BANK TIZIMLARIDA KIBERJINOYAT TAHDIDLARI: ULARNI ANIQLASH VA OLDINI OLISH STRATEGIYALARI

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 guruhtalabasi

Anotatsiya. Ushbu maqolada zamonaviy bank tizimlarida kiberjinoyatlar tahdidlari va ularni aniqlash hamda oldini olish bo'yicha samarali strategiyalar tahlil qilinadi. Banklarga qaratilgan asosiy kiberjinoyat usullari, jumladan, fishing, DDoS hujumlari, zararli dasturlar va insider tahdidlar ko'rib chiqiladi. Maqola, shuningdek, kiberjinoyatlarga qarshi sun'iy intellekt, ikki faktorli autentifikatsiya va shifrlash texnologiyalaridan foydalanish bo'yicha amaliy tavsiyalarni taqdim etadi.

Annotation. This article examines cybercrime threats in modern banking systems and provides effective strategies for detecting and preventing them. It highlights the main methods used by cybercriminals against banks, including phishing, DDoS attacks, malware, and insider threats. The article also offers practical recommendations on using artificial intelligence, two-factor authentication, and encryption technologies to combat cybercrime.

Аннотация.В статье анализируются угрозы киберпреступности в современных банковских системах и эффективные стратегии их обнаружения и предотвращения.

Рассматриваются основные методы киберпреступности, направленные против банков, включая фишинг, DDoS-атаки, вредоносное ПО и внутренние угрозы.

В статье также даны практические рекомендации по использованию искусственного интеллекта, двухфакторной аутентификации и технологий шифрования для борьбы с киберпреступностью.

Kalit so'zlar: Bank xavfsizligi Kiberjzioyatlar Fishing

DDoS hujumlari, Zararli dasturlar, Sun'iy intellect, Ikki faktorli autentifikatsiya, Shifrlash texnologiyalari, Xavfsizlik strategiyalari

Keywords: Banking Security Cybersecurity Phishing DDoS attacks, Malware, Artificial intelligence, Two-factor authentication, Encryption technologies, Security strategies

Ключевые слова: Банковская безопасность Киберпреступность Фишинг

DDoS-атаки, Вредоносное ПО, Искусственный интеллект, Двухфакторная аутентификация, Технологии шифрования, Стратегии безопасности

Zamonaviy bank tizimlari kiberjinoyatchilar uchun eng asosiy nishonlardan biri hisoblanadi. Moliyaviy ma’lumotlarning yuqori qiymati va mijozlar hisoblari bilan bog‘liq katta miqdordagi mablag‘ kiberjinoyatchilarni jalb qiladi. Kiberjinoyatlar bank tizimlariga nafaqat moliyaviy zarar, balki ishonchni yo‘qotish va obro‘sizlanish kabi jiddiy oqibatlarni keltirib chiqaradi. Ushbu maqolada banklarga qaratilgan asosiy kiberjinoyat tahdidlari va ularni aniqlash hamda oldini olish strategiyalari haqida so‘z boradi.

Banklarga Qaratilgan Asosiy Kiberjinoyat Tahdidlari

1. Fishing (Firibgarlik xabarlari):

Kiberjinoyatchilar elektron pochta, SMS yoki ijtimoiy tarmoqlar orqali mijozlarga soxta xabarlar yuborib, ulardan maxfiy ma’lumotlarni olishga urinadilar. Ushbu xabarlar ko‘pincha rasmiy bank xabarlariga o‘xshash qilib tayyorlanadi. Firibgarlik xabarlaridan zarar ko‘rgan mijozlar o‘z hisob ma’lumotlarini jinoyatchilarga berib qo‘yishi mumkin.

2. DDoS Hujumlari (Distributed Denial of Service):

Bu usulda kiberjinoyatchilar bank serverlariga katta hajmdagi so‘rovlar yuborib, tizimni ishdan chiqaradi. Bu holat mijozlarga xizmat ko‘rsatishni vaqtincha to‘xtatadi va bankning obro‘siga putur yetkazadi.

3. Zararli Dasturlar (Malware):

Jinoyatchilar mijozlarning kompyuterlari yoki mobil qurilmalariga zararli dasturlarni o‘rnatib, ulardan moliyaviy ma’lumotlarni o‘g‘irlaydi. Bunga trojan dasturlari, keyloggerlar va shifrlash dasturlari kiradi.

4. Insider Tahdidlar:

Ba’zi hollarda bank ichidagi xodimlar tomonidan ma’lumotlar noqonuniy ravishda oshkor qilinishi yoki ulardan foydalanilishi mumkin. Bu, odatda, ichki xavfsizlik tizimlarining zaifligi sabab yuzaga keladi.

5. Moliyaviy Firibgarlik:

Kiberjinoyatchilar o‘yinchilarni aldash orqali bankning moliyaviy tizimlaridan foyda olishga harakat qilishadi. Masalan, noqonuniy tranzaksiyalarni amalga oshirish yoki kredit hisoblarini buzish kabi harakatlar.

Kiberjinoyatlarni Aniqlash Strategiyalari

1. Sun’iy Intellekt va Tahlil Tizimlari:

Bank tizimlarida sun’iy intellekt asosida ishlaydigan xavfsizlik vositalarini joriy etish kiberhujumlarni tez aniqlashga yordam beradi. Ushbu tizimlar tranzaksiyalarni kuzatib, g‘ayrioddiy faoliyatni avtomatik aniqlaydi.

2. Real Vaqtda Monitoring:

Bank tizimlarini 24/7 monitoring qilish va har qanday shubhali faoliyatni darhol aniqlash uchun avtomatlashtirilgan tizimlardan foydalanish muhimdir.

3. Xodimlarni Tayyorlash:

Bank xodimlarini kiberxavfsizlik bo‘yicha muntazam treninglardan o‘tkazish orqali ularning tahdidlarni tez aniqlash qobiliyatini oshirish mumkin.

4. Mijozlarni Xabardor Qilish:

Bank mijozlariga phishing hujumlari, zararli dasturlar va boshqa kiberjinoyat usullari haqida muntazam ma’lumot berish, ularni ehtiyot choralarini ko‘rishga undaydi.

Kiberjinoyatlarga Qarshi Oldini Olish Choralari

1. Kuchli Shifrlash Texnologiyalari:

Bank va mijozlar o‘rtasidagi barcha tranzaksiyalar shifrlangan bo‘lishi kerak. Bu ma’lumotlarni jinoyatchilardan himoya qiladi.

2. Ikki Faktorli Autentifikatsiya:

Ikki faktorli autentifikatsiya (2FA) mijozlarning hisoblarini buzish ehtimolini kamaytiradi. Bu tizim foydalanuvchi login va parolidan tashqari, qo‘shimcha xavfsizlik kodini kiritishni talab qiladi.

3. Zaxira Nusxalar Yaratish:

Bank tizimlarining muntazam zaxira nusxalarini yaratish va ularni alohida joyda saqlash orqali kiberhujum oqibatida yo‘qolgan ma’lumotlarni tiklash mumkin.

4. Xavfsizlik Auditlari:

Bank tizimlarining xavfsizlik zaifliklarini aniqlash uchun muntazam auditlar o‘tkazish zarur. Bu kelgusidagi tahdidlarning oldini olishga yordam beradi.

Xulosa

Bank tizimlarida kiberjinoyatlarga qarshi kurash nafaqat moliyaviy xavfsizlikni ta’minlash, balki mijozlarning bankka bo‘lgan ishonchini saqlab qolish uchun ham muhimdir. Kiberjinoyatchilar tobora rivojlanayotgan tahdidlar bilan bank tizimlarini nishonga olmoqda.

Shuning uchun zamonaviy texnologiyalarni joriy etish, muntazam monitoring qilish va xodim hamda mijozlarni o‘qitish orqali bu tahdidlarga qarshi kurashish mumkin. Banklar va mijozlarning birgalikdagi harakatlari moliyaviy tizimning mustahkamligi va xavfsizligini ta’minlaydi.

Foydalanilgan adabiyotlar

1. Cisco Talos Intelligence."Cybersecurity in Banking and Financial Services." Bank sektoridagi kiberxavfsizlik muammolari va ularni bartaraf etish strategiyalari.
2. Kaspersky Lab."Top 5 Cyber Threats to Financial Institutions." Banklarga nisbatan keng tarqalgan kiberjinoyatlar va ularni oldini olish choralari.
3. Symantec Corporation. "Phishing and Malware Trends in the Financial Sector." Moliyaviy tizimlarga qaratilgan fishing va zararli dasturlar haqida tahliliy ma’lumot.
4. IBM Security Services. "Cybersecurity for Financial Institutions." IBM tomonidan bank tizimlari uchun xavfsizlik yechimlariga bag‘ishlangan tahlil.

5. Norton Security Insights. "The Rise of Cybercrime in Banking: Trends and Solutions." Kiberjinoyatlarning bank tizimlariga ta’siri va samarali yechimlar haqida hisobot.
6. IT Governance Blog. "How to Improve Cybersecurity in Banking." Bank tizimlari uchun kiberxavfsizlikni kuchaytirish usullari.