

**KIBERXAVFSIZLIK ZAMONAVIY TAHDIDLAR VA HIMOYA
CHORALARI****КИБЕРБЕЗОПАСНОСТЬ СОВРЕМЕННЫЕ УГРОЗЫ И МЕРЫ
ЗАЩИТЫ****CYBERSECURITY: MODERN THREATS AND PROTECTION MEASURES****Mirzaakbarov Dilshodbek Dovlatboyevich**

*Farg'ona davlat universiteti axborot texnologiyalari
kafedrası o'qituvchisi*

mdilshodbek@mail.ru

<https://orcid.org/0000-0002-5146-0467>

Ibrohimova Irodaxon Abdullajon qizi

Farg'ona davlat universiteti Chet tillari fakulteti

1-bosqich 24.108-guruh talabasi

Annotatsiya

Mazkur maqolada kiberxavfsizlik sohasidagi zamonaviy tahdidlar, ularning turlari, kelib chiqish sabablari hamda bu tahdidlarga qarshi ko'rilayotgan himoya choralari keng yoritilgan. Shu bilan birga, global va mahalliy miqyosda yuzaga kelayotgan xavflarga qarshi kurashishdagi dolzarb yondashuvlar, yuridik va texnologik choralar haqida ma'lumotlar berilgan.

Аннотация

В статье представлен комплексный обзор современных угроз в сфере кибербезопасности, их типов, причин возникновения и мер защиты, принимаемых против этих угроз. При этом предоставляется информация о современных подходах, правовых и технологических мерах по борьбе с возникающими угрозами в глобальном и локальном масштабе.

Abstract

This article provides a comprehensive overview of modern threats in the field of cybersecurity, their types, causes, and protective measures taken against these threats. At the same time, information is provided on current approaches, legal, and technological measures to combat emerging threats on a global and local scale.

Kalit so'zlar. Kiberxavfsizlik, tahdid, zararli dastur, himoya, ma'lumotlar xavfsizligi, kiberhujum, xavfsizlik siyosati.

Ключевые слова. кибербезопасность, угроза, вредоносное ПО, защита, безопасность данных, кибератака, политика безопасности.

Keywords. Cybersecurity, threat, malware, protection, data security, cyberattack, security policy.

KIRISH.

Axborot texnologiyalarining jadal rivojlanishi insoniyat hayotining barcha jabhalariga kirib bordi. Bugungi kunda internet orqali nafaqat muloqot, balki moliyaviy operatsiyalar, davlat boshqaruvi, sog'liqni saqlash, ta'lim va boshqa ko'plab sohalar faoliyat yuritmoqda. Shu sababli, axborotlarning xavfsizligi masalasi dolzarb bo'lib, kiberxavfsizlik eng muhim yo'nalishlardan biriga aylandi.

Kiberxavfsizlik tushunchasi va uning ahamiyati.

Kiberxavfsizlik — bu axborotlarni ruxsatsiz kirish, o'zgartirish yoki yo'q qilishdan himoya qilishga qaratilgan yondashuvlar, vositalar va strategiyalar majmuasidir. Kiberxavfsizlikning asosiy vazifasi — axborot tizimlarining uzluksiz, ishonchli va xavfsiz ishlashini ta'minlashdir. Ahamiyati esa beqiyosdir: u nafaqat shaxsiy ma'lumotlarning, balki davlat sirlarining, tijorat sirlari va moliyaviy resurslarning himoyasini kafolatlaydi.

Zamonaviy kiberxavf tahdidlari.

So'nggi yillarda kiberhujumlar miqyosi va murakkabligi oshib bormoqda. Asosiy tahdidlar quyidagilardan iborat:

- ✧ Zararli dasturlar (malware): viruslar, trojanlar, ransomware va boshqa zararli kodlar orqali tizimlarga hujum qilinadi.
- ✧ Fishing (phishing): yolg'on veb-saytlar yoki e-mail xabarlar orqali foydalanuvchilar shaxsiy ma'lumotlarini ochishga undaladi.
- ✧ DDoS hujumlar: axborot resurslariga ortiqcha so'rov yuborish orqali ularni ishdan chiqarish.
- ✧ Insayder tahdidlari: tashkilot ichidagi xodimlar tomonidan amalga oshiriladigan zararli harakatlar.
- ✧ Zero bunday xatoliklar hali aniqlanmagan yoki yaratilib chiqmagan tizimdagi zaifliklardan foydalaniladi.

Kiberxavfsizlik bo'yicha himoya choralari.

Tahdidlarga qarshi samarali kurashish uchun quyidagi choralar ko'rilishi lozim:

- ✧ Antivirus dasturlari: zararli dasturlarni aniqlash va yo'q qilishda muhim rol o'ynaydi.
- ✧ Firewall tizimlari: tarmoq orqali kiruvchi va chiquvchi axborotni nazorat qilishda foydalaniladi.
- ✧ Shifrlash texnologiyalari: ma'lumotlarni uchinchi shaxslardan himoyalashda ishlatiladi.
- ✧ Xodimlarni o'qitish: kiberxavfsizlik madaniyatini shakllantirish.

- ✧ Zaxira nusxalarini yaratish (backup): muhim axborotlarning yo‘qolishining oldini olish.
- ✧ Kiberxavfsizlik siyosatini ishlab chiqish: tashkilot darajasida qat’iy qoidalar va yondashuvlarni belgilash.

O‘zbekiston va dunyodagi amaliy yondashuvlar.

O‘zbekiston Respublikasi ham kiberxavfsizlik sohasida faol siyosat yuritmoqda. "Kiberxavfsizlik to‘g‘risida"gi qonun, Davlat axborot tizimlari va resurslarini himoyalash tartiblari hamda "Elektron hukumat" tizimi doirasidagi xavfsizlik talablarining kuchaytirilishi bunga misol bo‘la oladi. Dunyo miqyosida esa NATO, Yevropa Ittifoqi, AQSh kabi davlatlar va tashkilotlar global kiberxavfsizlik strategiyalarini ishlab chiqib, xalqaro hamkorlikni rivojlantirmoqda.

Natija va muhokama

Zamonaviy raqamli muhitda kiberxavfsizlik masalasi dolzarb muammolardan biriga aylangan. Tahlillar shuni ko‘rsatadiki, axborot-kommunikatsiya texnologiyalari rivojlangan sari kiberjinoyatchilik va zararli dasturiy ta‘minotlar soni ham ortib bormoqda. Ushbu maqolada ko‘rib chiqilgan zamonaviy tahdidlar — fishing, zararli dasturlar, DDoS hujumlari, ma‘lumotlar sızintisi kabi holatlar — axborot tizimlariga jiddiy xavf tug‘diradi. Shu sababli, samarali himoya choralari sifatida foydalanuvchi xabardorligini oshirish, xavfsizlik siyosatini shakllantirish, zamonaviy antivirus va xavfsizlik protokollaridan foydalanish muhim sanaladi. Shuningdek, xalqaro tajribalardan o‘rganish va milliy kiberxavfsizlik strategiyalarini ishlab chiqish dolzarb ahamiyat kasb etadi. Maqolada yoritilganidek, kiberxavfsizlik bugungi kunda nafaqat texnologik masala, balki ijtimoiy, huquqiy va iqtisodiy omillar bilan chambarchas bog‘liq. Zamonaviy tahdidlar ko‘plab shakllarda namoyon bo‘ladi va ular nafaqat texnik xatoliklardan, balki inson omili, noto‘g‘ri axborot siyosati va yetarlicha muhofaza qilinmagan tizimlardan kelib chiqadi. Muhokama davomida aniqlanishicha, faqatgina texnologik choralari yetarli emas — xavfsizlikni ta‘minlash uchun kompleks yondashuv, jumladan, foydalanuvchilarning axborot savodxonligini oshirish, sohada malakali mutaxassislar tayyorlash, xalqaro hamkorlik va qonunchilikni takomillashtirish zarur. Eng muhimi, bu chora-tadbirlar doimiy rivojlanib borayotgan tahdidlarga mos ravishda yangilanib turilishi lozim.

XULOSA

Siz hozir deyarli har kuni o‘qish va ish uchun foydalanayotgan texnologiya va internet bilan ham xuddi shunday; kiberxavfsizlik bo‘lmasa, sizning shaxsiy ma‘lumotlaringiz, joylashuvingiz, fotosuratlaringiz, kamerangiz va boshqa ko‘p narsalaringiz himoyalangan bo‘lardi va natijada, bu sizning shaxsiy hayotingiz haqidagi muhim ma‘lumotlarni jinoyatchilar uchun tayyor o‘ljaga aylantiradi. Agar

jinoyatchilar bunday ma'lumotlarga kirish imkoniga ega bo'lsa, ular sizning kredit kartalaringizdan foydalanishi, pulingizni o'g'irlashi va hatto shaxsni o'g'irlashi mumkin, Yana bir misol, agar sizda kompyuterlar va ma'lumotlarga tayanadigan shaxsiy biznesingiz bor va siz ushbu kompaniyani qurish uchun juda ko'p mehnat qildingiz. Ammo kiberxavfsizlik bo'lmasa, kompaniyangiz biznesdan chiqib ketishi va bir kechada barcha pul, ma'lumotlar va obro'sini yo'qotishi mumkin. Yuqorida kiberxavfsizlik nima uchun muhim ekanligiga ikkita misol keltirdik. Ammo bugungi virtual hayotimizda bunga juda ko'plab misollar keltirishimiz mumkin. Umuman olganda, biz kiberxavfsizlikni **internetning harbiy qismi** deb o'ylashimiz mumkin. Kiberxavfsizlik – zamonaviy dunyoning ajralmas qismi bo'lib, uning talablariga javob bera olmagan har qanday tashkilot yoki shaxs katta yo'qotishlarga duch kelishi mumkin. Tahdidlarning ko'pligi va murakkabligiga qaramay, ularga qarshi samarali chora-tadbirlar mavjud. Muhimi – ushbu choralarni izchil va to'g'ri qo'llay olishdir.

Adabiyotlar ro'yxati

1. Ахмедов А.Р. Информационная безопасность: учебное пособие. — Ташкент: Университет, 2021.—248с.
2. Qodirov B., Karimov D. Axborot xavfsizligi. — Toshkent: "Fan va texnologiya", 2020.180b.
3. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C.—NewYork:Wiley,2015.—784p.
4. Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec inTheory,and,Practice.—Elsevier,2019.—208p.
5. O'zbekiston Respublikasi Prezidentining 2020 yil 5 oktyabrdagi PQ-4851-son qarori "Kiberxavfsizlik sohasini yanada rivojlantirishchora-tadbirlarito'g'risida".
6. Dovlatboyevich, D. M., & Komiljonovna, M. M. (2022). Oliy Ta'lim Muassasalarida Bulutli Texnologiyalardan Foydalanish Metodikasi. Miasto Przyszłości, 29, 305-308.
7. B.Mo'minov. Informatika. O'quv qo'llanma T.: "Tafakkur bo'stoni", 2014 y.
8. Mirzaakbarov, D.D. (2021). DIREKTIONS for the introduction of new information technologies in education. Экономика и социум, 4(83).
9. Muzaffarxonov Saida'loxon, Mirzaakbarov Dilshodbek Dovlatboyevich "Sun'uy Intelekt Yordamida Pochta Xizmatini Tashkil Qilish" Miasto Przyszłości Kielce 2023.