AXBOROT XAVFSIZLIGI: MUAMMOLAR VA YECHIMLAR

Ma’rufov Elmurod Xosiljon o’g’li
Qo’shtepa tuman 1-son politexnikumi Maxsus fan o’qituvchisi

Annotatsiya: Ushbu maqolada axborot xavfsizligi sohasidagi dolzarb muammolar va ularning yechimlari yoritilgan. Raqamli texnologiyalar tez rivojlanayotgan bir paytda kiberxavfsizlik tahdidlari – xususan, kiberhujumlar, zararli dasturlar, ichki tahdidlar va shaxsiy ma’lumotlarning himoyasizligi kabi muammolar tobora kuchaymoqda. Maqolada zamonaviy antivirus va xavfsizlik dasturlaridan foydalanish, kuchli parol siyosatini joriy etish, foydalanuvchilarni o‘qitish, ma’lumotlarni zaxiralash kabi samarali himoya choralariga alohida e’tibor qaratilgan. Axborot xavfsizligini ta’minlash har bir foydalanuvchi va tashkilot zimmasidagi muhim vazifa ekanligi ta’kidlangan.
Kalit so’zlar: Axborot xavfsizligi, Kiberxavfsizlik, Kiberhujumlar, Antivirus dasturlari, Parol siyosati, Ma’lumotlarning maxfiyligi.

INFORMATION SECURITY: PROBLEMS AND SOLUTIONS

Abstract. TThis article discusses current issues in the field of information security and their solutions. At a time when digital technologies are rapidly developing, cybersecurity threats - in particular, cyberattacks, malware, insider threats, and personal data vulnerabilities - are becoming increasingly common. The article focuses on effective protection measures, such as using modern antivirus and security programs, implementing a strong password policy, training users, and backing up data. It is emphasized that ensuring information security is an important task for every user and organization.
Key words: Information security, Cybersecurity, Cyberattacks, Antivirus programs, Password policy, Data privacy.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПРОБЛЕМЫ И РЕШЕНИЯ

Аннотация: В статье рассматриваются актуальные проблемы в сфере информационной безопасности и пути их решения. В условиях стремительного развития цифровых технологий все чаще встречаются угрозы кибербезопасности, в частности кибератаки, вредоносное ПО, инсайдерские угрозы и уязвимости персональных данных. В статье особое внимание уделено эффективным мерам защиты, таким как использование современных антивирусных и защитных программ, внедрение надежной политики паролей, обучение пользователей и резервное копирование данных. Подчеркивается, что обеспечение информационной безопасности является важной задачей для каждого пользователя и организации.
Ключевые слова: Информационная безопасность, Кибербезопасность, Кибератаки, Антивирусные программы, Политика паролей, Конфиденциальность данных.

Axborot xavfsizligi: muammolar va yechimlar. Bugungi kunda axborot texnologiyalari hayotimizning ajralmas qismiga aylangan. Internet va raqamli qurilmalar yordamida katta hajmdagi ma'lumotlar almashiladi, saqlanadi va qayta ishlanadi. Shu bilan birga, axborot xavfsizligi muammolari ham tobora murakkablashib bormoqda. Axborot xavfsizligi – bu ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlashga qaratilgan chora-tadbirlar yig'indisidir.Bugungi raqamli dunyoda kiberhujumlar va zararli dasturlar axborot xavfsizligining eng katta tahdidlaridan biridir. Internet va kompyuter tarmoqlarining keng tarqalishi bilan, xakerlar turli usullar orqali tizimlarga hujum qilib, maxfiy ma'lumotlarni o'g'irlash, tizimlarni ishdan chiqarish yoki hatto moliyaviy zarar yetkazishga harakat qiladilar.

Kiberhujumlar turlari

Phishing (firibgarlik)

Phishing – bu foydalanuvchilarni soxta saytlar yoki elektron pochta orqali aldash va shaxsiy ma'lumotlarini, parollarini, bank kartalari ma'lumotlarini o'g'irlash usuli. Masalan, foydalanuvchiga bankdan yuborilgan ko'rinadigan soxta xabar orqali ularning hisob raqamiga kira olish.

DDoS (Distributed Denial of Service) hujumlari

Ushbu hujumda maqsadli veb-sayt yoki xizmatga millionlab so'rovlar yuborilib, uning ishlashini to'xtatish yoki sekinlashtirishdir. Bu kompaniyaning xizmat ko'rsatish faoliyatini to'xtatib qo'yishi mumkin.

Malware (zararli dasturlar)

Malware – zarar yetkazish uchun maxsus yaratilgan dasturlar to'plami bo'lib, viruslar, trojanlar, ransomware (qutqarish uchun pul talab qiluvchi dasturlar), spyware (ma'lumotlarni yashirin kuzatuvchi dasturlar) kabi turlarni o'z ichiga oladi.

Viruslar: O'zini ko'paytirib, tizimga zarar yetkazadi, fayllarni yo'q qiladi yoki o'zgartiradi.

Troyan otlari (Trojan horses): Foydalanuvchini aldaydi va zararli kodlarni yashirib, tizimga kirishga imkon beradi.

Ransomware: Ma'lumotlarni shifrlab, egasidan ochish uchun pul talab qiladi.

Spyware: Foydalanuvchi faoliyatini yashirincha kuzatadi va ma'lumotlarni o'g'irlaydi.

Kiberhujumlardan himoyalanish choralari

Antivirus dasturlarini o'rnatish va muntazam yangilash Antiviruslar zararli dasturlarni aniqlash va bloklashda yordam beradi. Ularni doimiy ravishda yangilab turish zarur.

Parollarni kuchaytirish va ikki faktorli autentifikatsiyani joriy etish Kuchli, murakkab parollar va qo'shimcha xavfsizlik qatlami hisoblanadigan ikki faktorli tasdiqlash himoyani sezilarli darajada oshiradi.

Shubhali havolalarga bosmaslik va noma'lum manbalardan dastur yuklab olmaslik

Phishing va zararli dasturlar ko‘pincha elektron pochta yoki xabarlar orqali tarqatiladi. Shu sababli, ishonchsiz manbalardan ehtiyotkorlik bilan foydalanish kerak.

Tizimlarni va dasturlarni yangilab turish
Yangilanishlar xavfsizlik zaifliklarini bartaraf etadi va tizimni himoya qiladi.

Xodimlar va foydalanuvchilarni o‘qitish
Tashkilotlarda xodimlarni kiberxavfsizlik bo‘yicha muntazam ravishda o‘qitish, firibgarlik va zararli dasturlardan himoyalanish qoidalarini o‘rgatish zarur.Axborot xavfsizligini ta’minlashda zamonaviy antivirus va xavfsizlik dasturlarining roli beqiyosdir. Har kuni minglab yangi zararli dasturlar va kiberhujum usullari paydo bo‘layotgan bir paytda, oddiy foydalanuvchi yoki yirik tashkilotlar uchun zamonaviy himoya vositalarisiz xavfsizlikni ta’minlash deyarli imkonsiz.

Antivirus dasturlarining vazifalari

Antivirus dasturlari — bu kompyuter va boshqa raqamli qurilmalarda zararli dasturlarni (malware, viruslar, trojanlar, spyware va boshqalar) aniqlash, bloklash va yo‘q qilish uchun mo‘ljallangan dasturlar to‘plamidir. Ularning asosiy vazifalari quyidagilardan iborat:

Real vaqt rejimida himoya qilish
Antivirus doimiy tarzda tizimni kuzatadi va har qanday shubhali faoliyatni aniqlashga harakat qiladi

Skane qilish (tekshirish)
Fayllarni, tizim papkalarini, USB qurilmalarni yoki butun diskni virus va zararli kodlarga tekshiradi.

Izolyatsiya qilish (karantin)
Zararli deb topilgan fayllarni tizimdan ajratib qo‘yadi, shunda ular boshqa fayllarga zarar yetkaza olmaydi.

Shifrlangan hujumlarni aniqlash
Ko‘plab zamonaviy antiviruslar tarmoq trafikini ham kuzatib borib, phishing, ransomware yoki DDoS hujumlarini aniqlay oladi.

Zamonaviy xavfsizlik dasturlarining imkoniyatlari

Zamonaviy xavfsizlik dasturlari antivirusdan ko‘ra kengroq funksiyalarga ega. Ular quyidagi xususiyatlarni o‘z ichiga olishi mumkin:

Firewall (tarmoqlararo xavfsizlik devori): Internet va lokal tarmoq o‘rtasidagi kirish-chiqishni nazorat qiladi.

Antiphishing moduli: Foydalanuvchini soxta sahifalar va firibgarliklardan ogohlantiradi.

VPN (Virtual Private Network): Foydalanuvchining internetda anonim va xavfsiz harakatlanishini ta’minlaydi.

Parol menejerlari: Kuchli parollarni yaratadi va ularni xavfsiz saqlaydi.

Zararlangan saytlarni bloklash: Antivirus dasturi zararli saytga kirishga urinishni avtomatik ravishda to‘xtatadi.

Mashhur antivirus va xavfsizlik dasturlari

Bugungi kunda ko‘plab ishonchli antivirus va xavfsizlik dasturlari mavjud. Ularning ayrimlari quyidagilardir:

Kaspersky
Bitdefender
Norton Security
ESET NOD32
Avast
McAfee
Windows Defender (Microsoft tomonidan taqdim etiladi)

Foydalanishda e’tiborli bo‘lish kerak bo‘lgan jihatlar

Doimiy yangilanish
Zamonaviy antivirus dasturlari muntazam ravishda yangilanib turishi kerak, chunki har kuni yangi zararli kodlar paydo bo‘ladi.

Litsenziyali versiyadan foydalanish
Nofaqat himoya, balki qo‘shimcha imkoniyatlar ham aynan to‘liq litsenziyali versiyalarda mavjud bo‘ladi. Nolegal yoki qaroqchi versiyalar xavfsizlikni o‘zi buzishi mumkin.

Yengil va samarali dastur tanlash
Tizimga ortiqcha yuk solmaydigan, foydalanuvchi uchun qulay interfeysga ega bo‘lgan dasturlar ustuvorlikka ega bo‘lishi kerak.

Axborot xavfsizligi – bu faqat texnik masala emas, balki har bir foydalanuvchi va tashkilot uchun mas’uliyatdir. Bugungi kunda kiberxavfsizlikka doir muammolar tobora ortib bormoqda, shuning uchun xavfsizlik choralarini kuchaytirish va doimiy ravishda yangilab borish talab etiladi. Har birimiz axborot xavfsizligini ta’minlashda faollik ko‘rsatib, o‘zimizni va atrofdagilarni himoya qilishimiz kerak.

REFERENCES:

· G‘ulomov S.S., Raximov T.T. *Axborot xavfsizligi asoslari.* – Toshkent: “Fan va texnologiya”, 2021.
· · Boboxo‘jayev A.S. *Kiberxavfsizlik asoslari.* – Toshkent: Iqtisodiyot va innovatsion texnologiyalar nashriyoti, 2020.
· · Stallings W. *Network Security Essentials: Applications and Standards.* – Pearson Education, 2020.
· https://www.ziyouz.com/kutubxona.