BANKLARDA KIBERJINOYAT XAVFSIZLIGI

Jorayev Biloliddin Sherali o'g'li
Andijon mashinasozlik instituti
"Intelektual boshqaruv va kompyuter tizimlari"fa'kulteti
"*Axborot* tizimlari va texnologiyalar" yonalishi 4-kurs 89-21 guruh talabasi

Anotatsiya

Ushbu maqolada bank sohasidagi kiberjinoyatlar va ularning salbiy ta'sirlari haqida so'z yuritiladi. Bank tizimlariga qaratilgan asosiy tahdidlar va ularga qarshi samarali choralar tahlil qilinadi. Kiberxavfsizlikni ta'minlashda texnologik innovatsiyalar, mijozlar va bank xodimlarining hamkorlikdagi roli yoritiladi.

Abstract

This article discusses cybercrime in the banking sector and its negative impact. The main threats to banking systems and effective countermeasures are analyzed. The role of technological innovations, customers and bank employees in ensuring cybersecurity is highlighted

Аннотация

В данной статье рассматривается киберпреступность в банковском секторе и ее негативные последствия. Анализируются основные угрозы банковским системам и эффективные меры противодействия. Будет подчеркнута роль технологических инноваций, клиентов и сотрудников банка в обеспечении кибербезопасности.

Kalit so'zlar: Bank xavfsizligi, kiberjinoyat, fishing, malware, DDoS hujumlari, shifrlash, autentifikatsiya, xavfsizlik chorasi.

Keywords: Banking security, cybercrime, phishing, malware, DDoS attacks, encryption, authentication, security measures.

Ключевые слова: Безопасность банковских операций, киберпреступность, фишинг, вредоносное ПО, DDoS-атаки, шифрование, аутентификация, меры безопасности

Zamonaviy texnologiyalar rivoji moliyaviy tizimlarga katta qulayliklar keltirgan bo'lsa-da, ularning xavfsizligi masalasi kiberjinoyatchilarning faoliyati sababli dolzarb bo'lib qolmoqda. Ayniqsa, bank sohasida kiberjinoyatlar orqali katta moliyaviy zarar yetkazish ehtimoli mavjud. Shu bois banklar uchun kiberxavfsizlikni ta'minlash ustuvor vazifalardan biridir.

Bank tizimlarida kuzatiladigan asosiy kiberjinoyat turlaridan biri fishing hisoblanadi. Bu usulda jinoyatchilar soxta xabarlar orqali mijozlarning shaxsiy

ma’lumotlarini qo‘lga kiritishga intiladilar. Shuningdek, zararli dasturlar, masalan, malware, foydalanuvchilarning qurilmalariga o‘rnatilib, ularning bank hisoblariga noqonuniy kirish imkonini yaratadi. DDoS hujumlari esa bank tizimlarini ishdan chiqarishga qaratilgan bo‘lib, xizmatlar sifatini pasaytiradi va mijozlarning noroziligiga sabab bo‘ladi.

Bu tahdidlarga qarshi samarali kurashish uchun banklar bir qator texnologik va tashkiliy choralarni ko‘rishi lozim. Masalan, ikki faktorli autentifikatsiya va biometrik xavfsizlik tizimlarini joriy etish orqali mijozlarning hisoblarini himoya qilish mumkin. Ma’lumotlarni shifrlash texnologiyalaridan foydalanish esa mijoz va bank o‘rtasidagi aloqa xavfsizligini ta’minlaydi. Shu bilan birga, xodimlar va mijozlarni xavfsizlik qoidalari bo‘yicha muntazam o‘qitish, bank tizimlarini real vaqt rejimida monitoring qilish va shubhali faoliyatlarni aniqlash uchun zamonaviy tahlil tizimlaridan foydalanish muhim hisoblanadi.

Mijozlar ham shaxsiy ma’lumotlarini himoya qilishda mas’uliyatni unutmasliklari kerak. Noma’lum manbalardan kelgan xabarlarga ishonmaslik, kuchli va noyob parollar qo‘llash, shuningdek, rasmiy bank ilovalarini ishlatish asosiy choralar hisoblanadi. Bank tomonidan taklif qilinayotgan qo‘shimcha xavfsizlik xizmatlaridan, masalan, tranzaksiyalar bo‘yicha SMS-xabarnomalardan foydalanish ham tavsiya etiladi.

Banklarda Kiberjinoyat Xavfsizligi: Tahdidlar va Himoya Yechimlari

Kiberjinoyatlar zamonaviy dunyoda eng katta xavfsizlik muammolaridan biri hisoblanadi. Ayniqsa, moliyaviy institutlar, jumladan, banklar kiberjinoyatchilar uchun jozibador nishonga aylangan. Bu holat bank tizimlarining o‘z faoliyatini uzluksiz va xavfsiz olib borishiga tahdid soladi. Kiberjinoyatchilar turli usullar yordamida bank mijozlarining mablag‘larini o‘g‘irlash, moliyaviy tizimni izdan chiqarish va ularga ishonchni pasaytirishga harakat qilishadi. Ushbu maqolada banklar duch keladigan asosiy tahdidlar, kiberjinoyatlarga qarshi kurashish choralarining muhim jihatlari va mijozlarning roli haqida batafsil ma’lumot beriladi.

Kiberjinoyatlarning Banklarga Ta’siri

Banklar kiberhujumlarga uchraganda, bu nafaqat moliyaviy zarar keltiradi, balki tashkilotning obro‘siga putur yetkazadi. Mijozlarning bankka bo‘lgan ishonchi pasayadi, bu esa uzoq muddatli iqtisodiy oqibatlarga olib kelishi mumkin. Bundan tashqari, bank tizimlarining ishdan chiqishi boshqa sohalarga ham domino effektini keltirib chiqarishi mumkin, chunki moliyaviy tizim ko‘plab boshqa tarmoqlar bilan uzviy bog‘liqdir.

Kiberjinoyatchilar Qo‘llaydigan Asosiy Usullar

Banklarga qarshi amalga oshiriladigan kiberjinoyatlarning eng keng tarqalgan turlari quyidagilardir:

1. Fishing: Firibgarlar soxta xabarlar orqali mijozlarning login, parol yoki karta ma’lumotlarini qo‘lga kiritishga harakat qiladi. Ushbu xabarlar ko‘pincha haqiqiy bank xabarlariga o‘xshash qilib tayyorlanadi.

2. Zararli dasturlar (malware): Jinoyatchilar foydalanuvchilarning qurilmalariga maxsus dasturlarni o‘rnatib, ulardan bank ma’lumotlarini o‘g‘irlash yoki tranzaksiyalarni noqonuniy ravishda amalga oshirish uchun foydalanadilar.

3. DDoS hujumlari: Bu usulda jinoyatchilar bank tizimiga katta hajmdagi so‘rovlar yuborib, uning faoliyatini izdan chiqaradi va mijozlar uchun xizmatlarni vaqtincha cheklaydi.

4. Insider tahdidlar: Bank ichidagi xodimlar orqali maxfiy ma’lumotlarning oshkor bo‘lishi yoki ulardan noqonuniy foydalanish ham katta muammo hisoblanadi.

Kiberxavfsizlikni Ta’minlashning Muhim Jihatlari

Kiberjinoyatlarga qarshi kurashda banklar quyidagi choralarni amalga oshirishlari lozim:

1. Avtomatlashtirilgan xavfsizlik tizimlari: Banklar zamonaviy xavfsizlik tizimlarini joriy etish orqali kiberhujumlarni real vaqt rejimida aniqlash imkoniyatiga ega bo‘lishadi. Masalan, sun’iy intellekt asosida ishlaydigan tahlil tizimlari yordamida shubhali faoliyatlarni tezda aniqlash mumkin.

2. Shifrlash texnologiyalari: Ma’lumotlarni shifrlash orqali mijozlar va bank o‘rtasidagi aloqa xavfsizligini ta’minlash kiberjinoyatchilarga qarshi samarali himoya vositasidir.

3. Ikki faktorli autentifikatsiya: Bu tizimda mijozlar nafaqat login va parolni, balki qo‘shimcha xavfsizlik kodini ham kiritishlari kerak bo‘ladi. Bu hisoblarni buzish imkoniyatini kamaytiradi.

4. Xodimlarni tayyorlash: Bank xodimlari kiberxavfsizlik bo‘yicha muntazam ravishda o‘qitilishi va treninglardan o‘tishi lozim. Bu ularning tahdidlarni tezda aniqlash va oldini olish qobiliyatini oshiradi.

Mijozlarning Mas’uliyati

Bank tizimlarining xavfsizligi nafaqat banklarning, balki mijozlarning ham o‘z ma’lumotlarini himoya qilishga mas’uliyatli yondashishiga bog‘liq. Mijozlarga quyidagi tavsiyalar beriladi:

Elektron pochta yoki SMS orqali yuborilgan shubhali xabarlarga javob bermaslik.

Kuchli va noyob parollarni ishlatish, ularni muntazam ravishda yangilab turish.

Bankning rasmiy ilovalari va veb-saytlaridan foydalanish.

Shubhali faoliyatni bankka tezda xabar qilish.

Xulosa

Banklarda kiberjinoyatlarga qarshi kurash zamonaviy moliyaviy tizimlarning ajralmas qismiga aylangan. Asosiy tahdidlarga fishing, zararli dasturlar, DDoS

hujumlari va hisoblarni buzish kiradi. Ularni bartaraf etishda kuchli autentifikatsiya tizimlari, shifrlash texnologiyalari, xodim va mijozlarni o‘qitish kabi choralarning samaradorligi yuqori. Shu bilan birga, mijozlar ham o‘z shaxsiy ma’lumotlarini himoya qilishda mas’uliyatni unutmasliklari lozim. Banklar va mijozlarning birgalikdagi harakatlari kiberjinoyatlarga qarshi kurashda asosiy omil bo‘ladi.

Qisqa qilib aytadigan bo`lsak, bank tizimlari va mijozlarning xavfsizligi o‘zaro hamkorlik va zamonaviy texnologiyalardan foydalanishga bog‘liq. Har bir tomon o‘z mas’uliyatini to‘g‘ri bajarsa, kiberjinoyatlarga qarshi samarali himoya barpo etish mumkin.

Foydalanilgan adabiyotlar va manbalar

1. Cisco Talos Intelligence: “Cybersecurity in Banking and Financial Services”.
2. Kaspersky: “Top 5 Cyber Threats to Financial Institutions”.
3. Symantec: “Phishing and Malware Trends in the Financial Sector”.