

YANGI O'ZBEKISTON: FANLARARO TADQIQOTLAR MAYDONI

respublika ilmiy-nazariy konferensiya

KIBER XAVFSIZLIK: ZAMONAVIY AXBOROT MUHITIDA MUAMMOLAR VA YECHIMLAR

Damirova Kamola Mirshod qizi,

Samarqand davlat chet tillar instituti 1-bosqich talabasi

Boboqulov Sherzod Sherqulovich,

Samarqand davlat chet tillar instituti o'qituvchisi

Abstract. Ushbu maqolada kiber xavfsizlikning zamonaviy jamiyatdagi o'rni, uning asosiy muammolari va ularni bartaraf etish yo'llari chuqur tahlil qilinadi. Axborot texnologiyalarining jadal rivojlanishi natijasida inson faoliyatining deyarli barcha sohaları raqamlashtirilmoqda. Shu bilan birga, kiber tahdidlar soni, murakkabligi va xavfi ham ortib bormoqda.

Tadqiqot davomida kiber hujumlarning asosiy turlari, jumladan viruslar, zararli dasturlar, fishing hujumlari va DDoS hujumlari o'rganildi. Shuningdek, foydalanuvchilarning xavfsizlikka nisbatan e'tiborsizligi, bilim darajasining pastligi va texnik zaifliklar asosiy muammolar sifatida aniqlandi.

Natijalar shuni ko'rsatadiki, samarali kiber xavfsizlikni ta'minlash uchun nafaqat zamonaviy texnik vositalar, balki foydalanuvchilarning axborot madaniyatini oshirish, ularni muntazam o'qitish va profilaktik choralarni kuchaytirish zarur. Mazkur maqola kiber xavfsizlikni mustahkamlash bo'yicha kompleks yondashuvni taklif etadi.

Introduction. Bugungi kunda axborot texnologiyalari inson hayotining ajralmas qismiga aylangan. Internet, mobil qurilmalar, bulutli texnologiyalar va raqamli platformalar yordamida kundalik faoliyatimizni samarali tashkil etmoqdamiz. Ta'lim, sog'liqni saqlash, bank tizimi, davlat boshqaruvi va biznes jarayonlari tobora ko'proq raqamli muhitga ko'chmoqda. Biroq ushbu jarayon bilan birga kiber xavfsizlik muammolari ham dolzarb tus olmoqda. Kiber xavfsizlik — bu axborot tizimlari, tarmoqlar va ma'lumotlarni noqonuniy kirish, buzilish, o'g'irlash yoki yo'q qilishdan himoya qilishga qaratilgan chora-tadbirlar majmuasidir.

Kiber tahdidlar turli ko'rinishda namoyon bo'ladi: viruslar, trojan dasturlar, ransomware, fishing hujumlari, DDoS hujumlari va boshqa zararli faoliyatlar. Ayniqsa, so'nggi yillarda sun'iy intellekt va avtomatlashtirilgan vositalardan foydalanib amalga oshirilayotgan hujumlar yanada murakkablashmoqda.

Shu sababli, kiber xavfsizlik masalasi nafaqat texnik, balki ijtimoiy, iqtisodiy va hatto siyosiy muammoga aylanib bormoqda. Mazkur maqolaning asosiy maqsadi kiber xavfsizlik sohasidagi mavjud muammolarni aniqlash, ularni tahlil qilish hamda samarali yechimlarni ishlab chiqishdan iborat.

Methods. Mazkur tadqiqotda ilmiy izlanishlarning bir nechta usullari qo'llanildi:

1. Tahliliy usul. Kiber xavfsizlik sohasiga oid ilmiy maqolalar, xalqaro hisobotlar va statistik ma'lumotlar o'rganildi. Ushbu manbalar asosida muammoning nazariy asoslari shakllantirildi.

2. Taqqoslash usuli. Turli xil kiber tahdidlar va ularga qarshi kurashish usullari solishtirildi. Masalan, antivirus dasturlari, firewall tizimlari va foydalanuvchi xulq-atvoriga asoslangan himoya usullari o'zaro tahlil qilindi.

3. Statistik tahlil. Kiber hujumlar soni, ularning iqtisodiy zarar darajasi va keng tarqalgan turlari bo'yicha mavjud statistik ma'lumotlar tahlil qilindi. Bu esa muammoning dolzarbligini aniqlash imkonini berdi.

4. Amaliy holatlarni o'rganish. Real hayotdagi kiber hujumlar :misollari o'rganilib, ularning sabab va oqibatlari chuqur tahlil qilindi. Bu orqali amaliy xulosalar chiqarildi.

Findings and Discussion. Tadqiqot natijalari shuni ko'rsatdiki, zamonaviy kiber tahdidlar tobora murakkablashib, keng ko'lamlı zarar yetkazish imkoniyatiga ega bo'lib bormoqda. Eng keng tarqalgan tahdidlar

YANGI O'ZBEKISTON: FANLARARO TADQIQOTLAR MAYDONI

respublika ilmiy-nazariy konferensiya

qatoriga zararli dasturlar (malware), fishing hujumlari va ransomware kiradi. Ayniqsa, fishing hujumlari orqali foydalanuvchilarning shaxsiy ma'lumotlarini qo'lga kiritish holatlari keskin ortgan.

Tahlillar shuni ko'rsatadiki, kiber hujumlarning katta qismi inson omili bilan bog'liq. Ya'ni, foydalanuvchilar tomonidan oddiy xavfsizlik qoidalariga amal qilinmasligi — kuchsiz parollardan foydalanish, noma'lum havolalarni ochish, shubhali fayllarni yuklab olish kabi holatlar asosiy zaiflik sifatida namoyon bo'lmoqda. Bundan tashqari, ko'plab tashkilotlarda zamonaviy xavfsizlik tizimlarining yetarli darajada joriy etilmagani ham muammoni yanada kuchaytiradi. Kichik va o'rta biznes subyektlari ko'pincha kiber xavfsizlikka yetarli mablag' ajratmaydi, bu esa ularni oson nishonga aylantiradi. Shu bilan birga, tadqiqot natijalari shuni ko'rsatadiki, samarali himoya faqat texnik vositalar bilan cheklanib qolmasligi kerak. Quyidagi choralar muhim ahamiyatga ega:

- Kuchli va murakkab parollardan foydalanish
- Ikki bosqichli autentifikatsiyani (2FA) joriy etish
- Dasturiy ta'minotni muntazam yangilab borish
- Foydalanuvchilarni kiber xavfsizlik bo'yicha o'qitish
- Tarmoqlarda monitoring va nazoratni kuchaytirish

Yana bir muhim jihat — davlat darajasida kiber xavfsizlik siyosatini rivojlantirish zarurati. Qonunchilikni takomillashtirish, maxsus kiber xavfsizlik markazlarini tashkil etish va xalqaro hamkorlikni rivojlantirish muhim yo'nalishlardan biridir.

Umuman olganda, kiber xavfsizlik masalasi kompleks yondashuvni talab qiladi. Texnik, tashkiliy va inson omillarini birgalikda hisobga olgan holda amalga oshirilgan chora-tadbirlar eng samarali natija beradi. **Conclusion.** Ushbu tadqiqot natijalari shuni ko'rsatdiki, kiber xavfsizlik zamonaviy axborot jamiyatining eng muhim va dolzarb muammolaridan biri hisoblanadi. Axborot texnologiyalarining jadal rivojlanishi inson hayotini sezilarli darajada yengillashtirgan bo'lsa-da, shu bilan birga turli kiber tahdidlar xavfini ham oshirmoqda. Maqola davomida kiber tahdidlarning asosiy turlari, ularning kelib chiqish sabablari va oqibatlari tahlil qilindi. Tadqiqot natijalariga ko'ra, kiber hujumlarning katta qismi inson omili bilan bog'liq bo'lib, foydalanuvchilarning axborot xavfsizligi bo'yicha bilim darajasining yetarli emasligi asosiy zaifliklardan biri ekanligi aniqlandi. Shuningdek, faqat texnik vositalar bilan cheklanib qolish yetarli emasligi, balki kompleks yondashuv zarurligi ta'kidlandi. Kuchli parollar, ikki bosqichli autentifikatsiya, muntazam yangilanishlar va tarmoq monitoringi kabi choralar bilan bir qatorda, foydalanuvchilarning axborot madaniyatini oshirish ham muhim ahamiyatga ega. Kelajakda kiber xavfsizlikni ta'minlash uchun davlat darajasida siyosatni kuchaytirish, xalqaro hamkorlikni rivojlantirish va innovatsion texnologiyalarni joriy etish zarur. Umuman olganda, kiber xavfsizlikni ta'minlash uzluksiz jarayon bo'lib, u doimiy e'tibor va takomillashtirishni talab qiladi.

References:

1. Stallings, W. (2018). *Cybersecurity Essentials*. Pearson Education.
2. Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach*. Pearson.
3. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
4. Whitman, M. E., & Mattord, H. J. (2019). *Principles of Information Security*. Cengage Learning.
5. ENISA (European Union Agency for Cybersecurity). (2023). *Threat Landscape Report*.
6. ISO/IEC 27001:2022. *Information Security Management Systems – Requirements*.
7. Verizon. (2024). *Data Breach Investigations Report (DBIR)*.
8. Symantec Corporation. (2023). *Internet Security Threat Report*.
9. O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi materiallari.
10. NIST (National Institute of Standards and Technology). (2022). *Cybersecurity Framework*.