Registered in Germany **Europa Revue Journal**
ISSN: 1862-6564 **Vol. 6 No. 6 (2026) Published June 16, 2026**

CURRENT ISSUES OF COMMON CYBERCRIMES AND PRACTICAL ASPECTS OF COMBATING THEM

ADILOVA MARJANGUL ELMURATOVNA
Lecturer at Karakalpak State University
ALIBEKOV ABBOS ANVAR O‘G‘LI
Student of Karakalpak State University

Abstract

This paper analyzes the most common crimes in the field of cybersecurity, their causes, their impact on public and national security, and the legal and practical mechanisms used to combat them. The rapid development of information and communication technologies, the widespread use of the Internet, and the integration of digital services into all areas of life have made cybercrime one of the most pressing challenges of the modern world. The study examines the nature of cyber threats and highlights the importance of strengthening cybersecurity measures to protect information systems and digital resources. The results of this research can serve as a theoretical and practical resource for law enforcement agencies, educational institutions, information technology specialists, and organizations operating in the field of cybersecurity.

Keywords

Cybersecurity, Cybercrime, Information Security, Phishing, DDoS Attacks, Malware, Computer Viruses, Trojan Programs, Spyware, Personal Data Protection, Financial Fraud, Strong Passwords, Two-Factor Authentication, Digital Technologies, Information Systems.

“KIBERXAVFSIZLIKDA KO‘P UCHRAYDIGAN JINOYATLARNING DOLZARB MUAMMOLAR VA ULARGA QARSHI KURASHISHNING AMALIY JIHATLARI”

Adilova Marjangul Elmuratovna - Qoraqalpoq davlat universiteti o‘qituvchisi
Alibekov Abbos Anvar O‘g‘li - Qoraqalpoq davlat universiteti talabasi

Annotatsiya: Mazkur ishda kiber xavfsizlik sohasida eng ko‘p uchraydigan jinoyatlar, ularning yuzaga kelish sabablari, jamiyat va davlat xavfsizligiga ta’siri

hamda ularga qarshi kurashishning huquqiy va amaliy mexanizmlari tahlil qilingan. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi, internet tarmog‘ining keng ommalashuvi va raqamli xizmatlarning hayotimizning barcha sohalariga kirib borishi natijasida kiberjinoyatchilik zamonaviy dunyoning eng dolzarb muammolaridan biriga aylandi. Ushbu tadqiqot natijalari huquqni muhofaza qiluvchi organlar, ta’lim muassasalari, axborot texnologiyalari mutaxassislari va kiberxavfsizlik sohasida faoliyat yurituvchi tashkilotlar uchun nazariy hamda amaliy manba sifatida xizmat qilishi mumkin.

Tayanch so‘zlar: kiberxavfsizlik, kiberjinoyat, axborot xavfsizligi, fishing, DDoS hujumlari, zararli dasturlar, kompyuter viruslari, troyan dasturlari, josuslik dasturlari, shaxsiy ma’lumotlarni himoya qilish, moliyaviy firibgarlik, kuchli parollar, ikki bosqichli autentifikatsiya, raqamli texnologiyalar, axborot tizimlari.

“АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАСПРОСТРАНЁННЫХ ПРЕСТУПЛЕНИЙ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ И ПРАКТИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ИМ”

Аннотация: В данной работе проанализированы наиболее распространённые преступления в сфере кибербезопасности, причины их возникновения, влияние на безопасность общества и государства, а также правовые и практические механизмы противодействия им. Стремительное развитие информационно-коммуникационных технологий, широкое распространение сети Интернет и внедрение цифровых услуг во все сферы жизнедеятельности привели к тому, что киберпреступность стала одной из наиболее актуальных проблем современного мира. В работе рассматриваются основные виды киберпреступлений, их особенности, последствия и угрозы для информационной безопасности. Особое внимание уделено вопросам совершенствования мер предупреждения и противодействия киберпреступности. Результаты данного исследования могут служить теоретическим и практическим источником для правоохранительных органов, образовательных учреждений, специалистов в области информационных технологий и организаций, осуществляющих деятельность в сфере кибербезопасности.

Ключевые слова: кибербезопасность, киберпреступность, информационная безопасность, фишинг, DDoS-атаки, вредоносное программное обеспечение, компьютерные вирусы, троянские программы, шпионское программное обеспечение, защита персональных данных, финансовое мошенничество, надежные пароли, двухфакторная аутентификация, цифровые технологии, информационные системы.

XXI asrda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha sohalarini raqamlashtirishga xizmat qilmoqda. Davlat boshqaruvi, bank-moliya tizimi, ta’lim, sog‘liqni saqlash va boshqa ko‘plab sohalarda zamonaviy axborot texnologiyalarining keng qo‘llanilishi insonlar hayotini yengillashtirish bilan bir qatorda yangi turdagi xavf va tahdidlarni ham yuzaga keltirmoqda. Kiberjinoyatchilik zamonaviy axborot makonida eng tez rivojlanayotgan noqonuniy faoliyat turlaridan biri hisoblanadi.

Xakerlik hujumlari, fishing, zararli dasturlar tarqatish, shaxsiy ma’lumotlarni o‘g‘irlash, bank kartalari orqali firibgarlik qilish va boshqa turdagi kiberjinoyatlar nafaqat alohida shaxslar, balki korxonalar, davlat tashkilotlari va hatto milliy xavfsizlikka ham jiddiy zarar yetkazmoqda. Mazkur jinoyatlarning murakkabligi va transmilliy xususiyatga ega ekanligi ularga qarshi kurashish jarayonini yanada qiyinlashtirmoqda. Mazkur ilmiy tatqiqot maqsadi kiberxavfsizlik sohasida eng ko‘p uchraydigan jinoyatlarning mohiyati va xususiyatlarini tahlil qilish, ularning yuzaga kelish omillarini aniqlash hamda ularga qarshi kurashishning huquqiy va amaliy jihatlarini yoritishdan iborat. Shuningdek, kiberjinoyatlarga qarshi kurashish bo‘yicha mavjud tajriba va mexanizmlar o‘rganilib, ushbu sohada samaradorlikni oshirishga qaratilgan taklif va tavsiyalar ishlab chiqiladi.

O‘zbekiston Respublikasi Prezidenti Sh. Mirziyoyev 2025-yil 30-apreldagi PQ-153- sonli “Axborot texnologiyalari yordamida sodir etilgan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora- tadbirlar to’g’risidagi” qarorda 2025-yil 5-mart kuni o‘tkazilgan Korrupsiyaga qarshi kurashish bo‘yicha milliy kengashning kengaytirilgan yig‘ilishida belgilangan vazifalarni samarali ijro etish hamda axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi

kurashish faoliyatini yanada kuchaytirish maqsadida ushbu qaror qabul qilingan. Ushbu qaror kiberjinoyatchiliklarning oldini olish mexanizmlari, kiberjinoyatlarni fosh qilish mexanizmlari, kiberjinoyatlarga qarshi kurarshishda ilmiy yondashuvlar alohida belgilangan[1]. Bugungi kunda raqamli texnologiyalar jadal rivojlanib, odamlarning kundalik hayotida muhim o‘rin egallamoqda. Internet va axborot texnologiyalarining rivojlanishi natijasida insonlar uchun yangi imkoniyatlar yaratildi, biznes jarayonlari optimallashtirildi, davlat xizmatlari raqamlashtirildi va global muloqot osonlashdi. Biroq, texnologik taraqqiyot bilan birga, yangi xavflar ham paydo bo‘ldi.

Kiberjinoyatlar nafaqat individual foydalanuvchilarga, balki biznes va davlat muassasalariga ham katta zarar yetkazmoqda. Ushbu jinoyatlar shaxsiy ma’lumotlarning o‘g‘irlanishi, moliyaviy firibgarlik, tarmoq hujumlari va axborot tizimlariga zarar yetkazish kabi holatlarni o‘z ichiga oladi. Ularning keng tarqalishi kiberxavfsizlik choralarining muhimligini oshirmoqda. Kiber jinoyatlarning turlari va ulardan himoyalanish choralari. Fishing - firibgarlarning soxta elektron pochta xabarlari, veb-saytlar yoki xabarlar orqali foydalanuvchilarning shaxsiy va moliyaviy ma’lumotlarini qo‘lga kiritish usulidir. Ko‘pincha bunday xabarlar banklar, davlat tashkilotlari yoki yirik kompaniyalardan kelganday tuyuladi.

Fishing hujumlari quyidagi shakllarda amalga oshirilishi mumkin:

Elektron pochta fishingi - foydalanuvchilarga soxta elektron pochta xabarlari yuboriladi, unda ular login va parollarini kiritishga undaladi.

Vishing (ovozli fishing) - telefon qo‘ng‘iroqlari orqali foydalanuvchilarni aldab, ularning shaxsiy yoki moliyaviy ma’lumotlarini olishga harakat qilinadi.

SMS fishing - soxta SMS xabarlar orqali foydalanuvchilar fishing havolalariga bosishiga undaladi.

Spear fishing - aniq bir shaxs yoki tashkilotni nishonga olgan fishing hujumi, bunda maxsus tayyorlangan xabarlar va shaxsiylashtirilgan ma’lumotlar ishlatiladi.

Fishing hujumlaridan himoyalanish uchun foydalanuvchilar shubhali xabarlarga ishonmasligi, elektron pochta yoki SMS orqali kelgan havolalarga bosishdan oldin ularning haqiqiyligini tekshirishi lozim. Shuningdek, ikki bosqichli autentifikatsiya va

[1] https://www.lex.uz/ru/docs/-7511145

xavfsizlik dasturlaridan foydalanish ham fishingga qarshi samarali choradir[2]. DDoS hujum (distributed denial of service, “xizmat ko‘rsatishning taqsimlangan rad etilishi”) - xakerlar tomonidan foydalanuvchilarning veb-sayt, server yoki tarmoqqa kirishini cheklashga bo‘lgan urinishi. Ular nishonga ko‘plab qurilmalardan zararli paketlar bilan hujum qilib, uni katta hajmdagi trafik bilan yuklaydi. Natijada xizmat vaqtincha ish faoliyatini to‘xtatishi, sekinlashishi yoki foydalanuvchilar so‘rovining bir qismini javobsiz qoldirishi mumkin[3]. DDoS hujumlarining asosiy turlari quyidagilardir:

Hajmli hujumlar (Volume-Based Attacks) - tarmoqni haddan tashqari trafik bilan to‘ldirish orqali xizmatlarni ishdan chiqarish.

Protokol hujumlari (Protocol Attacks) - tarmoq protokollarining zaif tomonlaridan foydalanib, server va tarmoqlarni izdan chiqarish.

Ilovalar darajasidagi hujumlar (Application Layer Attacks) - muayyan veb-sayt yoki xizmatga ortiqcha so‘rovlar yuborish orqali uning ishlashini sekinlashtirish yoki butunlay to‘xtatish.

DDoS hujumlaridan himoyalanish choralari:

Tarmoq filtrlash texnologiyalaridan foydalanish - DDoS hujumlarini oldindan aniqlash va zararli trafikni bloklash.

Cloud-based DDoS himoya xizmatlaridan foydalanish - Cloudflare, Akamai va AWS Shield kabi xizmatlar DDoS hujumlarini kamaytirishga yordam beradi.

Zaxira serverlar va yukni muvozanatlashtirish – trafikni turli serverlar o‘rtasida taqsimlash orqali hujumlarning ta’sirini kamaytirish.

Trafikni doimiy monitoring qilish - shubhali trafikni erta aniqlash va oldini olish uchun xavfsizlik tizimlaridan foydalanish.

DDoS hujumlari har qanday tashkilot yoki foydalanuvchi uchun jiddiy xavf tug‘dirishi mumkin, shuning uchun zamonaviy himoya choralari va xavfsizlik strategiyalaridan foydalanish muhimdir. Zararli dasturlar - bu foydalanuvchilarning kompyuter tizimlariga zarar yetkazish, shaxsiy ma’lumotlarini o‘g‘irlash yoki

[2] https://najottalim.uz/blog/fishing-hujumlari-nima-ulardan-qanday-himoyalanish-mumkin?srsltid=AfmBOoo38HomUDE6ojTqHY6Ynwp8ZEOrVNXM164C0mCoJMGpNiw2xWyG#:~:text=Email%20orqali%20fishing,idoralari%20nomidan%20gapiriladi.

[3] https://mohirdev.uz/blog/DDoS-hujumlar-nima-ozi/#:~:text=DDoS%20hujum%20(distributed,javobsiz%20qoldirishi%20mumkin.

noqonuniy maqsadlarda foydalanish uchun maxsus ishlab chiqilgan dasturlar to‘plamidir. Ular quyidagi turlarga bo‘linadi:

Kompyuter viruslari - o‘zini boshqa fayllarga qo‘shib oladigan va ularni buzadigan dasturlar.

Troyan dasturlari - foydalanuvchi tizimiga foydali dastur ko‘rinishida kirib, zarar yetkazuvchi kodlarni o‘z ichiga olgan zararli dasturlar.

Josuslik dasturlari (Spyware) - foydalanuvchining faoliyatini kuzatish va shaxsiy ma’lumotlarni yashirincha yig‘ish uchun mo‘ljallangan dasturlar.

Keyloggerlar - klaviatura bosishlarini qayd qilib, foydalanuvchi parollari va shaxsiy ma’lumotlarini o‘g‘irlovchi dasturlar.

Zararli dasturlar odatda xabarlari, shubhali havolalar yoki yolg‘on dasturlar orqali tarqaladi. Ulardan himoyalanish uchun ishonchli antivirus dasturlarini o‘rnatish, dasturlarni faqat rasmiy manbalardan yuklab olish va shubhali havolalarga bosmaslik muhimdir. Kuchli parollar ishlatish yani foydalanuvchilar o‘z hisoblarini himoya qilish uchun murakkab va takrorlanmas parollardan foydalanishlari kerak. Har bir xizmat uchun alohida parol yaratish va uni muntazam yangilab turish muhimdir.

Kuchli parol quyidagi xususiyatlarga ega bo‘lishi kerak:

Uzunlik – kamida 12-16 ta belgidan iborat bo‘lishi kerak.

Murakkablik – katta va kichik harflar, raqamlar hamda maxsus belgilar (!@#$%^&*()) qo‘llanilishi lozim.

Unikal bo‘lishi – har bir akkaunt uchun alohida parol ishlatilishi kerak.

Oldindan taxmin qilib bo‘lmaydigan bo‘lishi – foydalanuvchi ismi, tug‘ilgan sanasi yoki oddiy so‘zlar kiritilmasligi lozim.

Kuchli parollar yaratish va saqlash uchun quyidagi usullardan foydalanish tavsiya etiladi:

Parol menejer dasturlaridan foydalanish – LastPass, 1Password yoki Bitwarden kabi dasturlar yordamida parollarni xavfsiz saqlash va avtomatik yaratish mumkin.

Parollarni muntazam yangilash – har 3-6 oyda parollarni yangilash va avval ishlatilgan parollardan qayta foydalanmaslik kerak.

Shubhali manbalarga parol kiritmaslik – Fishing va boshqa firibgarlik usullari

orqali parollarni qo‘lga kiritishga urinishlardan ehtiyot bo‘lish zarur.

Shuningdek, hech qachon parollarni yozib qo‘ymaslik va boshqa shaxslar bilan ulashmaslik kerak. Xavfsiz va ishonchli parollar ishlatish orqali kiberjinoyatlardan himoyalanish imkoniyati sezilarli darajada oshadi. Kiberjinoyatlardan himoyalanish bugungi raqamli jamiyatning eng muhim vazifalaridan biridir. Internet va axborot texnologiyalaridan foydalanish kengayib borayotgan bir paytda fuqarolar, tashkilotlar va davlat idoralari o‘z axborot resurslarini himoya qilishga alohida e’tibor qaratishlari zarur. Xulosa qilib aytganda, axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi va raqamli transformatsiya jarayonlarining kengayishi kiberxavfsizlik masalasini zamonaviy jamiyatning eng muhim yo‘nalishlaridan biriga aylantirdi. Internet tarmog‘i va raqamli xizmatlardan foydalanish hajmining ortishi bilan bir qatorda kiberjinoyatlar soni, ko‘lami va murakkabligi ham ortib bormoqda. Xakerlik hujumlari, fishing, zararli dasturlar tarqatish, shaxsiy ma’lumotlarni o‘g‘irlash hamda moliyaviy firibgarlik kabi jinoyatlar fuqarolar, tashkilotlar va davlat manfaatlariga jiddiy zarar yetkazmoqda. Shunday qilib, kiberxavfsizlikni ta’minlash va kiberjinoyatlarning oldini olish raqamli jamiyatning barqaror rivojlanishi, fuqarolarning huquq va manfaatlarini himoya qilish hamda davlatning axborot suverenitetini mustahkamlashning muhim sharti hisoblanadi.

FOYDALANILGAN ADABIYOTLAR:

1) O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi 2022-yil 15-aprel, O‘RQ-764-sonli Qonuni.

2) O‘zbekiston Respublikasi Prezidentining "Axborot texnologiyalari yordamida sodir etilgan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida"gi 2025-yil 30-aprel, PQ-153-sonli Qarori.

3) G‘ulomov S. S., Shermuhammedov A. T. Axborot xavfsizligi va kiberxavfsizlik asoslari. Darslik. – Toshkent: "Yangi asr avlodi", 2021-yil.

4) Mamatov A. A., Xalilov M. M. Kibermakonda jinoyatchilikka qarshi kurashishning huquqiy va amaliy muammolari. // O‘zbekiston Milliy universiteti xabarlari (Ilmiy jurnal). – Toshkent, 2023-yil.

5) Karimov. I Axborot xavfsilik asoslari. Darslik. - Toshkent, 2016-yil.