujumlari va API hujumlari keng tahlil qilingan hamda moliyaviy tashkilotlar uchun raqamli xavfsizlikni ta’minlashda kompleks yondashuv muhimligi ko‘rsatib o‘tilgan.

Kalit so’zlar: Moliya tizimi, kiberxavfsizlik, fishing, ijtimoiy muhandislik zararli dasturlar, DDoS hujumlar, API hujumlar, ko‘p omilli autentifikatsiya.

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ В ФИНАНСОВОЙ СИСТЕМЕ

Сабирова Дилдор Арифовна
Доцент кафедры«Промышленный менеджмент и цифровые технологии» Международного Нордик университета
Азизов Олим Махмудович
Доцент кафедры «Финансы, банковское дело и бухгалтерский учет» Ташкентского международного университета финансового управления и технологий

Аннотация
В современном мире, где в финансовой системе ежедневно совершаются миллионы транзакций через цифровые каналы, обеспечение их безопасности является важным фактором для поддержания доверия и стабильности финансовых структур. В статье подробно анализируются основные киберугрозы, с которыми сталкиваются финансовые организации, такие как фишинг, социальная инженерия, вредоносные программы, DDoS-атаки и атаки на API. Также подчеркивается важность комплексного подхода к обеспечению цифровой безопасности в финансовом секторе.
Ключевые слова: Финансовая система, кибербезопасность, фишинг, социальная инженерия, вредоносные программы, DDoS-атаки, API-атаки, многофакторная аутентификация.

CYBERSECURITY ISSUES IN THE FINANCIAL SYSTEM

D
Associate Professor, Department of Industrial Management and Digital Technologies, International Nordic University
O
Associate Professor, Department of Finance, Banking, and Accounting, Tashkent International University of Financial Management and Technologies

Annotation
In today’s world, where millions of transactions are conducted through digital channels in the financial system, ensuring their security is a crucial factor in maintaining trust and stability in financial institutions. This article provides a detailed analysis of the main cyber threats faced by financial organizations—such as phishing, social engineering, malware, DDoS attacks, and API attacks—and emphasizes the importance of a comprehensive approach to digital security in the financial sector.

Keywords: Financial system, cybersecurity, phishing, social engineering, malware, DDoS attacks, API attacks, multi-factor authentication.

Jarayonlar tobora raqamli shaklga o‘tar ekan, moliya sohasida kiberxavfsizlik masalasi alohida barqarorligini ta’minlashda muhim omilga aylanmoqda. Maximize Market Research kompaniyasining tadqiqotlarga ko‘ra, bank, moliyaviy xizmatlar va sug'urta bozorida [5]

Moliya sohasi kiberjinoyatchilar uchun eng jozibador yo‘nalishlardan biri hisoblanadi. Chunki bu sohada juda katta hajmdagi maxfiy ma’lumotlar saqlanadi va qayta ishlanadi, bu esa uni tajovuzkorlar uchun “qulay o‘lja”ga aylantiradi. Moliya tashkilotlariga qarshi kiberhujumlar pul mablag‘larini o‘g‘irlash, maxfiy ma’lumotlar sizib chiqishi va tizimlarning ishlashida uzilishlarga olib kelishi mumkin.

AQShdagi eng yirik telekommunikatsiya kompaniyalaridan biri **Verizon Communications Inc.** hisobotiga ko‘ra, 2024-yilda aniqlangan **10,626 ta ma’lumot buzilishi** holatining **68% i inson omili** (xatolik, imtiyozlardan noto‘g‘ri foydalanish, o‘g‘irlangan ma’lumotlardan foydalanish yoki ijtimoiy muhandislik) bilan bog‘liq bo‘lgan. [6]

Ushbu maqolada biz moliyaviy tashkilotlar duch kelayotgan asosiy kiberxavflarni ko‘rib chiqamiz hamda moliya bozorining yetakchi vakillari tomonidan ushbu xavflarga qarshi kurashish bo‘yicha qo‘llanilayotgan usullar va amaliy tajribalarni tahlil qilamiz.

Mavzuga oid adabiyotlar sharhi

Raqamli transformatsiya jarayonida moliya sohasi kiberxavfsizlik tahdidlariga eng ko‘p duch keladigan sektorlardan biriga aylangan. Shu sababli, xalqaro miqyosda va O‘zbekistonda ushbu sohada olib borilgan tadqiqotlar kiberxavfsizlikning ahamiyatini va muammolarni chuqur tahlil qilishga qaratilgan.

O‘zbekistonda olib borilgan tadqiqotlar asosan moliyaviy institutlarning kiberxavfsizlikka tayyorgarligi va mavjud tahdidlarni yengish strategiyalariga qaratilgan.

Zokir Mamadiyarov va Doniyar Karshiev tomonidan yozilgan “Cybersecurity in Digital Banking: Safeguarding Customer Trust in Uzbekistan” nomli maqolada raqamli bank

xizmatlarida kiberxavfsizlikning hal qiluvchi o‘rni va uning O‘zbekistonda mijozlar ishonchini ta’minlashdagi ta’siri o‘rganilgan.[1]

A.Abdullaev , M. A.Al Absi, A. A.Al Absi, M.Sain, H. J. Lee tomonidan yozilgan va 2020 yilda bo‘lib o‘tgan 22 Xalqaro Ilg‘or Aloqa Texnologiyalari Konferensiyasi (ICACT) to’plamida chop etilgan “Classify and Analyze the Security Issues and Challenges in Mobile banking in Uzbekistan.” nomli maqolada O‘zbekistonda mobil bank xizmatlaridagi xavfsizlik muammolari tasniflanganhamda tahlil qilingan.[2]

D.D. Savenkova tomonidan yozilgan “Кибербезопасность финансово-кредитных организаций в условиях новых вызовов и угроз в цифровом пространстве” nomli maqolasida moliyaviy-kredit tashkilotlarining kiberhujumlardan himoyalanishi, kiberjinoyatlarga qarshi kurashish va huquqbuzarliklar uchun javobgarlik masalalariga bag‘ishlangan bo‘lib, ushbu muammolarni global darajadagi tahdid sifatida ko‘rib chiqadi.[3]

Tadqiqot metodologiyasi

Ushbu tadqiqot davomida ikkilamchi manbalar asosida tahlil olib borildi. Jumladan, mavzu bo‘yicha internetda e’lon qilingan ilmiy maqolalar, tahliliy hisobotlar, rasmiy veb-saytlarda chop etilgan ma’lumotlar, xalqaro tashkilotlar hamda moliya institutlarining ochiq ma’lumotlari o‘rganildi.

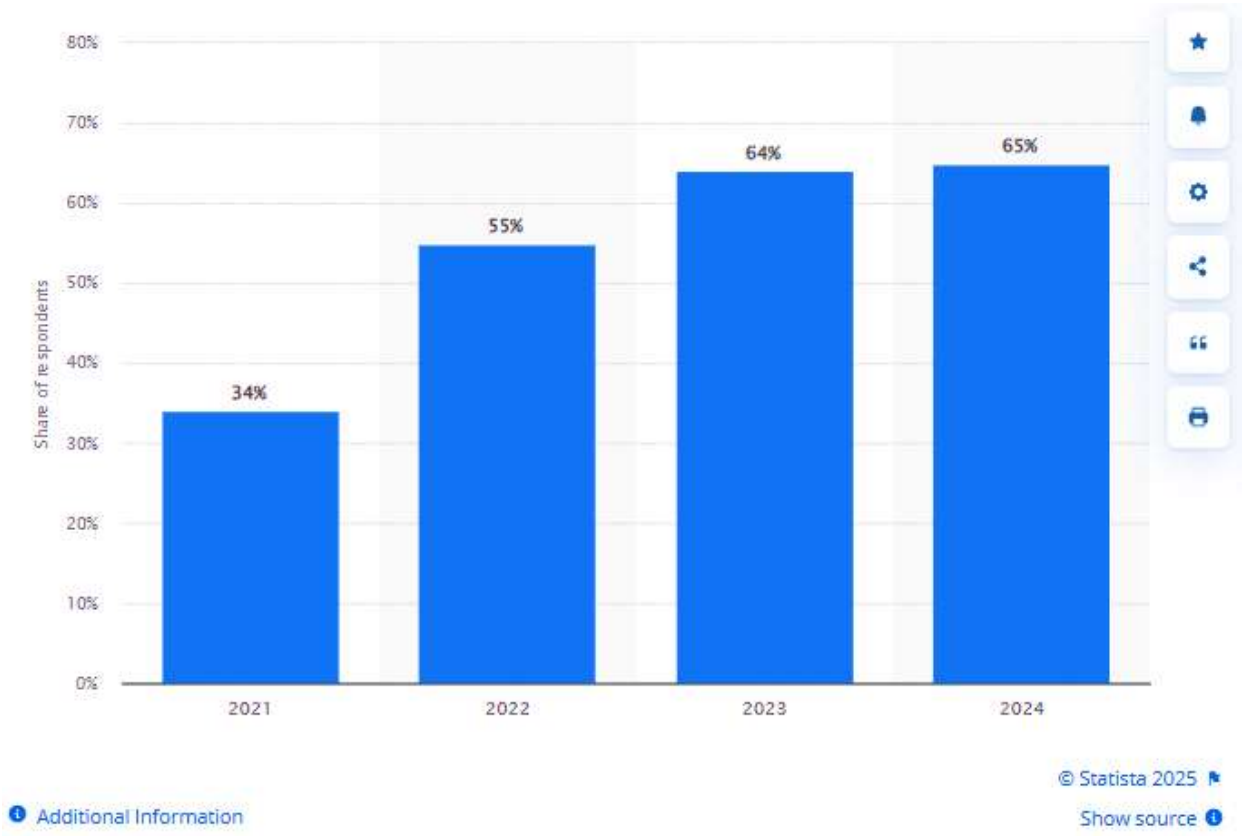
Natijalar

Kiberxavfsizlikni ta’minlash moliyaviy soha uchun hal qiluvchi ahamiyatga ega. Ma’lumotlar va infratuzilmaning ishonchli himoyasini ta’minlash har qanday moliya tashkiloti strategiyasining ajralmas qismidir.

Xalqaro Valyuta Jamg‘armasining (IMF) yangi hisobotiga ko‘ra, moliyaviy sektorda sodir bo‘layotgan kiberhujumlar global moliyaviy barqarorlik uchun jiddiy tahdid tug‘dirmoqda.

Moliyaviy sektor kiberxavf ostida ayniqsa zaif bo‘lib, bunday hujumlar natijasida yuzaga kelgan yo‘qotishlar tizimda katta uzilishlarga olib kelishi mumkin. Hisobotda qayd etilishicha, kiberhujumlar “moliyaviy muassasalarning operatsion barqarorligiga putur yetkazishi va makromoliyaviy barqarorlikka salbiy ta’sir ko‘rsatishi” mumkin.

- kiberhujumlar soni va ularning murakkabligi ortib bormoqda;
- moliyaviy sektor katta hajmdagi maxfiy ma’lumotlar va tranzaksiyalar bilan ishlaydi, bu esa uni alohida zaif qilmoqda;
- moliyaviy tashkilotlar uchun kiberhujumlar moliyalashtirish muammolari, obro‘ga putur yetishi, hattoki, bankrotlikka olib kelishi mumkin;
- 2000-yildan beri kiberhujumlarning 20% moliyaviy sektorga to‘g‘ri kelgan va $12 milliard bevosita yo‘qotishlar yuzaga kelgan;
- 2020-yildan beri bevosita yo‘qotishlar taxminan $2.5 milliardni tashkil etgan.[4]



1-rasm. 2021-yildan 2024-yilgacha dunyo bo‘yicha moliyaviy tashkilotlarga qilingan ransomware (ma'lumotlarni garovga oluvchi) hujumlar ulushi [8]

Xalqaro Valyuta Jamg‘armasining Global Moliyaviy Barqarorlik Hisobotiga ko‘ra, banklar kiberhujumlar uchun eng ko‘p nishon bo‘lmoqda. Bu yo‘qotishlarga bilvosita zararlar va obro‘ga salbiy ta’sirlar ham qo‘shilsa, real ko‘rsatkichlar yanada yuqori bo‘lishi mumkin.

Bugungi kunda moliya tizimida axborotlarga tahdidlar ko’rinishlarini ko’rib chiqamiz.

Fishing. Fishing hujumlari bu firibgarlik usullari bo‘lib, tajovuzkorlar ishonchli manba (masalan, bankdan kelgan elektron xabar yoki sayt) ko‘rinishida foydalanuvchilardan login, parol va bank rekvizitlari kabi maxfiy ma’lumotlarni olishga urinishadi. Ushbu hujum turi eng keng tarqalgan bo‘lib, tobora ommalashib bormoqda. “Kasperskiy laboratoriyasi” ma’lumotlariga ko‘ra, 2024-yilda Kaspersky xavfsizlik yechimlari butun dunyo bo‘ylab **893 milliondan ortiq fishing urinishlarini** aniqlab, ularni bloklagan. Bu 2023-yilga nisbatan **26% o‘sishni** anglatadi.[7]

Ijtimoiy muhandislik. Ijtimoiy muhandislik — bu tajovuzkorlarning odamlarni aldash orqali maxfiy ma’lumotlar yoki tizimlarga kirish imkonini qo‘lga kiritishga qaratilgan manipulyativ usullaridan biridir. Moliyaviy sektorda bunday usullar bank hisoblariga, moliyaviy ma’lumotlarga va boshqa axborotlarga kirish uchun ishlatiladi.

Zararli dasturlar. Zararli dasturiy ta’minot — bu moliyaviy sektor uchun eng jiddiy xavflardan biridir. Ular kompyuter tizimlari, tarmoqlar va ma’lumotlarga zarar yetkazish uchun mo‘ljallangan dasturlardir. Bunday dasturlar orqali maxfiy ma’lumotlar o‘g‘irlanadi, moliyaviy firibgarliklar amalga oshiriladi yoki tashkilotning normal faoliyatiga xalaqit yetkaziladi.

DDoS hujumlar. Xizmat ko‘rsatishdan voz kechish (DDoS) hujumlari moliya muassasalarining serverlari va tarmoq infratuzilmasini haddan tashqari yuklab, ularning

onlayn xizmatlarini vaqtincha ishdan chiqarishga qaratilgan. Bu kompaniyalar va ularning mijozlariga jiddiy moliyaviy yo‘qotishlar olib kelishi mumkin.

API hujumlar. Zamonaviy bank xizmatlarida turli tizimlarni birlashtirish va ma’lumot almashinuvi uchun dasturiy interfeyslar (API) tobora keng qo‘llanilmoqda. Biroq, API ishlatish xavfsizlik nuqtai nazaridan yangi zaifliklarni yuzaga keltiradi. Bu hujumlar autentifikatsiya tizimlarini chetlab o‘tish, himoyalangan ma’lumotlarga kirish va noto‘g‘ri ma’lumot yuborish orqali dasturiy ta’minot faoliyatini buzishga qaratilgan bo‘ladi.

Kiberxavfsizlik bo‘yicha samarali choralarni ishlab chiqish nafaqat maxfiy ma’lumotlarni himoya qilish, balki moliyaviy yo‘qotishlarning oldini olish, mijozlar ishonchini saqlab qolish va qonunchilik talablariga rioya etishni ta’minlash imkonini beradi. Bugungi kunda moliya

Maxfiy ma’lumotlarni himoya qilish. Maxfiy ma’lumotlarni himoya qilish moliya muassasalari oldidagi ustuvor vazifalardan biridir. Raqamli texnologiyalarning jadal rivojlanishi va onlayn platformalarga o‘tish bilan birga, saqlanayotgan va uzatilayotgan axborot hajmi sezilarli darajada oshdi. Mijozlarning shaxsiy ma’lumotlari, bank rekvizitlari va boshqa maxfiy ma’lumotlar ruxsatsiz kirish, o‘g‘irlik yoki sizib chiqishdan ishonchli himoyalangan bo‘lishi juda muhim;

Moliyaviy yo‘qotishlarning oldini olish. Kiberhujumlar moliyaviy tashkilotlarga jiddiy zarar yetkazishi mumkin, bu esa bevosita moliyaviy zararlarga olib keladi. Bank tizimlarining buzilishi, firibgarlik operatsiyalari, mablag‘larni o‘g‘irlash — bularning barchasi nafaqat kompaniyaning moliyaviy barqarorligiga, balki mijozlar va hamkorlar ishonchiga ham xavf tug‘diradi;

Mijozlar ishonchini saqlab qolish. Moliya tashkilotlari mijozlari o‘z mablag‘lari va shaxsiy ma’lumotlari ishonchli himoyada bo‘lishini kutishadi. Yuqori darajadagi kiberxavfsizlikni ta’minlash mijozlar ishonchini saqlashga va moliyaviy xizmatlardan qoniqish darajasini oshirishga xizmat qiladi. Mijozlar odatda ma’lumotlarining eng yuqori darajada himoyalanganiga ishonch hosil qiladigan tashkilotlarni tanlaydi;

Moliyaviy sohadagi keng tarqalgan kiberxavflar va hujum turlari. Moliyaviy sektorda kompaniyalar va ularning mijozlariga jiddiy zarar yetkazishi mumkin bo‘lgan turli xil kiberxavf va hujum turlari mavjud. Ushbu xavflarni chuqur tushunish — samarali kiberxavfsizlik strategiyalarini ishlab chiqish yo‘lidagi muhim qadamlardan biridir.

. Ushbu natijalar moliya tizimi kiberxavfsizlik sohasida jiddiy islohotlarga ehtiyoj borligini ko‘rsatadi.

Kiberxavfsizlik bo‘yicha samarali choralar ko‘rish — mijozlarning maxfiy ma’lumotlarini

Masalan, ko‘p omilli autentifikatsiya — bu foydalanuvchining shaxsini tasdiqlash uchun Foydalanuvchiga tizim yoki resurslarga kirish ruxsatini berishdan oldin, u bir nechta omillar orqali o‘z shaxsini tasdiqlashi kerak bo‘ladi.

Ko‘p omilli autentifikatsiya xavfsizlik darajasini oshiradi, chunki agar omillardan biri buzilgan bo‘lsa ham, tizimga kirish hali ham himoyalangan bo‘lib qoladi. Masalan, xodim fishing havolasini tanimay qolib, o‘z hisob ma’lumotlarini fishing saytiga kiritsa ham, ko‘p

orqali amalga oshiriladigan hujumlar paytida ham ko‘p omilli autentifikatsiya yordamida firibgarlikni o‘z vaqtida aniqlash ehtimoli yuqori bo‘ladi.

S
o
‘

[illegible]

Statistik ma’lumotlar shuni ko‘rsatadiki, moliyaviy tashkilotlar tobora ko‘proq kiberhujumlar

tashkilot miqyosida emas, balki davlat darajasida muvofiqlashtirilgan bo‘lishi zarur.

darajasiga ham bevosita bog‘liq;

D
e
m
a
k

moliya[illegible] xavfsizligini ta’minlash, zamonaviy himoya vositalarini joriy etish, xodimlar va foydalanuvchilarni kiberxavfsizlik madaniyatiga o‘rgatish dolzarb vazifalardan

Foydalanilgan adabiyotlar ro‘yxati

1. Nemadlyarov, Z., & Kashniev, D. (2024). Cybersecurity in Digital Banking: [illegible]
2. Abdullaev, A., Al-Absi, M. A., Al-Absi, A. A., Sain, M., & Lee, H. J. (2020, February). Classify and Analyze the Security Issues and Challenges in Mobile banking in Uzbekistan. In
3. https://cyberleninka.ru/article/n/kiberbezopasnost-finansovo-kreditnyh-organizatsiy-v-usloviyah-novyh-vyzovov-i-ugroz-v-tsifrovom-prostranstve/viewer
4. https://www.imf.org
5. https://www.maximizemarketresearch.com/market-report/cyber-security-in-bfsi-market-global-market/169820/?utm_source=Globenewslwire&utm_medium=PR
6. Verizon. 2024 Data Breach Investigations Report (DBIR).
7. https://www.statista.com/statistics/1460896/rate-ransomware-attacks-global/