O‘RTA OSIYODA IJTIMOIY VA GUMANITAR TADQIQOTLAR-Jurnali
1-son. 3-qism. Noyabr-2025

KIBERHUJUMLAR TURLARI VA ULARNING OLDINI OLISH STRATEGIYALARI

Qurbonaliyev G’olibjon Alisher o’g’li
Ichki Ishlar Vazirligi Akademiyasi

Annotatsiya: Ushbu maqolada kiberhujumlarning asosiy turlari va ularga qarshi samarali oldini olish strategiyalari tahlil qilinadi. Kiberxavfsizlik sohasidagi dolzarb muammo sifatida kiberhujumlar korxonalar, davlat tashkilotlari va individual foydalanuvchilarga katta zarar yetkazmoqda. Maqolada phishing, DDoS hujumlari, ransomware, malware va boshqa keng tarqalgan kiberhujum turlari batafsil ko‘rib chiqiladi. Shuningdek, kiberhujumlarga qarshi kurashda qo‘llaniladigan texnologik, tashkiliy va huquqiy chora-tadbirlar, jumladan, xavfsizlik devorlari (firewall), antivirus dasturlari, xodimlarni o‘qitish va axborot xavfsizligini boshqarish tizimlari muhokama qilinadi. Maqola zamonaviy kiberxavfsizlik strategiyalarining samaradorligini oshirishga yo‘naltirilgan tavsiyalarni ham o‘z ichiga oladi.

Kalit so‘zlar: Kiberhujumlar, kiberxavfsizlik, phishing, ransomware, DDoS, antivirus, firewall, axborot xavfsizligi, xavfsizlik siyosati, oldini olish strategiyalari.

Axborot texnologiyalari va internetning rivojlanishi insoniyat hayotining barcha jabhalariga chuqur ta’sir ko‘rsatdi. Biroq, raqamli infrastrukturadagi o‘sish bilan birga, kiberxavfsizlik sohasidagi tahdidlar ham keskin oshib bordi. Bugungi kunda kiberhujumlar nafaqat yirik kompaniyalar va davlat tashkilotlariga, balki kichik bizneslar va oddiy foydalanuvchilarga ham jiddiy xavf tug‘dirmoqda. Kiberhujumlar turli shakllarda namoyon bo‘lib, ular ma’lumotlarning o‘g‘irlanishi, tizimlarning ishdan chiqishi yoki moliyaviy zarar yetkazilishiga olib keladi.

Kiberhujumlarga qarshi kurashish va ularning oldini olish uchun samarali strategiyalarni ishlab chiqish zamonaviy kiberxavfsizlik tizimlarining asosiy vazifalaridan biridir. Ushbu maqolada kiberhujumlarning asosiy turlari – phishing, ransomware, DDoS (Distributed Denial of Service), malware va boshqalar, ularning xususiyatlari hamda ushbu tahdidlarga qarshi qo‘llaniladigan texnologik va tashkiliy chora-tadbirlar tahlil qilinadi. Shuningdek, kiberxavfsizlik sohasidagi zamonaviy yondashuvlar va ilg‘or texnologiyalar, xususan, sun’iy intellekt, mashinani o‘rganish hamda avtomatlashtirilgan xavfsizlik tizimlarining roli haqida ham fikr yuritiladi.

Axborot resurslarini himoya qilish samaradorligini oshirish uchun, tashkilotlar xavfsizlik siyosatini ishlab chiqishi, xodimlarni muntazam o‘qitishi va yangi tahdidlarga qarshi doimiy monitoring tizimini yo‘lga qo‘yishi lozim. Ushbu maqola kiberhujumlar va ularning oldini olish strategiyalariga oid keng qamrovli bilimlar bazasini taqdim etib, amaliyotda qo‘llanilishi mumkin bo‘lgan yechimlarni taklif etadi.

Kiberhujumlar zamonaviy raqamli dunyoning eng katta xavf-xatarlaridan biri hisoblanadi. Internet tarmog‘i va axborot tizimlari kengayishi bilan birga, kiberxavfsizlik sohasidagi tahdidlar ham yanada murakkablashib, ko‘lam jihatidan kengaymoqda. Kiberhujumlarning ko‘plab turlari mavjud bo‘lib, har biri o‘ziga xos usullar va maqsadlarga ega. Ularning eng ko‘p tarqalganlari sifatida phishing, ransomware, Distributed Denial of Service (DDoS), malware, va man-in-the-middle hujumlari ajralib turadi.

Phishing — bu ijtimoiy muhandislik usuliga asoslangan hujum bo‘lib, unda hujumchi soxta elektron pochta xabarlari, veb-saytlar yoki boshqa kommunikatsiya kanallari orqali foydalanuvchilarni aldashga harakat qiladi. Maqsad — foydalanuvchining shaxsiy ma’lumotlarini, jumladan login, parol yoki bank kartasi ma’lumotlarini qo‘lga kiritishdir. Phishing hujumlari odamlarning ishonchini suiiste’mol qilib, ko‘pincha korxonalar va banklar nomidan yuboriladi. Ushbu turdagi kiberhujumlarga qarshi samarali choralar sifatida foydalanuvchilarni muntazam ravishda xabardor qilish, ikki faktorli autentifikatsiya tizimini joriy etish va elektron pochta filtrlash tizimlaridan foydalanish tavsiya etiladi.

Ransomware — bu kompyuter yoki tarmoq tizimlarini bloklab, ularni ochish uchun foydalanuvchidan tovon puli talab qiluvchi zararli dasturlar toifasiga kiradi. Ransomware hujumlari ko‘pincha elektron pochta orqali yuborilgan zararli fayllar yoki zararli dasturlar o‘rnatilgan veb-saytlar orqali tarqaladi. Ushbu hujumlar natijasida korxona yoki tashkilot muhim ma’lumotlarga kira olmasligi, ish faoliyati to‘xtashi yoki moliyaviy yo‘qotishlarga duchor bo‘lishi mumkin. Oldini olish uchun muntazam zaxira nusxalarini yaratish, xavfsizlik dasturlarini yangilab borish va xodimlarni ransomware tahdidlariga qarshi o‘qitish muhim ahamiyatga ega.

Distributed Denial of Service (DDoS) hujumi — bu ma’lum bir xizmat yoki veb-saytga ko‘p miqdorda so‘rov yuborish orqali uni ishlamay qolishiga olib keladigan hujum turidir. Bu hujumlar ko‘pincha botnetlar yordamida amalga oshiriladi, ya’ni zararlangan qurilmalar tarmog‘i (botnet) bitta maqsadga qarata ko‘p sonli so‘rovlarni yuboradi. DDoS hujumlari natijasida korxonalar o‘z mijozlariga xizmat ko‘rsata olmay qoladi, bu esa moliyaviy zarar va obro‘ga putur yetkazadi. Ushbu turdagi hujumlarga qarshi kurashda tarmoqlarni monitoring qilish, trafikni filtrlash, va DDoS hujumlarini aniqlash hamda bartaraf etish uchun maxsus xizmatlardan foydalanish muhim.

Malware — zararli dasturlar umumiy nomi bo‘lib, ularning tarkibiga viruslar, trojanlar, spyware va boshqa zararli kodlar kiradi. Malware foydalanuvchi qurilmasiga yoki tarmoqka zarar yetkazish, ma’lumotlarni o‘g‘irlash yoki tizim ish faoliyatini buzish maqsadida yaratiladi. Ushbu dasturlar ko‘pincha zararli veb-saytlar, elektron pochta ilovalaridagi qo‘shimchalar yoki noqonuniy dasturlar orqali tarqaladi. Malwarega qarshi samarali himoya qilish uchun antivirus dasturlarini muntazam

yangilash, ruxsatsiz dasturlarni o‘rnatmaslik, va xavfsizlik siyosatiga qat’iy rioya qilish zarur.

Man-in-the-middle (MitM) hujumi — bu ikki tomonlama muloqot jarayoniga hujumchi aralashib, ma’lumotlarni o‘g‘irlash yoki o‘zgartirishga urinishidir. Masalan, hujumchi foydalanuvchi va server o‘rtasidagi trafikni tutib olib, ma’lumotlarni manipulyatsiya qilishi mumkin. Ushbu turdagi hujumlarning oldini olish uchun shifrlash texnologiyalari (masalan, TLS/SSL), xavfsiz Wi-Fi tarmoqlaridan foydalanish va VPN xizmatlarini qo‘llash tavsiya etiladi.

Kiberhujumlarga qarshi samarali strategiyalar texnologik, tashkiliy va huquqiy chora-tadbirlardan iborat. Texnologik choralar qatoriga xavfsizlik devorlari (firewall), antivirus va anti-malware dasturlari, shifrlash texnologiyalari, tarmoq monitoringi va hujumlarni aniqlash tizimlari kiradi. Ushbu vositalar tarmoq va tizimlarni himoya qilishda asosiy rol o‘ynaydi.

Tashkiliy choralar esa kompaniya yoki tashkilot ichida xavfsizlik siyosatini ishlab chiqish va uni qat’iy amalga oshirishni o‘z ichiga oladi. Bu jarayonda xodimlarni kiberxavfsizlik bo‘yicha muntazam o‘qitish, xavfsizlik bo‘yicha ichki nazorat tizimlarini yo‘lga qo‘yish muhimdir. Chunki ko‘plab kiberhujumlar inson omili sababli sodir bo‘ladi, masalan, xodimlarning zaif parollarni qo‘llashi yoki phishing xabarlariga ishonib qolishi.

Huquqiy choralar kiberhujumlarga qarshi kurashda davlat va xalqaro darajada qonunchilik va tartibga solish faoliyatini anglatadi. Kiberjinoiylikka qarshi qonunlar, maxfiylikni himoya qilish tartiblari, va kiberxavfsizlik standartlari ishlab chiqilishi va qat’iy qo‘llanilishi zarur. Shu bilan birga, xalqaro hamkorlik kiberxavfsizlikni ta’minlashda muhim ahamiyatga ega, chunki kiberhujumlar ko‘pincha chet elda joylashgan hujumchilar tomonidan amalga oshiriladi.

Zamonaviy texnologiyalar, xususan, sun’iy intellekt va mashinani o‘rganish, kiberxavfsizlik sohasida yangi imkoniyatlar yaratmoqda. Ushbu texnologiyalar yordamida kiberxavflarni oldindan aniqlash, hujumlarni avtomatik tarzda aniqlash va ularga qarshi tezkor javob berish tizimlari ishlab chiqilmoqda. Biroq, texnologik yangiliklar bilan bir qatorda, hujumchilarning ham uslublari doimiy rivojlanib bormoqda, shuning uchun xavfsizlik tizimlari ham doimiy yangilanib borishi kerak.

Xulosa qilib aytganda, kiberhujumlar va ularning oldini olish strategiyalari doimiy o‘zgarib turuvchi va murakkab soha hisoblanadi. Har bir tashkilot va foydalanuvchi o‘z tizimlarini himoya qilish uchun zamonaviy texnologiyalar va samarali tashkiliy choralarni birlashtirgan kompleks yondashuvni qo‘llashi zarur. Faqat shunday holatda raqamli dunyodagi tahdidlarga samarali javob qaytarish mumkin bo‘ladi.

Foydalanilgan adabiyotlar

1. Andress, J. (2014). *The Basics of Hacking and Penetration Testing*. Elsevier.
2. Amoroso, E. G. (2019). *Cyber Attacks: Protecting National Infrastructure*. Butterworth-Heinemann.
3. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press.
4. Stallings, W. (2017). *Network Security Essentials: Applications and Standards*. Pearson.
5. Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company.
6. Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94.
7. Symantec Corporation. (2022). *Internet Security Threat Report*.
8. Kaspersky Lab. (2023). *IT Threat Evolution Q1 2023*.
9. Rouse, M. (2020). *What is Phishing?* TechTarget. [Online] Available at: https://searchsecurity.techtarget.com/definition/phishing
10. Mitnick, K., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley.
11. National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1.
12. Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). *Investments in Information Security: A Real Options Perspective*. Journal of Cybersecurity, 3(2), 78-89.
13. Whitman, M., & Mattord, H. (2017). *Principles of Information Security*. Cengage Learning.
14. Kshetri, N. (2017). *Cybersecurity Strategies for Business*. IT Professional, 19(2), 20-27.
15. FireEye. (2023). *M-Trends Report: Cybersecurity Threats and Trends*.