

IT SOHASIDA AXBOROT XAVFSIZLIGI**Abdihakimov Mirjalol Akbar o'g'li****Matematika va informatika ta'lim yo'nalishi****O'ktamov Madadjon O'ktam o'g'li****SHDPI Matematika va ta'limda axborot texnologiyasi****kafedrasi o'qituvchisi****<https://doi.org/10.5281/zenodo.14997493>**

Annotatsiya: Ushbu maqolada axborot xavfsizligining asosiy tamoyillari, tahdid turlari va zamonaviy himoya usullari tahlil qilinadi. Axborot texnologiyalari rivojlanishi bilan birga kiberxavfsizlik muammolari ham ortib bormoqda. Ish davomida axborot xavfsizligining asosiy komponentlari – maxfiylik, yaxlitlik va mavjudlik tamoyillari ko'rib chiqiladi. Shuningdek, zararli dasturlar, fishing hujumlari, tarmoqlar orqali yetkaziladigan tahdidlar va inson omiliga bog'liq xavf-xatarlar haqida ma'lumot beriladi. Himoya mexanizmlari sifatida kriptografik usullar, autentifikatsiya tizimlari, xavfsizlik devorlari (firewall), antivirus dasturlar va boshqa texnologiyalar tahlil qilinadi.

Kalit so'zlar: axborot xavfsizligi, kiberxavfsizlik, kriptografiya, tarmoq xavfsizligi, tahdidlar, himoya vositalari.

Аннотация. В данной статье анализируются основные принципы информационной безопасности, виды угроз и современные методы защиты. Вместе с развитием информационных технологий возрастают и проблемы кибербезопасности. В ходе работы рассматриваются основные составляющие информационной безопасности – принципы конфиденциальности, целостности и доступности. Он также предоставляет информацию о вредоносном ПО, фишинговых атаках, сетевых угрозах и рисках, связанных с деятельностью человека. В качестве механизмов защиты анализируются криптографические методы, системы аутентификации, межсетевые экраны, антивирусные программы и другие технологии.

Ключевые слова: информационная безопасность, кибербезопасность, криптография, безопасность сети, угрозы, методы защиты.

Annotation: This article analyzes the main principles of information security, types of threats and modern protection methods. Along with the development of information technology, the problems of cyber security are also increasing. During the work, the main components of information security - confidentiality, integrity and availability principles are considered. It also provides information on malware, phishing attacks, network-borne threats, and human-caused risks. Cryptographic methods, authentication systems, firewalls, antivirus programs and other technologies are analyzed as protection mechanisms.

Keywords: information security, cybersecurity, cryptography, network security, threats, protection methods.

Axborot texnologiyalarining jadal rivojlanishi inson hayotining turli sohalariga, jumladan, iqtisodiyot, ta'lim, tibbiyot va biznes jarayonlariga katta ta'sir ko'rsatmoqda. Raqamli dunyoda axborot muhim strategik resursga aylangan bo'lib, uni ishonchli himoya qilish dolzarb muammolardan biri hisoblanadi. Shu sababli axborot xavfsizligini ta'minlash masalasi hozirgi kunda tashkilotlar, korxonalar va hatto oddiy foydalanuvchilar uchun ham katta ahamiyat kasb etmoqda.

Ushbu tezisda axborot xavfsizligi tushunchasi, asosiy tahdidlar va himoya usullari tahlil qilinadi. Ish davomida kiberxavfsizlik muammolariga sabab bo'luvchi omillar, zamonaviy himoya texnologiyalari va samarali xavfsizlik strategiyalari o'rganiladi. Shuningdek, tashkilotlar va individual foydalanuvchilar uchun axborot xavfsizligini ta'minlash bo'yicha tavsiyalar beriladi.

IT sohasida axborot xavfsizligi – bu dasturiy ta'minot, apparat vositalari va tarmoqlarning xavfsizligini ta'minlashga qaratilgan kompleks choralar yig'indisidir. IT infratuzilmalari rivojlanishi bilan birga, kiberxavfsizlik tahdidlarining ko'lami ham kengayib bormoqda. Bugungi kunda IT kompaniyalari, davlat idoralari va xususiy tashkilotlar o'z axborot tizimlarini himoya qilishga katta e'tibor qaratishlari talab etiladi.

IT sohasida axborot xavfsizligini ta'minlashning asosiy maqsadi – tizimlar va ma'lumotlarni ruxsatsiz kirish, buzish va yo'q qilishdan himoya qilishdir. Bunga quyidagi yo'nalishlar orqali erishish mumkin:

Bugungi IT muhitida axborot xavfsizligini ta'minlash uchun turli xalqaro standartlar, masalan, ISO/IEC 27001, NIST va GDPR talablariga rioya qilish muhim ahamiyat kasb etadi. Shuningdek, DevSecOps (Development, Security, and Operations) yondashuvi IT kompaniyalari uchun xavfsizlikni dasturiy ta'minot ishlab chiqish jarayonining ajralmas qismiga aylantirish imkonini beradi.

Axborot xavfsizligi tizimi maxfiylik (confidentiality), yaxlitlik (integrity) va mavjudlik (availability) kabi asosiy tamoyillarga asoslanadi. Ushbu tamoyillar ma'lumotlarning ruxsatsiz kirish, buzilish va yo'qolishidan himoyalanihini ta'minlaydi. Biroq, kiberxavfsizlik sohasidagi tahdidlar yildan-yilga ortib borayotganligi sababli, zamonaviy himoya vositalari va strategiyalarining doimiy ravishda takomillashtirilishi zarur.

Mazkur ishning dolzarbligi shundan iboratki, bugungi kunda ko'plab tashkilotlar va foydalanuvchilar kiberxavfsizlik choralari e'tiborsiz qoldirib, turli hujumlar natijasida sezilarli zarar ko'rmoqda. Shu bois axborot xavfsizligi bo'yicha samarali strategiyalar ishlab chiqish va ularni hayotga tatbiq etish zarurati ortib bormoqda.

Axborot xavfsizligi zamonaviy jamiyatda eng dolzarb masalalardan biri hisoblanadi. Texnologiyalar rivojlanishi bilan kiberxavfsizlik tahdidlarining turlari va ko'lami ortib bormoqda. Hozirgi kunda kompaniyalar, davlat tashkilotlari va oddiy foydalanuvchilar o'z ma'lumotlarini himoya qilish uchun samarali strategiyalar ishlab chiqishlari zarur.

Kiberhujumlarning asosiy turlari – fishing, zararli dasturlar, DDoS hujumlar, tarmoq ekspluatatsiyalari va inson omili orqali amalga oshiriladigan hujumlardir. Ayniqsa, ijtimoiy muhandislik (social engineering) usullaridan foydalangan holda foydalanuvchilarning shaxsiy ma'lumotlari va tizimga kirish huquqlarini qo'lga kiritish hozirda keng tarqalgan tahdid hisoblanadi.

Axborot xavfsizligini ta'minlashning samarali usullari mavjud bo'lib, ularga shifrlash texnologiyalari, autentifikatsiya tizimlari, xavfsizlik devorlari (firewall), antivirus dasturlar va tarmoq monitoringi kiradi. Kriptografik algoritmlar, masalan, AES, RSA va SHA, ma'lumotlarning yaxlitligi va maxfiyligini saqlashda muhim rol o'ynaydi. Shuningdek, ikki faktorli autentifikatsiya (2FA) va biometrik xavfsizlik choralari akkauntlarni ruxsatsiz kirishlardan himoya qilishda samarali hisoblanadi.

So'nggi yillarda sun'iy intellekt va mashinaviy o'rganish texnologiyalari kiberxavfsizlikni kuchaytirish uchun qo'llanilmoqda. AI algoritmlari zararli faoliyatlarni avtomatik ravishda

aniqlash va oldini olish imkonini beradi. Shuningdek, blokcheyn texnologiyasi markazlashmagan xavfsizlik tizimlarini yaratishda foydalanilmoqda.

Dunyo miqyosida axborot xavfsizligini tartibga soluvchi xalqaro standartlar mavjud. Masalan, ISO/IEC 27001 va NIST standartlari axborot xavfsizligi siyosatini shakllantirish uchun asosiy mezonlarni belgilaydi. GDPR esa foydalanuvchilarning shaxsiy ma'lumotlarini himoya qilish bo'yicha qat'iy talablarni o'z ichiga oladi. O'zbekistonda ham axborot xavfsizligi bo'yicha qonunchilik takomillashtirilib, davlat va xususiy sektor tashkilotlari uchun muhim talablar qo'yilmoqda.

Xulosa qilib aytganda, axborot xavfsizligini ta'minlash bugungi kunda har bir tashkilot va foydalanuvchi uchun muhim masala hisoblanadi. Himoya choralari, ilg'or texnologiyalar va foydalanuvchilarning xabardorligini oshirish orqali kiberxavfsizlikni mustahkamlash mumkin. Samarali strategiyalar ishlab chiqilmasa, raqamli tahdidlar nafaqat korxonalarga, balki butun jamiyatga jiddiy zarar yetkazishi mumkin. Shunday qilib, IT sohasida axborot xavfsizligi samarali boshqarilmasa, kiberhujumlar, ma'lumotlarning yo'qolishi va biznesning izdan chiqishi ehtimoli ortadi. Shu sababli, IT mutaxassislari xavfsizlik strategiyalarini takomillashtirib borishlari va zamonaviy himoya usullaridan samarali foydalanishlari zarur.

Foydalanilgan adabiyotlar/Используемая литература/References:

1. Qodirov, F. "OPTIMIZATION OF TELECOMMUNICATIONS POWER SUPPLY SYSTEMS BASED ON RELIABILITY CRITERIA." Science and innovation 2.A12 (2023): 15-20.
2. F Qodirov. Aholiga tibbiy xizmatlar ko'rsatishning rivojlanishini iqtisodiy-matematik modellashtirish. Scienceweb academic papers collection . 2023/1/1.
3. F Qodirov. Zamonaviy to'lov tizimlari tahlili va elektron pul birliklari. Scienceweb academic papers collection. 2023/1/1.
4. Farrux Qodirov. Zamonaviy trenajyor va simulyatsiya qiluvchi dasturlarning hozirgi kundagi ahamiyati. Scienceweb academic papers collection. 2023/1/1
5. Farrux Qodirov. BUSINESS INNOVATION MODEL OF INCOME AND COSTS FROM THE PROVISION OF MEDICAL SERVICES TO THE POPULATION. Scienceweb academic papers collection. 2023/1/1
6. Farrux Qodirov. ECONOMIC-MATHEMATICAL MODELING OF THE DEVELOPMENT OF THE PROVISION OF MEDICAL SERVICES TO THE POPULATION. Scienceweb academic papers collection. 2023/1/1
7. Farrux Qodirov. THE PLACE OF ECONOMETRICAL MODELING OF HEALTHCARE QUALITY IMPROVEMENT IN THE DIGITAL ECONOMY. Scienceweb academic papers collection. 2023/1/1
8. Farrux Qodirov. DEVELOPMENT OF SCIENTIFIC AND TECHNOLOGICAL SYSTEM OF MANAGEMENT OF INDUSTRIAL ENTERPRISES. Scienceweb academic papers collection. 2023/1/1
9. Ergash o'g'li, Qodirov Farrux. "CREATION OF ELECTRONIC MEDICAL BASE WITH THE HELP OF SOFTWARE PACKAGES FOR MEDICAL SERVICES IN THE REGIONS." Conferencea (2022): 128-130.
10. Ergash o'g'li, Qodirov Farrux. "IMPORTANCE OF KASH-HEALTH WEB PORTAL IN THE DEVELOPMENT OF MEDICAL SERVICES IN THE REGIONS." Conferencea (2022): 80-83..