ISSN 2181-3187

KIBERXAVFSIZLIK: ZAMONAVIY DUNYODA AXBOROTNI HIMOYA QILISHNING AHAMIYATI

CYBERSECURITY: THE IMPORTANCE OF PROTECTING INFORMATION IN THE MODERN WORLD

КИБЕРБЕЗОПАСНОСТЬ: ЗНАЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННОМ МИРЕ

Bahodirova Madinabonu Ro'zimuhammad qizi

FarDU Filologiya va tillarni o'qitish:

ingliz tili yo‘nalishi 24.111-guruh talabasi

Faxriddin O'rinboevich Toshboltayev

FarDU “Axborot texnologiyalari”

kafedrasi katta o‘qituvchisi (PhD)

Annotatsiya

Ushbu maqola kiberxavfsizlik atrofida yuzaga kelayotgan bir qancha masalalarni yoritadi. Unda turli xil yo‘nalishlarda,jumladan, kiberxavfsizlikning muhim maqsadlari, kiber tahdid turlari, ulardan himoyalanish usullari hamda jamiyatda uning qanday ahamiyat kasb etishi haqidagi batafsil ma’lumotlar berilgan. Shu bilan bir qatorda, maqola so'ngida o'quvchilarga o'z bilimlarini baholash uchun interaktiv testlar ham taqdim qilingan.

Abstract

This article highlights several issues emerging around cybersecurity. It provides detailed information in various areas, including the main objectives of cybersecurity, types of cyber threats, methods of protection against them, and the

ISSN 2181-3187

significance of cybersecurity in society. Additionally, at the end of the article, interactive tests are offered for readers to assess their knowledge.

Аннотация

В данной статье освещаются несколько вопросов, возникающих вокруг кибербезопасности. В ней представлена подробная информация по различным направлениям, включая основные цели кибербезопасности, виды киберугроз, методы защиты от них, а также значимость кибербезопасности в обществе. Кроме того, в конце статьи читателям предлагаются интерактивные тесты для оценки своих знаний.

Kalit so'zlar:

Kiberxavfsizlik, axborot texnologiyalari, raqamli tahdidlar, ma'lumotlarni himoya qilish, kiberhujumlar, axborot xavfsizligi, kiberjinoyatchilik, raqamli infratuzilma, sun'iy intellekt, himoya strategiyalari

Kirish

Bugungi globallashuv hamda raqamli texnologiyalar davrida inson faoliyatining deyarli barcha sohalari internet va zamonaviy axborot texnologiyalariga bog‘liq holda rivojlanmoqda. Internet tarmog‘i orqali ma'lumot almashish, ishlash va bilim olish kundalik hayotimizning ajralmas qismiga aylanib ulgurgan. Ammo raqamli imkoniyatlarning ortishi bilan bir qatorda, turli xil kiberxavflar va tahdidlar ham ko'payib bormoqda. Ayniqsa, shaxsiy va maxfiy ma'lumotlarning o‘g‘irlanishi, ma'lumotlar bazalarining buzilishi kabi holatlar ko‘p uchrayotgan holatlardan biri hisoblanadi. Shu sababli, axborotni himoya qilish va raqamli xavfsizlikni ta'minlash zamonaviy jamiyat uchun nihoyatda muhim masalaga aylangan. Kiberxavfsizlik sohasida ko‘rilayotgan chora-tadbirlar, texnologik innovatsiyalar va huquqiy tizimlarning roli tobora ortib bormoqda.

Kiberxavfsizlikning asosiy jihatlari

ISSN 2181-3187

1. Kiberxavfsizlikning mohiyati va ahamiyati

Kiberxavfsizlik atamasi deb zamonaviy raqamli dunyoda ma'lumotlar va axborot tizimlarini turli tahdidlardan himoya qilishga aytiladi. Bu soha nafaqat shaxsiy va tijorat ma'lumotlarini, balki milliy xavfsizlik, sog‘liqni saqlash tizimi va moliyaviy sektor kabi muhim infratuzilmalarning uzluksiz faoliyatini ta'minlashda ham katta ahamiyatga egadir. Bugungi kunda korxonalar hamda davlat idoralari o‘z ma'lumotlarini himoya qilish maqsadida katta mablag‘ bilan birgalikda resurslarni ham sarflamoqda. Chunki birgina ma'lumotlar sizishi millionlab zarar keltirishi, kompaniya obro‘siga putur yetkazishi yoki undan ham biroz og'ir holatda iqtisodiy tizimni izdan chiqarishi ham mumkin. Shu sababli, kiberxavfsizlik barcha sohalarda ishonch va barqarorlikning asosini yaratadi.

2. Kiberxavfsizlikka tahdid soluvchi asosiy omillar

Kiberxavfsizlikni buzishga qaratilgan tahdidlar soni va shakli yildan-yilga ortib borishi kuzatilmoqda. Eng keng tarqalgan tahdidlarni quyidagilarda ko'rish mumkin:

Fishing va ijtimoiy muhandislik: foydalanuvchilarga soxta elektron pochta xabarlari yoki veb-sahifalar jo'natish orqali shaxsiy ma'lumotlarini firibgarlik yo‘li bilan qo‘lga kiritish.

Zararli dasturlar (malware): viruslar, troyanlar va boshqa zararli dasturlar tizimlarga zarar beradi yoki maxfiy ma'lumotlarni o‘g‘irlaydi.

Tarmoqqa noqonuniy kirish (hacking): tizimdagi zaifliklardan foydalanib, ruxsatsiz kirish va o‘sha ma'lumotlarga aralashish.

Ransomware hujumlari: komputer tizimlarini bloklab, ularni ochish uchun bir oz qiymatda yoki katta pul (ko‘pincha kriptovalyutada) talab qilish.

Bunga qo'shimcha ravishda, ichki tahdidlar — ya'ni tashkilot ichidagi xodimlar tomonidan qasddan yoki ehtiyotsizlik bilan sodir etilgan axborot sizishlari ham katta

ISSN 2181-3187

xavf tug‘diradi. Kiberjinoyatchilar zamonaviy texnologiyalardan foydalanib tobora murakkab va aqlli hujum usullarini ishlab chiqishmoqda.

3. Kiberxavfsizlikni ta'minlash va mustahkamlash yo‘llari

Kiberxavfsizlikni kuchaytirish uchun qator strategik va texnik choralar mavjud:

Ma'lumotlarni shifrlash: barcha muhim ma'lumotlar shifrlanishi, ya'ni maxfiy holda bo'lishi kerak. Bu hujumchilarda ma'lumotdan foydalanish imkonini yo'q qiladi.

Xavfsizlik devorlari (firewalls) va IDS/IPS tizimlari: tarmoqqa beruxsat kirishlarning oldini olish hamda mavjud hujumlarni aniqlash uchun qo‘llaniladi.

Kuchli autentifikatsiya tizimlari: oddiy parollar o‘rniga ikki bosqichli autentifikatsiya yoki biometrik autentifikatsiyadan foydalanish ham xavfsizlikni bir qancha oshiradi.

Xodimlar uchun kiberxavfsizlik bo‘yicha treninglar: aksariyat hujumlar insoniy xatolar natijasida muvaffaqiyatli amalga oshiriladi. Foydalanuvchilarga xavfsizlik madaniyatini singdirish tahdidlarning oldini olishda muhim rol o‘ynaydi.

Zaxira nusxalarini yaratish (backup): tizimlar buzilgan taqdirda ham ma'lumotlarni tezda tiklash imkonini beruvchi muntazam zaxiralash amaliyoti kerak.

Kiberxavfsizlikka sarmoya kiritish nafaqat hozirgi, balki kelajakdagi tahdidlarga qarshi kurashishda ham samara beradigan vositadir.

4. Kiberxavfsizlikning kelajagi va yangi tendensiyalari

Kelajakda kiberxavfsizlik texnologiyalari yanada rivojlanib, murakkab va aqlli tahdidlarni ham aniqlay oladigan tizimlarga aylanishi kutilmoqda. Ayniqsa, quyidagi ba'zi sohalar diqqat markazida bo‘ladi:

ISSN 2181-3187

Sun'iy intellekt (AI) va mashinali o‘rganish (ML): tahdidlarni real vaqt rejimida aniqlash va oldini olish uchun sun'iy intellekt imkoniyatlaridan keng foydalaniladi.

Blokcheyn texnologiyalari: ma'lumotlarning shaffofligini va o‘zgartirilmasligini ta'minlash uchun blokcheyn texnologiyalari keng joriy etilmoqda.

IoT xavfsizligi: aqlli qurilmalar sonining ortishi bilan Internet of Things (IoT) xavfsizligini ta'minlash ustuvor vazifaga aylanmoqda.

Kiberxavfsizlikda xalqaro hamkorlik: davlatlar va yirik korporatsiyalar o‘rtasida axborot almashinuvi va tahdidlarga qarshi birgalikda harakat qilish tendensiyasi kuchaymoqda.

Shuningdek, kiberxavfsizlik sohasida malakali mutaxassislarning yetishmasligi global muammo bo‘lib qolmoqda. Bu esa, kelajakda ushbu sohada bilim va ko‘nikmaga ega bo‘lgan kadrlarga bo‘lgan ehtiyojni yanada oshiradi.

Xulosa

Zamonaviy raqamli dunyoda kiberxavfsizlik har bir shaxs, tashkilot va butun jamiyat uchun ustuvor ahamiyat kasb etmoqda. Raqamli infratuzilmalar kengaygani sayin, ularga tahdid soluvchi xavf-xatarlar ham ortib bormoqda. Bu sharoitda axborotlarni himoya qilish, tizimlarning barqarorligini saqlash va foydalanuvchilarni xabardor qilish muhim vazifaga aylanadi. Kiberxavfsizlikni ta'minlash faqat texnologik yechimlar bilan emas, balki inson omiliga e'tibor qaratish, xavfsizlik madaniyatini shakllantirish orqali ham amalga oshirilishi mumkin.

Kelajakda sun'iy intellekt, mashinali o‘rganish va blokcheyn kabi ilg‘or texnologiyalar kiberxavfsizlik sohasiga yanada katta imkoniyatlar ochishi kutiladi. Shu bilan bir qatorda, kiberjinoyatchilik shakllari ham murakkablashib boradi, bu esa doimiy ravishda yangi himoya strategiyalarini ishlab chiqishni va amalga oshirishni

ISSN 2181-3187

talab etadi. Shunday ekan, axborot texnologiyalari sohasida rivojlanishning ajralmas qismi sifatida kiberxavfsizlikni chuqur o‘rganish va unga doimiy e'tibor qaratish har birimizning muhim vazifamiz hisoblanadi.

O'zingizni sinab ko‘ring!

Quyidagi savollarga javob bering va o‘zingizning kiberxavfsizlik bo‘yicha tayyorgarlik darajangizni baholang:

1. Parollaringiz har bir sayt uchun alohidami va murakkabmi?

2. 2FA (ikki faktorli autentifikatsiya) tizimidan foydalanasizmi?

3. Shubhali havolalarga ehtiyotkorlik bilan yondashasizmi?

4. Muhim fayllaringizni muntazam zaxiralaysizmi?

5. Qurilmalaringizda antivirus dasturlari o‘rnatilganmi?

Natijalar:

4-5 ta "Ha" — Ajoyib! Siz yaxshi himoyalangansiz!

2-3 ta "Ha" — Yaxshi, lekin yanada ehtiyotkorlik zarur.

0-1 ta "Ha" — Kiberxavfsizlik haqida ko‘proq o‘rganishga ehtiyoj bor.

Foydalanilgan adabiyotlar:

1. Stallings, W. (2018). Network Security Essentials: Applications and Standards (6th ed.). Pearson Education.

2. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.

3. Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

ISSN 2181-3187

4. Kaspersky Lab. (2023). The State of Cybersecurity: Trends and Challenges. Rasmiy hisobot.

5. Symantec. (2022). Internet Security Threat Report. Symantec korporatsiyasi nashri.

6. Uzbekistan Respublikasi Prezidentining 2020-yil 15-sentabrdagi PQ-4829-sonli qarori. “Kiberxavfsizlik sohasini rivojlantirish strategiyasi to‘g‘risida”.

7. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity.

8. Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group.