ZAMONAVIY KIBERXAVFSIZLIK TAHDIDLARI VA HIMOYA USULLARI

Nusratillayev Madamin O‘ktam o‘g‘li, Razzoqov Ilhom Dovranovich
Qarshi davlat universiteti
nusratillayevmadamin@gmail.com
razzokov.id@qarshidu.uz

Annotatsiya. Ushbu tezisda zamonaviy kiberxavfsizlik tahdidlari — *fishing, ransomware, DDoS hujumlari, ijtimoiy muhandislik, identifikatsiya ma'lumotlarini o‘g‘irlash va dasturiy zaifliklar — hamda ularga qarshi qo‘llaniladigan asosiy himoya vositalari (sun’iy intellekt/mashinaviy o‘rganish, Zero Trust, ko‘p bosqichli autentifikatsiya, SIEM/SOC, EDR/XDR) qisqacha tahlil qilingan. Tadqiqot ilmiy manbalar va xalqaro standartlarga (ENISA, NIST, OWASP) asoslangan bo‘lib, natijalar zamonaviy kiberhimoya faqat bitta vosita bilan emas, balki texnik yechimlar, xavfsizlik siyosati va xodimlar malakasini birlashtiruvchi ko‘p qatlamli yondashuv orqali ta’minlanishi lozimligini ko‘rsatadi.*

Kalit so‘zlar: *kiberxavfsizlik, fishing, ransomware, DDoS, ijtimoiy muhandislik, Zero Trust, sun’iy intellekt, SIEM/SOC, EDR/XDR, MFA.*

Raqamli texnologiyalarning jadal rivojlanishi natijasida axborot tizimlari davlat boshqaruvi, bank-moliya, ta’lim va sog‘liqni saqlash kabi sohalarning ajralmas qismiga aylandi. Tashkilotlar faoliyati kompyuter tarmoqlari, bulutli xizmatlar va raqamli ma’lumotlarga tobora ko‘proq bog‘liq bo‘lib bormoqda, bu esa axborot resurslarini himoya qilish masalasini yanada dolzarb qilmoqda. ENISA tahdidlar landshafti tahlilida xizmatlarning mavjudligiga qarshi hujumlar va ma’lumotlarga nisbatan tahdidlar so‘nggi yillardagi eng dolzarb tahdid turlari sifatida qayd etilgan [1]. Zamonaviy kiberhujumlar ko‘p bosqichli va moslashuvchan xarakterga ega: hujumchi dastlab fishing orqali hisob ma’lumotlarini qo‘lga kiritishi, so‘ngra tizimga kirib imtiyozlarini oshirishi

mumkin. Tezisning maqsadi - zamonaviy kiberxavfsizlik tahdidlarini tahlil qilish va ularga qarshi qo‘llanilayotgan himoya usullarini umumlashtirishdan iborat.

Tadqiqot ko‘rib chiqish xarakteriga ega bo‘lib, xalqaro tashkilotlarning hisobotlari va xavfsizlik standartlari (ENISA, NIST, OWASP) tahlil qilindi. Manbalar tahdidning dolzarbligi, hujum mexanizmi, potensial zarar, aniqlash murakkabligi va mavjud himoya usullari mezonlari asosida ko‘rib chiqildi. NIST AI Risk Management Framework sun’iy intellekt tizimlaridan foydalanish jarayonidagi xavflarni boshqarish masalalariga bag‘ishlangan [2]. NIST SP 800-207 standartida Zero Trust modeli foydalanuvchi yoki qurilmaning tarmoqdagi joylashuvidan qat’iy nazar ularga ishonmaslik tamoyiliga asoslanishi ko‘rsatilgan [3]. OWASP Top 10 ro‘yxatida esa Broken Access Control, Cryptographic Failures va Injection kabi zaifliklar veb-ilovalar uchun eng xavfli tahdidlar sifatida keltirilgan [4].

Fishing - foydalanuvchini aldab, uning maxfiy ma’lumotlarini qo‘lga kiritishga qaratilgan hujum bo‘lib, sun’iy intellekt yordamida yaratilgan shaxsiylashtirilgan xabarlarni aniqlashni yanada qiyinlashtirmoqda; himoya vositasi sifatida MFA va elektron pochta filtrlari muhim ahamiyat kasb etadi. Ransomware ma’lumotlarni shifrlab, tiklash evaziga to‘lov talab qiluvchi zararli dastur bo‘lib, zamonaviy hujumlarda ma’lumotlarni o‘g‘irlash orqali “double extortion” usuli ham qo‘llanilmoqda; asosiy himoya choralariga zaxira nusxalash, tizimlarni yangilash

va EDR/XDR vositalari kiradi. DDoS hujumlari IoT qurilmalaridan tashkil topgan botnetlarning kengayishi hisobiga tobora kuchayib bormoqda, shuning uchun bunday tahdidlarga qarshi tarmoq trafigini filtrlash, so‘rovlar sonini cheklash (rate limiting) hamda CDN texnologiyalaridan foydalanish orqali xizmatlarning uzluksiz va barqaror ishlashini ta’minlash mumkin. Ijtimoiy muhandislik inson psixologiyasidagi zaif jihatlardan foydalanadi, shu sababli xodimlarni muntazam o‘qitish zarur. Himoya texnologiyalari orasida Zero Trust arxitekturasi (“ishonchni avtomatik bermaslik” tamoyili), ko‘p bosqichli autentifikatsiya, SIEM/SOC (hodisalarni monitoring va tahlil qilish) hamda EDR/XDR (endpoint va tarmoq

darajasida aniqlash) alohida o‘rin tutadi. Sun’iy intellekt tahdidlarni erta aniqlashda samarali bo‘lsada, false positive va adversarial hujumlar kabi cheklovlarga ega bo‘lgani bois inson mutaxassislarini to‘liq almashtira olmaydi [2].

Tahlil natijasida quyidagi tendensiyalar aniqlandi: birinchidan, kiberhujumlar tobora ko‘p bosqichli xarakter kasb etmoqda; ikkinchidan, inson omili kiberxavfsizlikning eng zaif nuqtalaridan biri bo‘lib qolmoqda; uchinchidan, sun’iy intellekt himoya va hujum maqsadida bir vaqtda qo‘llanilishi mumkin bo‘lgan dual-use texnologiya hisoblanadi; to‘rtinchidan, samarali himoya bitta vositaga emas, balki ko‘p qatlamli (defense in depth) modelga asoslanishi lozim. Shu asosda quyidagi umumlashtirilgan zanjir taklif etiladi:

Foydalanuvchi xavfsizligi → MFA → Zero Trust → Firewall/IDS/IPS → EDR/XDR → SIEM/SOC → Incident Response → Backup va Recovery.

Bunday yondashuvda bitta qatlam buzilgan taqdirda ham qolgan qatlamlar hujum oqibatlarini minimallashtiradi.

Tadqiqot natijalariga ko‘ra, fishing, ransomware, DDoS, ijtimoiy muhandislik va identifikatsiya ma’lumotlarini o‘g‘irlash tashkilotlar uchun eng dolzarb kiberxavflar hisoblanadi. Ularga samarali qarshi turish uchun MFA, Zero Trust, SIEM/SOC, EDR/XDR, ma’lumotlarni muntazam zaxiralash va xodimlarni o‘qitish choralarini kompleks tarzda qo‘llash maqsadga muvofiqdir.

ADABIYOTLAR RO‘YXATI

1. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. ENISA, 2024.

2. Tabassi, E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. National Institute of Standards and Technology, 2023.

3. Rose, S., Borchert, O., Mitchell, S., Connelly, S. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology, 2020.

4. OWASP Foundation. OWASP Top 10:2021. Open Web Application Security Project, 2021.