# KIBERXAVFSIZLIKDAGI DOLZARB MUAMMOLAR VA ULARNING YECHIMLARI

**Kodirov Akbar Shuxratovich**
*Shahrisabz davlat pedagogika instituti*
*“Matematika va amaliy matematika” kafedrasi Katta o'qituvchisi*
*E-mail: akbar2005ak@gmail.com*
*ORSID: 0000-0002-3656-5770*
**Nurmaxmatova Saida Alisher qizi**
*Shahrisabiz davlat pedagogika instituti*
*Matematika va informatika yo’nalishi talabasi*
*E-mail: saidanurmaxmatova356@gmail.com*

**Annotatsiya**. *Ushbu maqolada kiberxavfsizlik sohasidagi dolzarb muammolar, ularning kelib chiqish sabablari hamda yechimlari haqida batafsil so‘z yuritiladi. Maqolada kiberjinoyatchilik, fishing hujumlari, zararli dasturlar, shaxsiy ma’lumotlarning o‘g‘irlanishi va ijtimoiy tarmoqlardagi xavflar tahlil qilingan. Shuningdek, axborot xavfsizligini ta’minlash yo‘llari, zamonaviy himoya tizimlari va foydalanuvchilarning internet madaniyatini oshirish masalalari yoritilgan. Kiberxavfsizlikni mustahkamlash jamiyat va davlat taraqqiyoti uchun muhim omillardan biri ekanligi ta’kidlangan.*

**Kalit so‘zlar**: *kiberxavfsizlik, axborot xavfsizligi, kiberjinoyatchilik, fishing, zararli dasturlar, internet xavfsizligi, shaxsiy ma’lumotlar, viruslar, axborot texnologiyalari.*

**Annotation** *This article discusses current cybersecurity issues, their causes, and possible solutions in detail. The article analyzes cybercrime, phishing attacks, malicious software, theft of personal data, and threats in social networks. It also highlights methods of ensuring information security, modern protection systems, and improving users’ digital literacy. The importance of strengthening cybersecurity as a key factor in the development of society and the state is emphasized.*

**Keywords**: *cybersecurity, information security, cybercrime, phishing, malicious software, internet security, personal data, viruses, information technologies.*

**Аннотация** *В данной статье подробно рассматриваются актуальные проблемы кибербезопасности, причины их возникновения и пути решения. В статье анализируются киберпреступность, фишинговые атаки, вредоносные программы, кража персональных данных и угрозы в социальных сетях. Также освещаются вопросы обеспечения информационной безопасности, современные системы защиты и повышение интернет-культуры пользователей. Подчеркивается, что укрепление кибербезопасности является одним из важных факторов развития общества и государства.*

**Ключевые слова**: *кибербезопасность, информационная безопасность, киберпреступность, фишинг, вредоносные программы, интернет-безопасность, персональные данные, вирусы, информационные технологии.*

**KIRISH**

Bugungi kunda insoniyat hayotini internet va axborot texnologiyalarisiz tasavvur qilish juda qiyin. Chunki zamonaviy dunyoda deyarli barcha sohalar raqamli tizimlar orqali boshqarilmoqda. Insonlar kundalik hayotida internetdan foydalanib ta’lim olmoqda, ishlamoqda, savdo qilmoqda, muloqot qilmoqda va turli xizmatlardan foydalanmoqda. Hozirda bank tizimlari, davlat xizmatlari, tibbiyot, transport, ta’lim va ishlab chiqarish jarayonlari ham kompyuter texnologiyalariga bog‘liq bo‘lib qolgan. Bu esa inson hayotini ancha qulaylashtirdi va vaqtni tejash imkonini yaratdi. Ammo texnologiyalar rivojlanishi bilan bir qatorda yangi tahdid va xavf-xatarlar ham yuzaga kelmoqda. Ayniqsa, kiberxavfsizlik masalasi bugungi kunning eng dolzarb muammolaridan biri sifatida namoyon bo‘lmoqda. Chunki internet orqali amalga oshirilayotgan jinoyatlar soni yil sayin ortib bormoqda. Turli xil xakerlik hujumlari, shaxsiy ma’lumotlarni o‘g‘irlash, internet firibgarligi, zararli dasturlar va soxta axborotlar jamiyat xavfsizligiga jiddiy tahdid tug‘dirmoqda. Kiberxavfsizlik deganda kompyuter tizimlari, internet tarmoqlari, serverlar, mobil qurilmalar va ma’lumotlarni noqonuniy kirish, buzish yoki yo‘q qilishdan himoya qilish tushuniladi. Kiberxavfsizlikning asosiy maqsadi axborotlarning maxfiyligi, yaxlitligi va ishonchliligini saqlashdan iboratdir. Hozirgi davrda axborot eng qimmat boyliklardan biri hisoblanadi. Shu sababli axborotni himoya qilish har bir davlat va jamiyat uchun ustuvor vazifaga aylangan.

Kiberxavfsizlikning ahamiyati kundan-kunga ortib bormoqda. Sababi insonlar internetga tobora ko‘proq bog‘lanib bormoqda. Hozir oddiy inson ham internet orqali bank xizmatlaridan foydalanadi, pul o‘tkazmalarini amalga oshiradi yoki muhim hujjatlarni elektron shaklda yuboradi. Agar internet tizimlari yaxshi himoyalanmagan bo‘lsa, foydalanuvchilarning shaxsiy ma’lumotlari o‘g‘irlanishi yoki katta moliyaviy zarar yuzaga kelishi mumkin. Masalan, biror inson internet banking xizmatidan foydalanganda uning karta ma’lumotlari firibgarlar qo‘liga tushib qolsa, hisobidagi pullar o‘g‘irlanadi. Yoki davlat tashkilotlari tizimlariga hujum qilinsa, muhim ma’lumotlar yo‘qolishi mumkin. Bu esa nafaqat iqtisodiy, balki siyosiy va ijtimoiy muammolarni ham keltirib chiqaradi. Shu sababli bugungi kunda barcha davlatlar kiberxavfsizlik tizimini kuchaytirishga alohida e’tibor qaratmoqda. Chunki zamonaviy urushlar faqat qurol bilan emas, balki axborot va texnologiyalar orqali ham olib borilmoqda.

Kiberxavfsizlikdagi asosiy dolzarb muammolar. Kiberjinoyatchilikning kuchayishi Hozirgi kunda eng katta muammolardan biri bu kiberjinoyatchilikning keskin rivojlanayotganidir. Xakerlar turli zararli dasturlar va maxsus texnologiyalar yordamida tashkilotlarning axborot tizimlariga noqonuniy kirib bormoqda. Ularning asosiy maqsadi moliyaviy foyda olish, maxfiy ma’lumotlarni qo‘lga kiritish yoki tizim faoliyatini izdan chiqarishdan iborat. Masalan, ayrim xakerlar bank tizimlariga hujum qilib, millionlab dollar mablag‘larni o‘g‘irlashga harakat qiladi. Yirik kompaniyalarning serverlari buzilib, maxfiy

hujjatlar internetga tarqalib ketgan holatlar ham ko‘p uchramoqda. Ba’zi hollarda esa xakerlar davlat tashkilotlariga hujum qilib, siyosiy maqsadlarni ko‘zlaydi. Kiberjinoyatchilikning xavfli tomoni shundaki, jinoyatchilar dunyoning istalgan nuqtasidan turib hujum uyushtirishi mumkin. Ularni aniqlash va javobgarlikka tortish esa juda murakkab jarayon hisoblanadi.

Shaxsiy ma’lumotlarning o‘g‘irlanishi Bugungi kunda foydalanuvchilarning shaxsiy ma’lumotlari eng qimmat resurslardan biriga aylangan. Internet foydalanuvchilari ko‘pincha o‘z ma’lumotlariga e’tiborsiz qaraydi. Oddiy parollardan foydalanish, noma’lum havolalarga kirish yoki ijtimoiy tarmoqlarda ortiqcha ma’lumot joylashtirish natijasida shaxsiy axborotlar firibgarlar qo‘liga tushib qolmoqda. Masalan, ayrim insonlar tug‘ilgan sanasi yoki telefon raqamini parol sifatida ishlatadi. Bunday parollarni topish juda oson bo‘lgani sababli xakerlar akkauntlarni tez buzadi. Natijada foydalanuvchilarning elektron pochtasi, bank kartalari yoki ijtimoiy tarmoqdagi sahifalari nazoratdan chiqadi. Bundan tashqari, internetdagi ayrim saytlar foydalanuvchilar ma’lumotlarini yashirin ravishda yig‘ib, boshqa tashkilotlarga sotishi mumkin. Bu esa shaxsiy hayot daxlsizligiga jiddiy tahdid hisoblanadi.

Fishing va internet firibgarligi. Fishing internetdagi eng keng tarqalgan firibgarlik usullaridan biridir. Unda foydalanuvchilar aldov yo‘li bilan o‘z ma’lumotlarini firibgarlarga topshirib qo‘yadi. Ko‘pincha firibgarlar bank yoki mashhur sayt nomidan soxta xabar yuboradi. Masalan, foydalanuvchiga “Kartangiz bloklandi” degan SMS keladi va havola orqali ma’lumotlarini tasdiqlash so‘raladi. Aslida esa bu xabar firibgarlar tomonidan yuborilgan bo‘ladi. Foydalanuvchi karta raqami va parolini kiritishi bilan pullari o‘g‘irlanadi.

Yana bir misol sifatida “Siz avtomobil yutdingiz” yoki “Sovrin qo‘lga kiritdingiz” kabi yolg‘on reklama va havolalarni aytish mumkin. Ko‘plab insonlar bunga ishonib, shaxsiy ma’lumotlarini firibgarlarga topshiradi.

Virus va zararli dasturlar. Kompyuter viruslari va zararli dasturlar ham kiberxavfsizlikdagi eng xavfli tahdidlardan biridir. Viruslar kompyuter tizimiga kirib, ma’lumotlarni o‘chirishi, fayllarni bloklashi yoki foydalanuvchi ustidan yashirin nazorat o‘rnatishi mumkin. Masalan, ransomware deb ataluvchi virus foydalanuvchining barcha fayllarini shifrlab qo‘yadi va ularni qayta tiklash uchun pul talab qiladi. Agar foydalanuvchi to‘lov qilmasa, muhim hujjatlar butunlay yo‘qolishi mumkin. Ba’zan zararli dasturlar oddiy mobil ilovalar orqali ham tarqaladi. Foydalanuvchi noma’lum ilovani yuklab olgach, telefonidagi ma’lumotlar yashirin ravishda boshqa shaxslarga yuborilishi mumkin.

Ijtimoiy tarmoqlardagi xavflar. Bugungi kunda millionlab insonlar ijtimoiy tarmoqlardan foydalanadi. Ammo bu platformalarda ham ko‘plab xavf-xatarlar mavjud. Soxta akkauntlar, yolg‘on ma’lumotlar va internet orqali tahdid qilish holatlari tobora ortib bormoqda. Masalan, ayrim firibgarlar mashhur inson nomidan sahifa ochib, odamlardan pul yig‘ishga urinadi. Yoki yoshlarni aldab, turli noqonuniy ishlarga jalb qiladi. Ayrim hollarda esa foydalanuvchilarning shaxsiy suratlari yoki yozishmalari noqonuniy tarqatiladi. Ijtimoiy tarmoqlardagi yana bir katta muammo bu yolg‘on axborotlarning tez tarqalishidir. Bunday ma’lumotlar jamiyatda vahima va tushunmovchiliklarni yuzaga keltirishi mumkin.

Sun’iy intellekt bilan bog‘liq xavflar. Sun’iy intellekt texnologiyalari insoniyat uchun katta imkoniyatlar yaratmoqda. Ammo undan noto‘g‘ri maqsadlarda foydalanish xavfi ham mavjud. Hozirda ayrim xakerlar sun’iy intellekt yordamida murakkab kiberhujumlar uyushtirmoqda. Masalan, deepfake texnologiyasi yordamida insonlarning soxta video va ovozlari yaratilmoqda. Bu esa odamlarni aldash yoki obro‘siga putur yetkazish uchun ishlatilishi mumkin. Kelajakda sun’iy intellekt asosidagi avtomatik xakerlik dasturlari paydo bo‘lishi ehtimoli ham mavjud. Shu sababli bu texnologiyalarni nazorat qilish juda muhim.

Kiberxavfsizlikni ta’minlash uchun zamonaviy antivirus dasturlari va himoya tizimlaridan foydalanish zarur. Har bir tashkilot o‘z serverlari va ma’lumotlar bazasini kuchli himoya qilishi kerak. Masalan, firewall tizimlari zararli trafikni bloklaydi, antivirus dasturlari esa viruslarni aniqlab yo‘q qiladi. Bundan tashqari, ma’lumotlarni shifrlash texnologiyalari ham axborotni himoya qilishda katta rol o‘ynaydi.

Murakkab parollardan foydalanish. Ko‘plab kiberhujumlar oddiy parollar sababli sodir bo‘ladi. Shu sababli foydalanuvchilar murakkab va uzun parollardan foydalanishi kerak. Parollarda harflar, raqamlar va maxsus belgilar aralash bo‘lishi xavfsizlikni oshiradi.

Masalan, “12345” yoki “password” kabi oddiy parollarni buzish juda oson. Ammo murakkab parollar xakerlar ishini ancha qiyinlashtiradi.

Internet madaniyatini oshirish Kiberxavfsizlikni ta’minlashda inson omili juda muhim hisoblanadi. Har bir foydalanuvchi internet xavfsizligi qoidalarini bilishi kerak. Noma’lum havolalarga kirmaslik, shaxsiy ma’lumotlarni begonalarga bermaslik va internetdagi har bir ma’lumotga ishonib ketmaslik zarur. Shu sababli maktab va universitetlarda kiberxavfsizlik bo‘yicha darslar tashkil etilishi katta ahamiyatga ega.

Kiberxavfsizlik muammolarining yechimlari. Kiberxavfsizlik sohasidagi muammolarni bartaraf etish kompleks yondashuvni talab qiladi. Bu nafaqat texnik himoya vositalarini, balki foydalanuvchilarning ongini oshirish va davlat darajasidagi chora-tadbirlarni ham o‘z ichiga oladi. Birinchi navbatda, texnik himoya tizimlarini rivojlantirish muhim hisoblanadi. Tashkilotlar va individual foydalanuvchilar zamonaviy antivirus dasturlari, firewall tizimlari hamda intrusion detection system (IDS) kabi texnologiyalardan foydalanishi kerak. Ushbu vositalar zararli faoliyatni erta aniqlash va uni oldini olish imkonini beradi. Shuningdek, ma’lumotlarni shifrlash (encryption) texnologiyalari axborotning maxfiyligini ta’minlashda muhim rol o‘ynaydi.

Ikkinchi muhim yo‘nalish — foydalanuvchilarning raqamli savodxonligini oshirishdir. Ko‘plab kiberhujumlar inson xatosi sababli sodir bo‘ladi. Shu sababli odamlar shubhali havolalarni ochmaslik, noma’lum fayllarni yuklab olmaslik va shaxsiy ma’lumotlarni begonalarga bermaslik kabi asosiy xavfsizlik qoidalarini bilishi zarur. Ta’lim muassasalarida kiberxavfsizlik bo‘yicha maxsus kurslar va treninglar joriy etilishi bu muammoni sezilarli darajada kamaytiradi.

Uchinchi yo‘nalish — kuchli autentifikatsiya tizimlarini joriy etishdir. Oddiy parollar o‘rniga murakkab parollar, ikki bosqichli autentifikatsiya (2FA) va biometrik tizimlardan foydalanish kiberhujumlarning oldini olishda samarali hisoblanadi. Bu usullar foydalanuvchi akkauntlariga ruxsatsiz kirishni qiyinlashtiradi.

To‘rtinchi muhim yechim — ma’lumotlarni muntazam zaxiralash (backup) hisoblanadi. Zararli dasturlar yoki texnik nosozliklar natijasida ma’lumotlar yo‘qolishi mumkin. Agar foydalanuvchi yoki tashkilotda doimiy backup tizimi mavjud bo‘lsa, yo‘qolgan ma’lumotlarni tezda tiklash imkoni bo‘ladi.

**Beshinchi yo‘nalish** — qonunchilikni takomillashtirish va xalqaro hamkorlikni kuchaytirishdir. Kiberjinoyatchilik global xarakterga ega bo‘lgani uchun davlatlar o‘rtasida axborot almashinuvi va hamkorlik juda muhim. Kiberjinoyatchilarni aniqlash va jazolash tizimi kuchli bo‘lsa, bunday jinoyatlar soni kamayadi.

Shuningdek, sun’iy intellekt asosida ishlovchi himoya tizimlarini rivojlantirish ham zamonaviy yechimlardan biridir. AI texnologiyalari shubhali faoliyatni tez aniqlash va avtomatik ravishda bloklash imkonini beradi.

Qonunchilikni kuchaytirish. Davlat tomonidan kiberjinoyatlarga qarshi qat’iy qonunlar ishlab chiqilishi zarur. Chunki internet orqali sodir etilayotgan jinoyatlar soni tobora ortmoqda.

Kiberjinoyatchilarni aniqlash va jazolash tizimi kuchli bo‘lsa, bu jinoyatlar soni kamayadi. Bundan tashqari, xalqaro hamkorlikni rivojlantirish ham muhim hisoblanadi.

Malakali mutaxassislarni tayyorlash Bugungi kunda kiberxavfsizlik sohasida malakali mutaxassislarga talab juda katta. Shu sababli yoshlarni IT va axborot xavfsizligi sohalariga qiziqtirish zarur. Universitetlarda zamonaviy laboratoriyalar tashkil etish, amaliy mashg‘ulotlarni kuchaytirish va xalqaro tajribalarni o‘rganish bu sohaning rivojlanishiga yordam beradi. O‘zbekistonda kiberxavfsizlikning rivojlanishi O‘zbekistonda ham kiberxavfsizlikka katta e’tibor qaratilmoqda. Mamlakatimizda raqamli texnologiyalar rivojlanib borayotgani sababli axborot xavfsizligini ta’minlash muhim vazifaga aylangan.

Bugungi kunda davlat xizmatlari elektron shaklga o‘tayotgani, internet banking va elektron to‘lov tizimlari keng rivojlanayotgani kiberxavfsizlikni yanada mustahkamlashni talab qilmoqda.Shu maqsadda mamlakatimizda axborot xavfsizligi markazlari tashkil etilmoqda, yosh mutaxassislarni tayyorlash bo‘yicha keng imkoniyatlar yaratilmoqda va zamonaviy himoya texnologiyalari joriy qilinmoqda.

Xulosa. Xulosa qilib aytganda, kiberxavfsizlik bugungi zamonaviy dunyoning eng muhim masalalaridan biridir. Texnologiyalar rivojlangani sari internetdagi xavf-xatarlar ham ortib bormoqda. Kiberjinoyatchilik, fishing, zararli dasturlar, shaxsiy ma’lumotlarning o‘g‘irlanishi va ijtimoiy tarmoqlardagi xavflar insonlar va tashkilotlarga katta zarar yetkazmoqda.

Bu muammolarni bartaraf etish uchun zamonaviy himoya tizimlaridan foydalanish, aholining internet savodxonligini oshirish, kuchli qonunchilik yaratish va malakali mutaxassislarni tayyorlash zarur deb o'ylayman.

## FOYDALANILGAN ADABIYOTLAR:

1. Axborot xavfsizligi asoslari – Toshkent, 2021.
2. Kiberxavfsizlik va axborotni himoyalash texnologiyalari – Toshkent axborot texnologiyalari universiteti nashriyoti, 2022.

3. O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi. Axborot xavfsizligi va kiberxavfsizlik bo‘yicha me’yoriy hujjatlar. Toshkent, 2024.
4. O‘zbekiston Respublikasi Prezidenti. “Raqamli O‘zbekiston – 2030” strategiyasi to‘g‘risidagi farmon. Toshkent, 2020.
5. Charles P. Pfleeger. Security in Computing. Prentice Hall, 2015.
6. Kaspersky. Kiberxavfsizlik bo‘yicha tahliliy hisobotlar, 2023.