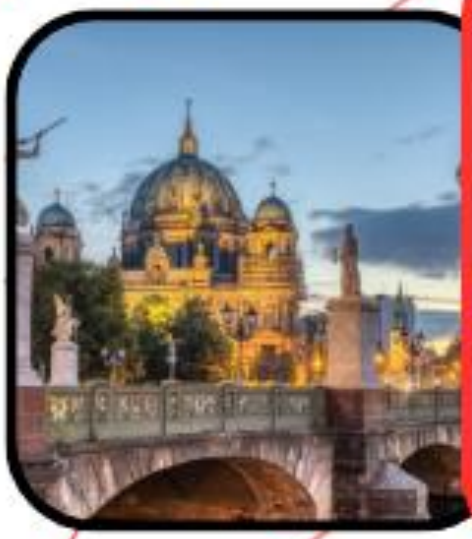
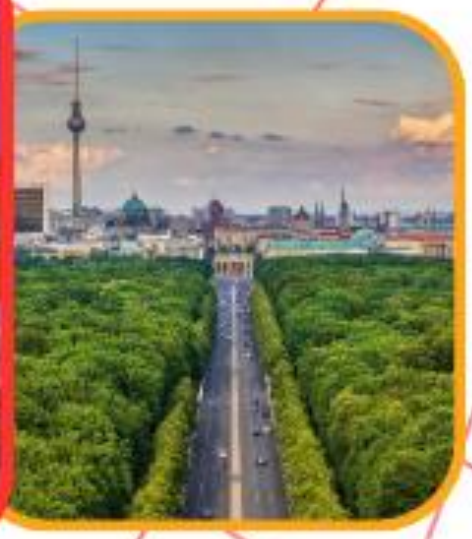
EOC
EUROASIAN ONLINE CONFERENCES

GERMANY
CONFERENCE

INTERNATIONAL CONFERENCE ON SCIENCE, ENGINEERING AND TECHNOLOGY





Google Scholar zenodo OpenAIRE doi digital object identifier

INTERNATIONAL CONFERENCE ON SCIENCE, ENGINEERING AND TECHNOLOGY: a collection scientific works of the International scientific conference – Hamburg, Germany, 2026 Issue 5

Languages of publication: Uzbek**,** English, Russian, German, Italian, Spanish,

The collection consists of scientific research of scientists, graduate students and students who took part in the International Scientific online conference **« INTERNATIONAL CONFERENCE ON SCIENCE, ENGINEERING AND TECHNOLOGY »**. Which took place in Hamburg 2026.

Conference proceedings are recommended for scientists and teachers in higher education establishments. They can be used in education, including the process of post - graduate teaching, preparation for obtain bachelors' and masters' degrees. The review of all articles was accomplished by experts, materials are according to authors copyright. The authors are responsible for content, researches results and errors.

Raqamli huquq va kiber jinoyatlar.

Bakirov Muhammadnosir Dilshodbek o'g'li
Qodirov Muhammadziyo Baxtiyor o'g'li
Farg'ona Viloyati Yuridik texnikumi 44-24 guruh o'quvchilari

Annotatsiya. Ushbu maqolada raqamli huquq tushunchasi va zamonaviy axborot jamiyatida kiber jinoyatlar muammosi tahlil qilinadi. Raqamli texnologiyalarning jadal rivojlanishi natijasida internetdan foydalanish kundalik hayotning ajralmas qismiga aylangan bo'lib, bu esa yangi imkoniyatlar bilan bir qatorda huquqiy muammolarni ham yuzaga keltirmoqda. Tadqiqotda raqamli faoliyatni tartibga soluvchi huquqiy mexanizmlar, shuningdek, xakerlik, shaxsiy ma'lumotlarni o'g'irlash, onlayn firibgarlik, ma'lumotlar bazasiga noqonuniy kirish va kiber tahdidlar kabi asosiy kiber jinoyat turlari tahlil qilinadi. Shuningdek, kiber jinoyatlarning transchegaraviy xususiyati va texnologik murakkabligi sababli ularni aniqlash hamda oldini olishdagi muammolar ko'rib chiqiladi. Maqolada kiber xavfsizlikni mustahkamlash, xalqaro hamkorlikni rivojlantirish va aholining raqamli savodxonligini oshirish kabi yechimlar ham taklif etiladi. Natijalar raqamli muhitda xavfsizlik va huquqiy tartibni ta'minlashda samarali huquqiy mexanizmlarni ishlab chiqish zarurligini ko'rsatadi.

Kalit so'zlar: raqamli huquq, kiber jinoyat, kiber xavfsizlik, axborot texnologiyalari, onlayn firibgarlik, ma'lumotlar himoyasi, xakerlik, raqamli xavfsizlik, internet huquqi, huquqiy tartibga solish.

Asosiy qism

Raqamli huquq tushunchasi va uning ahamiyati. Raqamli huquq zamonaviy axborot jamiyatida internet, raqamli platformalar va axborot texnologiyalaridan foydalanishni tartibga soluvchi huquqiy normalar majmuasidir. Bugungi kunda davlatlar raqamli iqtisodiyotga o'tish jarayonida fuqarolarning huquqlarini himoya qilish, ma'lumotlar xavfsizligini ta'minlash va kiber makondagi munosabatlarni tartibga solishga alohida e'tibor qaratmoqda. Raqamli huquq shaxsiy ma'lumotlarni himoya qilish, elektron tijorat, elektron hujjatlar aylanishi hamda kiber jinoyatlarga qarshi kurashish kabi yo'nalishlarni o'z ichiga oladi.

Raqamli muhitning kengayishi bilan birga huquqiy munosabatlar ham murakkablashib bormoqda. Internet orqali amalga oshiriladigan har qanday faoliyat huquqiy jihatdan tartibga solinishi zarur, chunki bu jarayonda foydalanuvchilarning huquqlari buzilishi ehtimoli yuqori.

Kiber jinoyatlar va ularning turlari. Kiber jinoyatlar — bu kompyuter tizimlari, internet tarmoqlari yoki raqamli qurilmalar yordamida sodir etiladigan noqonuniy harakatlardir. Ular zamonaviy jamiyat uchun jiddiy xavf tug'diradi va iqtisodiy, ijtimoiy hamda shaxsiy zarar yetkazishi mumkin.

Keng tarqalgan kiber jinoyat turlariga quyidagilar kiradi:

- **Xakerlik (hacking)** — tizimlarga noqonuniy kirish va ma'lumotlarni o'zgartirish yoki o'g'irlash.

- **Onlayn firibgarlik** — internet orqali foydalanuvchilarni aldash va moliyaviy zarar yetkazish.
- **Shaxsiy ma’lumotlarni o‘g‘irlash** — fuqarolarning maxfiy ma’lumotlarini noqonuniy qo‘lga kiritish va ulardan foydalanish.
- **DDoS hujumlar** — tizim yoki serverlarni ishdan chiqarish maqsadida ortiqcha trafik yuborish.
- **Kiber tahdid va kiber zo‘ravonlik** — ijtimoiy tarmoqlar orqali shaxsga bosim o‘tkazish yoki tahdid qilish.

Ushbu jinoyatlar ko‘pincha transchegaraviy xarakterga ega bo‘lib, ularni aniqlash va jazolash jarayoni murakkab hisoblanadi.

Kiber jinoyatlarga qarshi kurash muammolari. Kiber jinoyatlarga qarshi kurashishda bir qator muammolar mavjud. Eng asosiy muammolardan biri — jinoyatchilarning anonimligi va ularning turli davlatlardan faoliyat yuritishidir. Bu esa huquqni muhofaza qiluvchi organlar uchun ularni aniqlashni qiyinlashtiradi.

Bundan tashqari, texnologik rivojlanish jinoyat usullarining ham murakkablashishiga olib kelmoqda. Ko‘plab davlatlarda kiber jinoyatlarga qarshi qonunchilik yetarli darajada rivojlanmagan yoki amaliyotda to‘liq ishlamaydi. Mutaxassislar yetishmasligi ham ushbu sohada muhim muammo hisoblanadi.

Raqamli xavfsizlikni ta’minlash yo‘llari. Kiber jinoyatlarga qarshi samarali kurashish uchun bir qator chora-tadbirlar ishlab chiqilmoqda. Birinchidan, milliy qonunchilikni takomillashtirish va kiber jinoyatlar uchun aniq javobgarlik mexanizmlarini joriy etish zarur. Ikkinchidan, xalqaro hamkorlikni kuchaytirish orqali transchegaraviy jinoyatlarga qarshi kurashish samaradorligini oshirish mumkin.

Shuningdek, axborot xavfsizligi bo‘yicha mutaxassislarni tayyorlash, fuqarolarning raqamli savodxonligini oshirish va zamonaviy kiber xavfsizlik texnologiyalaridan foydalanish muhim ahamiyatga ega. Ta’lim muassasalarida raqamli huquq va kiber xavfsizlik bo‘yicha bilimlarni kengaytirish ham kelajakdagi xavflarni kamaytirishga yordam beradi.

Xulosa. Xulosa qilib aytganda, raqamli huquq va kiber jinoyatlar zamonaviy axborot jamiyatining eng muhim va dolzarb muammolaridan biri hisoblanadi. Raqamli texnologiyalarning jadal rivojlanishi natijasida inson hayotining barcha sohalarida internet va axborot tizimlaridan keng foydalanilmoqda, bu esa yangi huquqiy munosabatlarni shakllantirmoqda.

Tadqiqot natijalari shuni ko‘rsatadiki, kiber jinoyatlar sonining ortib borishi raqamli xavfsizlikni ta’minlashda jiddiy muammolarni yuzaga keltirmoqda. Xususan, xakerlik, onlayn firibgarlik, shaxsiy ma’lumotlarni o‘g‘irlash va boshqa kiber hujumlar jamiyat va iqtisodiyotga sezilarli zarar yetkazmoqda. Ushbu jinoyatlarning transchegaraviy xarakterga ega ekanligi ularni aniqlash va jazolash jarayonini yanada murakkablashtiradi.

Shu sababli, raqamli huquqni rivojlantirish, milliy va xalqaro qonunchilikni takomillashtirish, kiber xavfsizlik tizimini mustahkamlash hamda aholining

raqamli savodxonligini oshirish muhim ahamiyatga ega. Faqat kompleks yondashuv orqali raqamli muhitda xavfsizlik va huquqiy tartibni ta’minlash mumkin.

Adabiyotlar ro‘yxati

1. Castells, M. (2010). *The Rise of the Network Society*. Wiley-Blackwell.
2. Lessig, L. (2006). *Code: Version 2.0*. Basic Books.
3. Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.
4. Yar, M. (2013). *Cybercrime and Society*. SAGE Publications.
5. Clough, J. (2015). *Principles of Cybercrime*. Cambridge University Press.
6. UNODC (2020). *Comprehensive Study on Cybercrime*. United Nations Office on Drugs and Crime.
7. Council of Europe (2001). *Budapest Convention on Cybercrime*.
8. OECD (2019). *Digital Security Risk Management for Economic and Social Prosperity*. OECD Publishing.