UDK 004.056

KIBERXAVFSIZLIKDA TAHDIDLAR VA HIMOYA USULLARI

Xaydarov K.S., *PhD,*
E-mail:kamoliddin1506@gmail.com
Namangan davlat texnika universiteti

Annotatsiya: Ushbu maqolada kiberxavfsizlik sohasidagi asosiy tahdidlar va ularni bartaraf etishning zamonaviy usullari tahlil qilinadi. Shuningdek, axborot tizimlari va tarmoqlarni himoyalashning samarali mexanizmlari ko‘rib chiqiladi.

Аннотация: В данной статье анализируются основные угрозы в сфере кибербезопасности и современные методы их предотвращения. Также рассматриваются эффективные механизмы защиты информационных систем и компьютерных сетей.

Abstract: This article analyzes the main threats in the field of cybersecurity and modern methods of their prevention. In addition, effective mechanisms for protecting information systems and computer networks are considered.

Kalit so‘zlar: kiberxavfsizlik, zararli dasturlar, phishing, shifrlash, firewall, autentifikatsiya.

Ключевые слова: кибербезопасность, вредоносные программы, фишинг, шифрование, межсетевой экран (firewall), аутентификация.

Keywords: cybersecurity, malware, phishing, encryption, firewall, authentication.

So‘nggi yillarda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha sohalariga chuqur kirib bordi. Davlat boshqaruvi, bank-moliya tizimi, ta’lim, sog‘liqni saqlash, sanoat va transport sohalarida raqamli texnologiyalardan keng foydalanilmoqda. Raqamlashtirish jarayoni samaradorlikni oshirish va xizmatlar sifatini yaxshilash imkonini bersada, u bilan birga kiberxavfsizlik bilan bog‘liq yangi tahdidlarni ham yuzaga keltirmoqda.

O‘zbekiston Respublikasida kiberxavfsizlik masalalariga davlat siyosati darajasida alohida e’tibor qaratilmoqda. Jumladan, O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF–6079-son Farmoni bilan tasdiqlangan “Raqamli O‘zbekiston – 2030” strategiyasida axborot xavfsizligini ta’minlash, kiberxavfsizlik tizimini rivojlantirish va zamonaviy himoya mexanizmlarini joriy etish ustuvor vazifalar sifatida belgilangan [1].

Shuningdek, O‘zbekiston Respublikasi Prezidentining 2021-yil 26-martdagi PQ–5053-son Qarorida axborot xavfsizligini mustahkamlash, davlat organlari va muhim infratuzilma obyektlarining kiberhimoyasini kuchaytirish, malakali mutaxassislar tayyorlash masalalariga alohida urg‘u berilgan. Mazkur hujjatlar mamlakatda kiberxavfsizlikni ta’minlashning huquqiy va tashkiliy asoslarini yaratishda muhim ahamiyat kasb etadi [2]..

Bugungi kunda axborot resurslari strategik ahamiyatga ega bo‘lib, ularni himoyalash davlat va jamiyat xavfsizligining muhim omillaridan biri hisoblanadi. Internet tarmoqlarining kengayishi, bulutli texnologiyalar, mobil qurilmalar va IoT tizimlarining ommalashuvi kiberhujumlar uchun yangi imkoniyatlar yaratmoqda. Natijada zararli dasturlar, phishing hujumlari, tarmoq hujumlari, ma’lumotlarni o‘g‘irlash va tizimlarni ishdan chiqarishga qaratilgan kiberjinoyatlar soni ortib bormoqda.

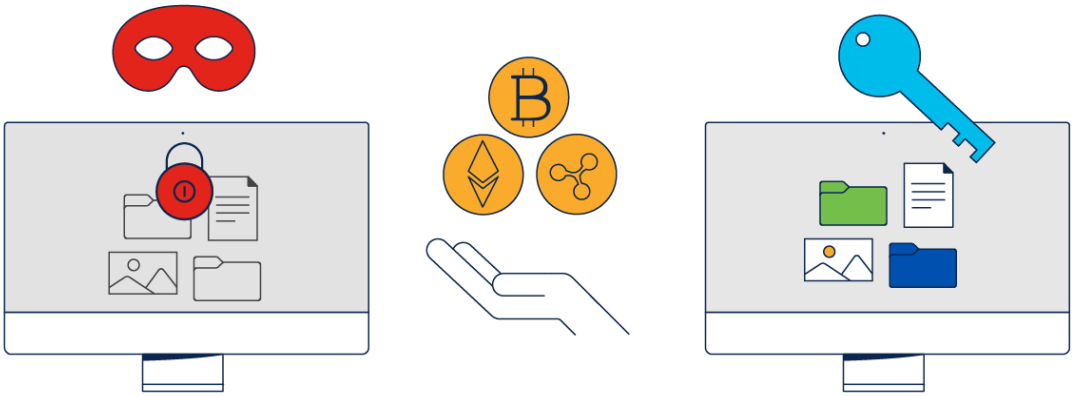
Kiberxavfsizlik nafaqat texnik masala, balki tashkiliy, huquqiy va ijtimoiy jihatlarni ham qamrab oluvchi kompleks muammo hisoblanadi. Axborot tizimlarining zaifligi moddiy zarar, maxfiy ma’lumotlarning yo‘qolishi va tashkilotlar obro‘siga putur yetkazishi mumkin. Shu sababli, zamonaviy sharoitda kiberxavfsizlikni ta’minlash har bir davlat, tashkilot va foydalanuvchi uchun muhim vazifaga aylangan.

Kiberxavfsizlikning asosiy maqsadi axborotning maxfiyligi, yaxlitligi va mavjudligini ta’minlashdan iboratdir. Ushbu tamoyillar axborot xavfsizligi tizimining poydevorini tashkil etadi.

Mazkur maqolada kiberxavfsizlik sohasidagi asosiy tahdidlar va ularni bartaraf etishning samarali usullari tahlil qilinadi [3-4].

Kiberxavfsizlik tahdidlari — axborot tizimlari, kompyuter tarmoqlari va ma'lumotlarga ruxsatsiz kirish, ularni buzish, o'g'irlash yoki yo'q qilishga qaratilgan harakatlar majmuasidir. Zamonaviy axborot jamiyatida raqamli texnologiyalarning keng qo'llanilishi bilan bir qatorda kiber tahdidlar ko'lami ham kengayib, ularning murakkabligi ortib bormoqda. Ushbu tahdidlar nafaqat texnik muammolarni, balki iqtisodiy, ijtimoiy va huquqiy oqibatlarni ham keltirib chiqaradi.

Eng keng tarqalgan kiber tahdidlardan biri zararli dasturlardir. Zararli dasturlar foydalanuvchi kompyuteri yoki tarmog'iga yashirin ravishda kirib, tizim faoliyatiga zarar yetkazadigan dasturlardir. Ular ko'pincha internet orqali yuklab olingan noma'lum fayllar yoki zararli havolalar orqali tarqaladi. Viruslar fayllarni buzadi, troyan dasturlari foydali dastur ko'rinishida yashirinadi, ransomware ma'lumotlarni shifrlab to'lov talab qiladi, spyware esa foydalanuvchini kuzatadi.



1-rasm. Zararli dasturlar (Malware)

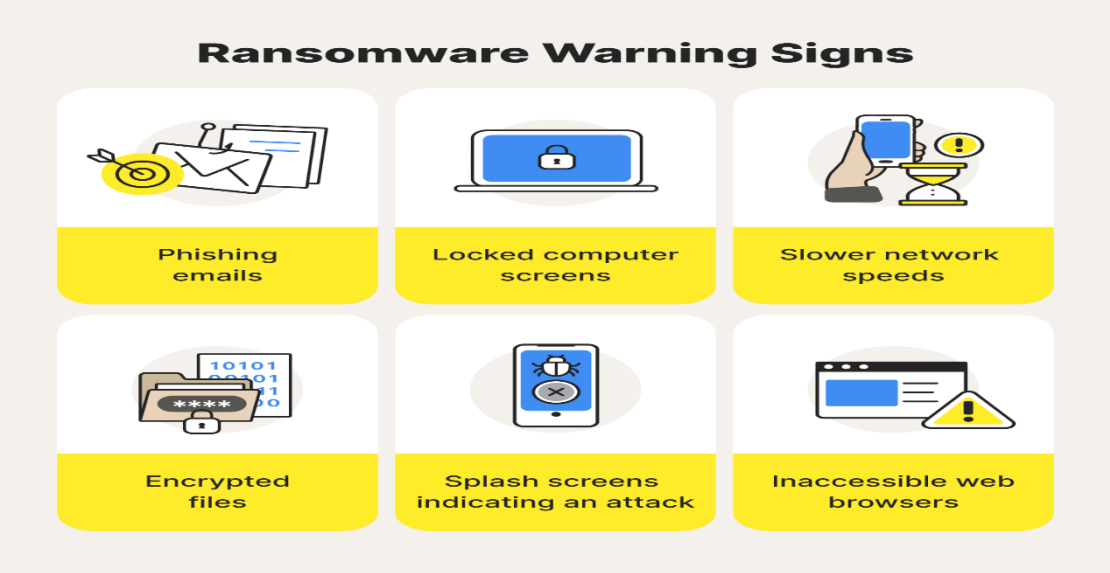
Tarmoq hujumlari ham kiber tahdidlarning muhim yo'nalishlaridan biridir. Bunday hujumlar orqali hakerlar kompyuter tarmoqlariga ta'sir ko'rsatib, ularning ishlashini izdan chiqarishga harakat qiladi. DDoS hujumlari, "odam o'rtada" (Man-in-the-Middle) usuli, parollarni tanlashga asoslangan brute force hujumlari hamda veb-ilovalarga qarshi SQL injection hujumlari tarmoq tahdidlariga misol bo'la oladi. Ushbu hujumlar natijasida serverlar faoliyati to'xtashi, ma'lumotlar buzilishi yoki tizimlarga ruxsatsiz kirish holatlari yuzaga keladi.

Ichki tahdidlar ham kiberxavfsizlik uchun jiddiy xavf tug'diradi. Ular tashkilot ichidagi xodimlarning ehtiyotsizligi, malakasizligi yoki qasddan amalga oshirilgan harakatlari natijasida yuzaga keladi. Masalan, zaif parollardan foydalanish, maxfiy ma'lumotlarni himoyasiz saqlash yoki noto'g'ri tizim sozlamalari ichki tahdidlarning asosiy sabablaridan hisoblanadi.

Bundan tashqari, ijtimoiy muhandislik usullari orqali amalga oshiriladigan hujumlar ham tobora keng tarqalmoqda. Ushbu usulda hujumchilar inson psixologiyasidan foydalanib, foydalanuvchilardan maxfiy ma'lumotlarni olishga harakat qiladi. Telefon orqali aldash, soxta texnik yordam xizmatlari yoki ishonchli shaxs sifatida murojaat qilish kabi usullar bunga misol bo'la oladi.

Phishing — foydalanuvchini aldash orqali maxfiy ma'lumotlarni qo'lga kiritishga qaratilgan kiberhujum turidir. Bunda hujumchilar soxta elektron pochta xabarlari, yolg'on veb-

saytlar yoki ijtimoiy tarmoqlardagi soxta sahifalardan foydalanadi. Foydalanuvchi ishonib login va parolini kiritganda, ma’lumot hujumchiga uzatiladi.



2-rasm. Phishing hujumi namunasi.

Tarmoq hujumlari kompyuter tarmoqlari orqali amalga oshiriladi. DDoS hujumlari serverga juda ko‘p so‘rov yuborib uni ishdan chiqaradi, Man-in-the-Middle hujumida esa ma’lumot uzatish jarayoni yashirin kuzatiladi. Brute Force usulida parollar avtomatik tanlanadi, SQL Injection orqali esa ma’lumotlar bazasiga zarar yetkaziladi [5].



3-rasm. Tarmoq hujumi (DDoS) tasviri

Ichki tahdidlar tashkilot ichidagi xodimlar yoki foydalanuvchilar tomonidan yuzaga keladi. Bunga ehtiyotsizlik, zaif parollardan foydalanish, ma’lumotlarni himoyasiz saqlash yoki ruxsatsiz tashqi qurilmalardan foydalanish sabab bo‘lishi mumkin. Ko‘plab axborot xavfsizligi hodisalari inson omili bilan bog‘liq ekanligi kuzatilgan.



4-rasm. Ichki tahdidlar modeli

Ijtimoiy muhandislik — inson psixologiyasidan foydalanib, ma’lumotlarni qo‘lga kiritish usulidir. Hujumchilar o‘zini texnik yordam xodimi yoki tashkilot vakili sifatida tanishtirib, foydalanuvchidan parol yoki maxfiy ma’lumotlarni so‘raydi. Bu turdagi hujumlarda texnik vositadan ko‘ra insonning ishonuvchanligi asosiy nison bo‘ladi.

Texnologiyalar rivojlanishi bilan yangi tahdidlar ham paydo bo‘lmoqda. Bulutli xizmatlarga hujumlar, IoT qurilmalarining zaifligi, sun’iy intellekt asosidagi zararli dasturlar va ma’lumotlar sizib chiqishi zamonaviy kiberxavfsizlikning asosiy muammolaridan biri hisoblanadi.

Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi bilan bir qatorda kiberxavfsizlik masalalari ham dolzarb ahamiyat kasb etmoqda. Axborot tizimlari va kompyuter tarmoqlarining keng qo‘llanilishi turli xil kiber tahdidlarning paydo bo‘lishiga sabab bo‘lib, zararli dasturlar, phishing hujumlari, tarmoq hujumlari, ichki tahdidlar hamda ijtimoiy muhandislik usullari axborot xavfsizligiga jiddiy xavf tug‘dirmoqda. Ushbu tahdidlar nafaqat texnik nosozliklarga, balki iqtisodiy zarar, maxfiy ma’lumotlarning yo‘qolishi va tashkilotlar faoliyatining izdan chiqishiga ham olib kelishi mumkin.

Maqolada kiberxavfsizlik tahdidlarining asosiy turlari tahlil qilinib, ularning ishlash mexanizmlari hamda xavflilik darajasi yoritildi. Shuningdek, zamonaviy axborot tizimlarini himoyalashda kompleks yondashuv — texnik, tashkiliy va huquqiy choralarni uyg‘unlashtirish zarurligi asoslab berildi. Antivirus vositalari, tarmoq xavfsizlik devorlari (firewall), shifrlash usullari, autentifikatsiya mexanizmlari va foydalanuvchilarni xabardor qilish kabi chora-tadbirlar kiber tahdidlarning oldini olishda muhim ahamiyatga ega ekanligi ko‘rsatildi.

Xulosa sifatida aytish mumkinki, kiberxavfsizlikni ta’minlash doimiy takomillashtirishni talab qiladigan jarayon bo‘lib, davlat organlari, tashkilotlar va oddiy foydalanuvchilarning hamkorlikdagi harakatlari orqali samarali natijalarga erishish mumkin. Axborot xavfsizligi bo‘yicha bilim va ko‘nikmalarni oshirish hamda zamonaviy himoya texnologiyalarini joriy etish kelajakdagi kiber tahdidlarga qarshi kurashning muhim omili hisoblanadi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Prezidenti. (2020). PF–6079-son Farmon: “Raqamli O‘zbekiston – 2030” strategiyasi. Toshkent, O‘zbekiston Respublikasi qonunchilik hujjatlari to‘plami.

2. O‘zbekiston Respublikasi Prezidenti. (2021). PQ–5053-son Qaror: Axborot xavfsizligini ta’minlash choratadbirlari. Toshkent, O‘zbekiston Respublikasi qonunchilik hujjatlari to‘plami.

3. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson Education.

4. Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach*. Pearson.

5. Sayfullayevich, X. K., & Qizi, A. H. R. (2024). CISCO MARSHRUTIZATORINI SOZLASH VA ISHLASH JARAYONINI TEKSHIRISH. Механика и технология, 4(17), 260-263.

6. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information Security Management Systems (ISMS). Geneva, Switzerland.

7. Xaydarov, K. S. (2025). ZAMONAVIY TARMOQ XAVFSIZLIGINI TA'MINLASHDA CISCO PACKET TRACER DASTURINI IMKONIYATLARI. Экономика и социум, (1-2 (128)), 509-512.

8. O‘zbekiston Respublikasi Oliy Majlisi. (2003). “Axborotlashtirish to‘g‘risida”gi Qonun. Toshkent.