ISSN 3060-4567

KIBERXAVFSIZLIK: ZAMONAVIY TAHDIDLAR VA HIMOYA CHORALARI

CYBERSECURITY: MODERN THREATS AND PROTECTIVE MEASURES

КИБЕРБЕЗОПАСНОСТЬ: СОВРЕМЕННЫЕ УГРОЗЫ И МЕРЫ ЗАЩИТЫ

Toshboltayev Faxriddin O'rinboyevich

FarDU "Axborot texnologiyalari" kafedrasi katta o'qituvchisi (PhD)

Nazirjonova Oydinoy To'lqinjon qizi

FarDU, chet tillari fakulteti, filologiya va tillarni o'qitish:ingliz tili 1- kurs talabasi

Annotatsiya*: Ushbu maqolada zamonaviy kiberxavfsizlik tahdidlari va ularga qarshi kurashish yo'llari ko'rib chiqiladi. Avvalo, raqamli makonda tez-tez uchrab turadigan tahdidlar — zararli dasturlar, xakerlik hujumlari, ma'lumotlar sizib chiqishi va ijtimoiy muhandislik usullari haqida so'z yuritiladi. Shundan so'ng, bu tahdidlarga qarshi samarali himoya choralari, xavfsizlik siyosatlari va zamonaviy texnologik yechimlar muhokama qilinadi. Maqola asosan amaliy ahamiyat kasb etadi va tashkilotlar hamda oddiy foydalanuvchilar uchun kiberxavfsizlikni ta'minlash bo'yicha amaliy tavsiyalar beradi.*

Abstract: *This article examines modern cybersecurity threats and ways to counter them. First, it discusses the main threats frequently encountered in the digital space — such as malware, hacking attacks, data breaches, and social engineering techniques. Then, effective protection measures, security policies, and modern technological solutions against these threats are reviewed. The article is primarily of practical value and provides recommendations for organizations and individual users on ensuring cybersecurity.*

Аннотация*: В данной статье рассматриваются современные угрозы кибербезопасности и способы борьбы с ними. Сначала обсуждаются основные*

угрозы, часто встречающиеся в цифровом пространстве — вредоносные программы, хакерские атаки, утечки данных и методы социальной инженерии. Затем анализируются эффективные меры защиты, политики безопасности и современные технологические решения для противодействия этим угрозам. Статья в основном носит практический характер и содержит рекомендации для организаций и отдельных пользователей по обеспечению кибербезопасности.

Kalit so'zlar: *Kiberxavfsizlik, kiber tahdidlar, zararli dasturlar (malware), xakerlik hujumlari, ma'lumotlar sizib chiqishi, ijtimoiy muhandislik (social engineering), himoya choralari, xavfsizlik siyosati, raqamli xavfsizlik, tarmoq xavfsizligi, axborot xavfsizligi, shifrlash (encryption), parol himoyasi, antivirus dasturlari, ddos hujumlari, kiberhujumlar profilaktikasi, xavfsizlik protokollari, identifikatsiya va autentifikatsiya, kompyuter xavfsizligi, internet xavfsizligi.*

Keywords: *Cybersecurity, cyber threats, malware, hacking attacks, data breaches, social engineering, protection measures, security policies, digital security, network security, information security, encryption, password protection, antivirus software, DDoS attacks, cyberattack prevention, security protocols, identification and authentication, computer security, internet security.*

Ключевые слова: *Кибербезопасность, киберугрозы, вредоносные программы (malware), хакерские атаки, утечки данных, социальная инженерия, меры защиты, политика безопасности, цифровая безопасность, безопасность сети, информационная безопасность, шифрование (encryption), защита паролей, антивирусные программы, DDoS атаки, профилактика кибератак, протоколы безопасности, идентификация и аутентификация, безопасность компьютера, безопасность интернета.*

KIRISH

Bugungi kunda texnologiyalar hayotimizning ajralmas qismiga aylangan. Internet va raqamli tizimlar butun dunyo bo‘ylab axborot almashish, biznes faoliyatini tashkil etish, va shaxsiy kommunikatsiyalarni olib borish imkoniyatlarini taqdim etadi. Biroq, bu imkoniyatlar bilan birga, turli xavflar ham paydo bo‘lmoqda. Kiberxavfsizlik

bu tahdidlarga qarshi samarali kurashish va raqamli dunyoni himoya qilish uchun zarur bo‘lgan choralardan iboratdir. Shuningdek, har bir kishi va tashkilotning raqamli xavfsizligini ta’minlash masalasi, endi nafaqat mutaxassislar, balki keng jamoatchilik uchun ham dolzarb bo‘lib qolgan.

Zararli dasturlar (malware), xakerlik hujumlari, ma'lumotlar o‘g‘irlanishi, phishing va ijtimoiy muhandislik usullari kabi tahdidlar, raqamli dunyoning tabiiy qismiga aylangan. Ushbu tahdidlar, nafaqat katta korporatsiyalar, balki kichik va o‘rta bizneslar, hatto individual foydalanuvchilar uchun ham real xavf tug‘diradi. Masalan, shaxsiy ma'lumotlar va moliyaviy hisoblar o‘g‘irlanishi, davlatlar va tashkilotlar orasida xavfsizlikni buzadigan xakerlik hujumlari, kompaniyalar uchun katta moliyaviy yo‘qotishlarga olib kelishi mumkin.

Kiberhujumlar va tahdidlarga qarshi kurashish uchun, zamonaviy xavfsizlik choralariga ehtiyoj ortib bormoqda. Bugungi kunda, xavfsizlik siyosatlari va texnologik yechimlar nafaqat zararli dasturlarni aniqlash, balki ularga qarshi samarali himoya choralarini amalga oshirishga qaratilgan. Raqamli xavfsizlikni ta'minlash uchun shifrlash (encryption), xavfsizlik protokollari, antivirus dasturlari, va tarmoq himoyasi kabi ilg‘or texnologiyalar zarur. Shu bilan birga, foydalanuvchilarning ongli va ehtiyotkorligi ham katta rol o‘ynaydi, chunki kiberhujumlarning ko‘p qismini inson omili tashkil etadi.

Ushbu maqolada kiberxavfsizlikni ta'minlash uchun zarur bo‘lgan himoya choralari, xavfsizlik siyosatlari va ilg‘or texnologiyalar haqida batafsil so‘z yuritiladi. Maqola, foydalanuvchilarga va tashkilotlarga kiberxavfsizlikni yaxshilash uchun amaliy tavsiyalar berishga qaratilgan. Har bir shaxs va tashkilot o‘z raqamli xavfsizligini ta’minlash uchun zamonaviy tahdidlarga qarshi kurashishda yangi yondashuvlar va strategiyalarni joriy etishi zarur.

KIBERXAVFSIZLIKNING AHAMIYATI VA ZARARLI DASTURLAR, HAKKERLAR XUJUMI

Bugungi kunda kiberxavfsizlik nafaqat yirik kompaniyalar, balki har birimiz uchun ham muhim masala hisoblanadi. Internet va raqamli texnologiyalar hayotimizning ajralmas qismiga aylangani sayin, bizning shaxsiy ma'lumotlarimiz va

ISSN 3060-4567

moliyaviy hisoblarimiz xavf ostiga tushadi. Har kuni internetda turli xil xatarlar mavjud: zararli dasturlar, xakerlik hujumlari, ma'lumotlarning o‘g‘irlanishi va boshqa tahdidlar. Shu sababli, kiberxavfsizlikni ta'minlash uchun zamonaviy texnologiyalar va samarali himoya choralariga ehtiyoj ortmoqda.

Zararli dasturlar (malware) kiberxavfsizlik tahdidlarining eng keng tarqalgan va zararli turlaridan biridir. Ular foydalanuvchilarning tizimlariga kirib, ma'lumotlarini o‘g‘irlaydi, tizimlarni buzadi, yoki ularni xavfli holatga keltiradi. Zararli dasturlar orasida **ransomware** (talab qilish dasturlari) va **troyanlar** kabi turlari keng tarqalgan. Ransomware dasturi, odatda, tizimga kirganidan so‘ng, foydalanuvchining ma'lumotlarini shifrlaydi va undan keyin ma'lumotlarni qaytarish uchun pul talab qiladi. Bu turdagi hujumlar, xususan, yirik kompaniyalar va tashkilotlar uchun katta zarar keltirishi mumkin. Misol uchun, 2017-yilda **“WannaCry”** ransomware hujumi dunyo bo‘ylab minglab kompaniyalarni, davlat tashkilotlarini va boshqa muhim infratuzilmalarning tizimlarini shifrlash orqali zararlandi. Hujumning ta'siri tufayli, ko‘plab tashkilotlar bir necha kun davomida o‘z ish faoliyatini to‘xtatishga majbur bo‘lishdi, bu esa ularga katta moliyaviy yo‘qotishlarga olib keldi.

Shuningdek, **troyan** dasturlari, o‘zini xavfsiz va ishonchli dastur sifatida ko‘rsatib, foydalanuvchining kompyuteriga kiradi va tizimda cheksiz zarar keltiradi. Ular ko‘pincha **email**, **download link** yoki boshqa shakllarda tarqatiladi. Misol uchun, bir troyan dasturi, foydalanuvchi tizimiga kirganidan keyin, bank hisob raqamlariga kirish uchun foydalanuvchining shaxsiy ma'lumotlarini o‘g‘irlaydi yoki ularning kompyuter tizimlarini remote kirish orqali boshqaradi. Bu turdagi zararli dasturlar, ko‘pincha o‘zgaruvchan va yashirin holatda bo‘lib, foydalanuvchilar uchun sezilmas bo‘lishi mumkin.

Bundan tashqari, **xakerlik hujumlari** ham kiberxavfsizlikni jiddiy tahdid qilishda davom etmoqda. Xakerlar, o‘zlarining malakali usullari yordamida tizimga kirib, foydalanuvchilarning yoki tashkilotlarning ma'lumotlarini o‘g‘irlaydi. 2017-yilda **Equifax** kompaniyasiga qilingan xakerlik hujumi, jahon miqyosida eng yirik va eng zararli hujumlardan biri bo‘ldi. Bu hujum natijasida 147 milliondan ortiq amerikaliklarning shaxsiy ma'lumotlari, shu jumladan kredit tarixlari va identifikatsiya

raqamlari o‘g‘irlandi. Bu kabi hujumlar nafaqat kompaniyalarga, balki foydalanuvchilarning shaxsiy xavfsizligiga ham jiddiy zarar yetkazadi. Xakerlar tizimga kirganida, ular nafaqat moliyaviy ma'lumotlarni o‘g‘irlaydi, balki foydalanuvchi ishonchini suiiste'mol qilib, boshqa hujumlarga ham tayyorlanadi.

Ushbu turdagi tahdidlar, kiberxavfsizlikni ta'minlash zaruratini yana bir bor tasdiqlaydi. Agar foydalanuvchilar va tashkilotlar zararli dasturlar va xakerlik hujumlariga qarshi samarali himoya choralarini ko‘rmasalar, ular katta moliyaviy zararlar va shaxsiy ma'lumotlarning o‘g‘irlanishiga duch kelishlari mumkin. Shu sababli, kompaniyalar va individual foydalanuvchilar o‘z tizimlarini doimiy ravishda yangilab turishlari, kuchli xavfsizlik siyosatlarini amalga oshirishlari va zamonaviy texnologiyalarni foydalanishlari lozim.

Zararli dasturlar va xakerlik tahdidlari doimo rivojlanib bormoqda. Shu bois, kiberxavfsizlikni ta'minlash uchun zamonaviy va samarali himoya choralarini joriy etish, tizimlarni muntazam ravishda tekshirib turish va foydalanuvchilarni kiberxavfsizlik masalalari bo‘yicha o‘qitish juda muhimdir. Aks holda, bu tahdidlar bizning raqamli hayotimizga katta salbiy ta'sir ko‘rsatishi mumkin.

Zararli dasturlar (malware) va xakerlik hujumlarining oldini olish uchun samarali himoya choralarini ko‘rish juda muhim. Zamonaviy xavf-xatarlar va tahdidlarga qarshi kurashishda faqat texnologiyalardan foydalanish yetarli emas; foydalanuvchilarni muntazam ravishda o‘qitish va xavfsizlikni ta’minlashda kuchli siyosatlarni amalga oshirish ham muhimdir. Quyida zararli dasturlar va xakerlik hujumlarini oldini olish bo‘yicha ba'zi samarali himoya choralari keltirilgan:

Kuchli parollar va ularni muntazam yangilash

Kuchli parollar yaratish va ularni muntazam ravishda yangilash zarur. Parollar uzoq va murakkab bo‘lishi kerak, shuningdek, har bir tizim yoki hisob uchun alohida parol qo‘yish maqsadga muvofiqdir. Oddiy va oson taxmin qilinadigan parollarni ishlatish, xakerlarga tizimga kirish imkoniyatini yaratadi. Parol boshqaruvchilari yordamida barcha parollarni xavfsiz tarzda saqlash va boshqarish mumkin.

Ikki faktorli autentifikatsiya (2FA)

Ikki faktorli autentifikatsiya (2FA) tizimi orqali tizimga kirishda qo‘shimcha xavfsizlik qatlami qo‘shiladi. Bu texnologiya foydalanuvchidan parolni kiritgandan so‘ng, telefon raqamiga yoki emailga yuborilgan kodni kiritishni talab qiladi. 2FA yordamida, hatto agar xaker foydalanuvchining parolini o‘g‘irlagan bo‘lsa ham, tizimga kirish imkoniyati bo‘lmaydi.

Antivirus dasturlari va tizim yangilanishlari

Antivirus dasturlarini muntazam yangilab borish va ularni tizimga o‘rnatish zarur. Bu dasturlar zararli kodlarni aniqlash va ularni tizimdan o‘chirishda yordam beradi. Shuningdek, tizimni doimiy ravishda yangilab turish kerak, chunki xavfsizlikni ta'minlovchi yangilanishlar yangi tahdidlarga qarshi kurashishda muhim rol o‘ynaydi. Agar tizim yangilanmasa, eski versiyalarni ishlatish, xakerlarga tizimga kirish imkoniyatini yaratadi.

Xavfsizlik devorlari (Firewalls)

Tarmoq xavfsizligini ta'minlash uchun xavfsizlik devorlarini (firewall) ishlatish juda muhimdir. Bu dasturlar, tizim va tarmoq o‘rtasidagi aloqani nazorat qiladi va noma'lum yoki shubhali trafikni bloklaydi. Firewalldan foydalanish, tarmoqdagi noxush faoliyatni aniqlash va oldini olish imkoniyatini beradi. Shuningdek, tashkilotlar o‘z tizimlarida xavfsizlik devorlarini sozlash orqali o‘z tarmog‘ini himoya qilishlari mumkin.

Shifrlash texnologiyalari

Shifrlash, ma'lumotlarni o‘g‘irlashni oldini olishda muhim vositadir. Agar ma'lumotlar o‘g‘irlangan bo‘lsa ham, ular shifrlangan bo‘lsa, faqat tegishli kalit bilan ochilishi mumkin. Bu xavfsizlik chorasini faqat shaxsiy yoki muhim ma'lumotlar uchun emas, balki butun tizim uchun qo‘llash maqsadga muvofiqdir. Shifrlash texnologiyalarini joriy etish orqali, ma'lumotlar tashqi tahdidlardan himoyalangan bo‘ladi.

Phishing hujumlariga qarshi himoya

Phishing hujumlarining oldini olish uchun foydalanuvchilarni aldamchi elektron xatlar yoki havolalarga qarshi ehtiyotkorlik bilan o‘qitish kerak. Xakerlar ko‘pincha rasmiy kompaniyalar nomidan email yuborib, foydalanuvchilardan shaxsiy

ISSN 3060-4567

ma'lumotlarni olishga harakat qilishadi. Bunday hujumlardan himoya qilish uchun, foydalanuvchilarga email yoki SMS orqali yuborilgan havolalar va ilovalarni tekshirishni, shuningdek, shubhali xabarlarni ochmaslikni o‘rgatish zarur. Ehtiyotkorlik bilan ishlash, kiberxavfsizlikni mustahkamlashda muhim rol o‘ynaydi.

Xodimlarni kiberxavfsizlikka o‘qitish

Kompaniyalar uchun xavfsizlik siyosatlarining muhim jihatlaridan biri, xodimlarni muntazam ravishda kiberxavfsizlik bo‘yicha o‘qitishdir. Xodimlarga kiberhujumlar haqida doimiy ravishda ma'lumot berib borish, phishing, troyanlar va boshqa zararli dasturlarni qanday aniqlash va ularga qarshi qanday choralar ko‘rish kerakligini o‘rgatish kerak. O‘qitish orqali, xodimlar kiberxavfsizlikka nisbatan mas'uliyatli bo‘lishlari va kompaniya xavfsizligini ta'minlashga yordam berishlari mumkin.

Ma'lumotlarni zaxiralash

Ma'lumotlarni muntazam ravishda zaxiralash, zararli dasturlar yoki xakerlik hujumlari natijasida ma'lumotlar yo‘qolishi yoki zarar ko‘rishi holatida ularga tezda kirish imkonini beradi. Zaxiralar, tizimni tezda tiklash va ma'lumotlarni tiklashda yordam beradi. Zaxiralash jarayonini avtomatlashtirish va ularni xavfsiz joyda saqlash juda muhimdir. Bu, kompaniyalar va foydalanuvchilar uchun katta xavfsizlik kafolati bo‘lishi mumkin.

Tarmoqni monitoring qilish

Tarmoqdagi barcha faoliyatni monitoring qilish, shubhali harakatlarni aniqlashda yordam beradi. Yirik tashkilotlar tarmoqni doimiy ravishda monitoring qilib borishlari kerak. Shubhali faoliyatni tezda aniqlash, uni bloklash va boshqa xavfsizlik choralarini qo‘llash imkonini beradi. Tarmoqda noma'lum yoki qoidaga xilof harakatlarni aniqlash uchun maxsus tizimlar va dasturlarni joriy etish zarur.

Yuqoridagi himoya choralarini samarali amalga oshirish, foydalanuvchilarning va tashkilotlarning kiberxavfsizligini ta'minlashda muhim ahamiyatga ega. Raqamli dunyoda xavf-xatarlar har doim mavjud bo‘lishi mumkin, lekin bu choralar yordamida ularning oldini olish mumkin. Har bir foydalanuvchi va kompaniya o‘z xavfsizlik choralarini mustahkamlab, kiberhujumlardan samarali himoyalanishi zarur.

Xulosa sifatida shuni aytishimiz mumkinki, kiberxavfsizlik zamonaviy dunyoda juda muhim ahamiyat kasb etadi, chunki bizning hayotimizning ko‘p qismi raqamli texnologiyalar va internetga bog‘liq. Zararli dasturlar, xakerlik hujumlari va boshqa xavf-xatarlar nafaqat katta kompaniyalar, balki oddiy foydalanuvchilar uchun ham jiddiy muammolarga aylanishi mumkin. Ammo, samarali himoya choralari va xavfsizlik siyosatlarini joriy etish orqali, bu tahdidlarga qarshi turish mumkin.

Kuchli parollar, ikki faktorli autentifikatsiya (2FA), antivirus dasturlari, va tizimlarni doimiy ravishda yangilab borish kabi choralar, zararli dasturlardan va xakerlik hujumlaridan himoyalanishda asosiy vositalardir. Shifrlash texnologiyalari va xavfsizlik devorlari orqali ma'lumotlar va tizimlar yanada mustahkamlanadi. Bundan tashqari, foydalanuvchilarni phishing hujumlariga qarshi o‘qitish va ularni kiberxavfsizlik bo‘yicha muntazam ravishda xabardor qilish, zararli hujumlarga qarshi kurashishda muhim rol o‘ynaydi.

Xodimlarni o‘qitish va ma'lumotlarni zaxiralash kabi amaliy choralar orqali tashkilotlar o‘z tizimlarini yanada xavfsiz qilishlari mumkin. Tarmoqni doimiy ravishda monitoring qilish va shubhali faoliyatlarni tezda aniqlash, xavfsizlikni ta'minlashga yordam beradi.

Shunday qilib, kiberxavfsizlik nafaqat texnologik yechimlarga, balki ongli foydalanuvchilarga, kuchli xavfsizlik siyosatlariga va tashkilotlarning mas'uliyatiga ham bog‘liq. Zamonaviy tahdidlarga qarshi kurashishda samarali himoya choralari, himoyalangan tizimlar va doimiy yangilanishlar orqali biz o‘z raqamli xavfsizligimizni ta'minlashimiz mumkin.

FOYDALANILGAN MANBALAR

1. **National Cyber Security Centre (NCSC)** - https://www.ncsc.gov.uk/

- Bu saytda zamonaviy kiberxavfsizlik tahdidlari va himoya choralariga oid keng qamrovli ma'lumotlar mavjud.

2. **Kaspersky Lab** - https://www.kaspersky.com/- Kaspersky xavfsizlik kompaniyasi, zararli dasturlar, troyanlar, ransomware va boshqa kiberxavfsizlik tahdidlari bo‘yicha chuqur tahlillar va maqolalar taqdim etadi.

ISSN 3060-4567

3. **Symantec (Norton)** - https://www.broadcom.com/company/newsroom/press-releases?filtr=Symantec - Norton antivirus dasturi ishlab chiqaruvchisi, kiberxavfsizlik bo‘yicha eng so‘nggi yangiliklar va texnologiyalarni taqdim etadi.

4. **SANS Institute** - https://www.sans.org/ - SANS Institute, kiberxavfsizlikka oid ta'lim resurslari va ilmiy ishlanmalarni taqdim etadi.

5. **OWASP (Open Web Application Security Project)** - https://owasp.org/- OWASP, veb ilovalar xavfsizligini ta'minlash bo‘yicha global harakatni boshqaradi va xavfsizlik tahlillari, qo‘llanmalar va vositalarni taqdim etadi.

6. **Cybersecurity & Infrastructure Security Agency (CISA)** - https://www.cisa.gov/ - CISA, AQSh hukumati tomonidan taqdim etilgan kiberxavfsizlik va infratuzilma xavfsizligi resurslarining asosiy manbai.

7. **MITRE ATT&CK** - https://attack.mitre.org/ - MITRE ATT&CK, kiberhujumlar va ularning oldini olish bo‘yicha dunyo miqyosida qabul qilingan metodologiya va vositalarni taqdim etadi.

8. **US-CERT (United States Computer Emergency Readiness Team)** - https://www.us-cert.cisa.gov/ - Bu sayt, kiberhujumlar va ularning oldini olish uchun zarur bo‘lgan xavfsizlik choralari haqida ma'lumot beradi.