KIBERXAVFSIZLIK MUAMMOLARI VA ULARNING YECHIMLARI

Andijon Davlat chet tillari instituti
Nizomidinova Bibixojar Sirojidin qizi
Ilmiy maslahatchi: ***Orziqulova Z***

Annotatsiya: Ushbu maqolada zamonaviy axborotlashgan jamiyatda kiberxavfsizlik muammolari, ularning kelib chiqish sabablari va global miqyosdagi tahdidlari tahlil qilinadi. Shuningdek, kiberjinoyatchilik turlari, axborot tizimlarining zaifliklari hamda ularni bartaraf etish bo‘yicha samarali yechimlar ko‘rib chiqiladi. Tadqiqot natijalariga asoslanib, davlat, tashkilot va shaxs darajasida qo‘llanilishi mumkin bo‘lgan xavfsizlik choralariga alohida e’tibor qaratilgan.

Kalit so‘zlar: kiberxavfsizlik, axborot xavfsizligi, kiberhujum, zararli dasturlar, ma’lumotlar himoyasi, tarmoq xavfsizligi, autentifikatsiya, shifrlash

Аннотация: В данной статье рассматриваются актуальные проблемы кибербезопасности в условиях современного информационного общества, а также анализируются причины их возникновения и угрозы глобального масштаба. В рамках исследования проведён комплексный анализ основных видов киберпреступности, выявлены уязвимости информационных систем и определены факторы, способствующие их возникновению. Особое внимание уделено разработке и обоснованию эффективных мер по обеспечению кибербезопасности, включая технические, организационные и правовые подходы. На основе полученных результатов предложены практические рекомендации по повышению уровня защиты информации на государственном, организационном и индивидуальном уровнях.

Ключевые слова: кибербезопасность, информационная безопасность, кибератаки, вредоносное программное обеспечение, защита данных, сетевая безопасность, аутентификация, шифрование, киберпреступность

Abstract: This article examines cybersecurity challenges in the context of the modern information society, including their underlying causes and global-scale threats. The study analyzes the main types of cybercrime, identifies vulnerabilities in information systems, and explores effective approaches to their mitigation. Based on the research findings, particular emphasis is placed on security measures that can be implemented at the governmental, organizational, and individual levels.

Keywords: cybersecurity, information security, cyberattacks, malware, data protection, network security, authentication, encryption

Bugungi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha sohalarini qamrab olmoqda. Internet, mobil qurilmalar va

raqamli xizmatlarning keng tarqalishi inson faoliyatini sezilarli darajada osonlashtirdi. Biroq bu jarayon bilan birga yangi xavf-xatarlar — kiberxavfsizlik muammolari ham yuzaga keldi.

Kiberxavfsizlik — bu axborot tizimlari, tarmoqlar va ma’lumotlarni ruxsatsiz kirish, buzish yoki yo‘q qilishdan himoya qilishga qaratilgan chora-tadbirlar majmuasidir. So‘nggi yillarda kiberhujumlar soni va murakkabligi ortib borayotgani ushbu sohaning dolzarbligini yanada oshirmoqda.

Mazkur maqolaning maqsadi kiberxavfsizlik sohasidagi asosiy muammolarni tahlil qilish hamda ularni bartaraf etishning samarali usullarini ilmiy asosda yoritishdan iborat.

Kiberxavfsizlik tushunchasi axborot xavfsizligining muhim tarkibiy qismi bo‘lib, u kompyuter tizimlari, tarmoqlar va raqamli ma’lumotlarni himoya qilishni o‘z ichiga oladi. Zamonaviy iqtisodiyot va boshqaruv tizimlari bevosita axborot texnologiyalariga bog‘liq bo‘lib qolganligi sababli, ularning ishonchliligi kiberxavfsizlik darajasiga chambarchas bog‘liqdir. Kiberxavfsizlikning ahamiyati quyidagilar bilan izohlanadi: maxfiy ma’lumotlarni himoya qilish; moliyaviy yo‘qotishlarning oldini olish; davlat xavfsizligini ta’minlash; tashkilotlar obro‘sini saqlash. Kiberhujumlarning ko‘payishi. So‘nggi yillarda kiberhujumlar soni keskin ortib bormoqda. Xakerlar turli usullar orqali tizimlarga kirib borib, ma’lumotlarni o‘g‘irlash yoki yo‘q qilishga harakat qilmoqda. Zararli dasturlar (malware): Zararli dasturlar — viruslar, trojanlar, ransomware kabi vositalar orqali tizimlarga zarar yetkaziladi. Ayniqsa, ransomware hujumlari tashkilotlar uchun katta xavf tug‘diradi.
Foydalanuvchi xatolari: Ko‘plab kiberhujumlar inson omili bilan bog‘liq. Kuchsiz parollar, shubhali havolalarga bosish va xavfsizlik qoidalariga rioya qilmaslik asosiy sabablar sirasiga kiradi. Tarmoq zaifliklari: Dasturiy ta’minotdagi xatoliklar va yangilanishlarning o‘z vaqtida o‘rnatilmasligi tizimlarni himoyasiz qoldiradi.
IoT qurilmalar xavfsizligi: Internetga ulangan qurilmalar (IoT) ko‘pincha yetarli darajada himoyalanmagan bo‘ladi va bu ularni hujumlar uchun oson nishonga aylantiradi. Kiberxavfsizlik tahdidlarining turlari: Phishing — foydalanuvchini aldash orqali ma’lumotlarini qo‘lga kiritish; DDoS hujumlar — serverlarni ortiqcha yuklama bilan ishdan chiqarish; Man-in-the-middle — ma’lumot uzatishda aralashish; SQL injection — ma’lumotlar bazasiga noqonuniy kirish; Zero-day hujumlar — hali aniqlanmagan zaifliklardan foydalanish. Kiberxavfsizlikni ta’minlash usullari: Texnik choralar; Kuchli shifrlash algoritmlaridan foydalanish; Antivirus va firewall tizimlarini joriy etish; Tizimlarni muntazam yangilab borish; Ikki bosqichli autentifikatsiyani qo‘llash. Tashkiliy choralar: Xodimlarni muntazam o‘qitish; Axborot xavfsizligi siyosatini ishlab chiqish; Risklarni baholash va monitoring qilish. Huquqiy choralar: Kiberjinoyatchilikka qarshi qonunchilikni kuchaytirish; Ma’lumotlarni himoya qilish bo‘yicha normativ hujjatlarni takomillashtirish.

Sun’iy intellekt va mashinaviy o‘rganish texnologiyalari kiberxavfsizlikni ta’minlashda muhim rol o‘ynamoqda. Ushbu texnologiyalar orqali tahdidlarni oldindan aniqlash va tezkor javob berish imkoniyati yaratilmoqda. Blockchain texnologiyasi esa ma’lumotlarni o‘zgarmas shaklda saqlash orqali xavfsizlikni oshiradi. Kelajakda kiberxavfsizlik quyidagi yo‘nalishlarda rivojlanadi: avtomatlashtirilgan himoya tizimlari; global kiberxavfsizlik hamkorligi; kvant kriptografiyasi; kiberxavfsizlik mutaxassislariga bo‘lgan talabning ortishi.

Xulosa qilib aytganda, kiberxavfsizlik zamonaviy jamiyatning ajralmas qismi hisoblanadi. Axborot texnologiyalarining rivojlanishi bilan bog‘liq xavf-xatarlar ham ortib bormoqda. Shu sababli, kiberxavfsizlikni ta’minlash kompleks yondashuvni talab etadi. Davlat, tashkilot va individual foydalanuvchilar o‘z darajasida zarur choralarni ko‘rishi lozim. Faqatgina texnik vositalar emas, balki inson omili va huquqiy asoslar ham muhim ahamiyat kasb etadi.

Foydalanilgan adabiyotlar

1. Stallings W.
   Network Security Essentials: Applications and Standards. 6th ed. – Pearson, 2020. – 464 p.
   (Kiberhujumlar, shifrlash, autentifikatsiya: 35–78-betlar)
2. Whitman M. E., Mattord H. J.
   Principles of Information Security. 6th ed. –Cengage Learning, 2021.656 p.
3. (Kiberxavfsizlik muammolari va risklar: 50–95-betlar)
   ISO/IEC 27001:2022
   Information Security Management Systems – Requirements. – ISO, 2022.
4. (Axborot xavfsizligi siyosati va boshqaruvi: 10–25-betlar)
   Kurose J. F., Ross K. W.
   Computer Networking: A Top-Down Approach. –8th ed. Pearson, 2021. – 864 p.
   (Tarmoq xavfsizligi va DDoS: 720–760-betlar)
5. Anderson R.
   Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. – Wiley, 2020. – 1232 p. (Kiberjinoyatchilik va tizim zaifliklari: 120–180-betlar)
6. ENISA (European Union Agency for Cybersecurity)
   Threat Landscape Report 2023.
   (Zamonaviy tahdidlar, ransomware: 15–40-betlar)
   NIST (National Institute of Standards and Technology)
   Cybersecurity Framework (CSF) 2.0. – 2024.
   (Risk boshqaruvi va himoya choralar: 20–55-betlar)