KRIMINOLOGIYA
VA JINOIY ODIL SUDLOV

ILMIY-AMALIY JURNAL

2025-yil 2-son

VOLUME 5 / ISSUE 2 / 2025
ISSUE DOI: 10.51788/TSUL.CCJ.5.2.

ISSN 2181-2179
DOI: 10.51788/TSUL.CCJ.

MUASSIS:
TOSHKENT DAVLAT YURIDIK UNIVERSITETI

"Kriminologiya va jinoiy odil sudlov" ilmiy-amaliy jurnali O'zbekiston matbuot va axborot agentligi tomonidan 2021-yil 18-martda 1160-sonli guvohnoma bilan davlat ro'yxatidan o'tkazilgan.

Ushbu jurnal O'zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi bilan hamkorlikda tashkil etilgan.

Jurnal O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasi jurnallari ro'yxatiga kiritilgan.

Sotuvda kelishilgan narxda.

Nashr bo'yicha mas'ul:
O. Choriyev

Muharrirlar:
Y. Mahmudov, M. Sharifova,
Sh. Beknazarova, Y. Yarmolik,
E. Mustafayev
Musahhih:
S. Rasulova
Texnik muharrir:
U. Sapayev
Dizayner:
D. Rajapov

Tahririyat manzili:
100047. Toshkent shahri,
Sayilgoh ko'chasi, 35.

Tel.: (0371) 233-66-36, 233-41-09.
Faks: (0371) 233-37-48.
Veb-sayt: www.ccj.tsul.uz
E-mail: criminologyjournal@tsul.uz

Obuna indeksi: 1386.

Nashriyot litsenziyasi
№ 174625, 29.11.2023.

Jurnal 2025-yil 23-iyunda,
bosmaxonaga topshirildi.
Qog'oz bichimi: A4.
Shartli bosma tabog'i: 6
Adadi: 100. Buyurtma: № 115.

Bosmaxona litsenziyasi
29.11.2023 № 174626

TDYU bosmaxonasida chop etildi.
Bosmaxona manzili:
100047. Toshkent shahri,
Sayilgoh ko'chasi, 37.

ISSN 2181-2179
DOI: 10.51788/tsul.ccj.

УЧРЕДИТЕЛЬ:
ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ

Правовой научно-практический журнал «Криминология и уголовное правосудие» зарегистрирован Агентством печати и информации Узбекистана 18 марта 2021 года с удостоверением № 1160.

Журнал создан при сотрудничестве с Правоохранительной академией Республики Узбекистан.

Журнал включён в перечень журналов Высшей аттестационной комиссии при Министерстве высшего образования, науки и инноваций Республики Узбекистан.

Реализуется по договорной цене.

Ответственный за выпуск:
О. Чориев

Редакторы:
Й. Махмудов, М. Шарифова,
Ш. Бекназарова, Е. Ярмолик,
Э. Мустафаев
Корректор:
С. Расулова
Технический редактор:
У. Сапаев
Дизайнер:
Д. Ражапов

Адрес редакции:
100047. Город Ташкент,
улица Сайилгох, 35.

Тел.: (0371) 233-66-36, 233-41-09.
Факс: (0371) 233-37-48.
Веб-сайт: www.ccj.tsul.uz
E-mail: criminologyjournal@tsul.uz

Подписной индекс: 1386.

Издательская лицензия от
29.11.2023, № 174625.

Журнал передан в типографию
23.06.2025.
Формат бумаги: А4.
Усл. п. л. 6. Тираж: 100 экз.
Номер заказа: 115.

Лицензия типографии от
№ 174626, 29.11.2023.

Отпечатано в типографии
Ташкентского государственного
юридического университета.
100047, г. Ташкент, ул. Сайилгох, дом 37.

FOUNDER:
TASHKENT STATE UNIVERSITY OF LAW

"The scientific-practical journal "Criminology and Criminal Justice" was registered by the Press and Information Agency of Uzbekistan on March 18, 2021, with certificate No. 1160.

This journal was founded in cooperation with the Law Enforcement Academy of the Republic of Uzbekistan.

The journal is included in the list of journals of the Higher Attestation Commission under the Ministry of Higher Education, Science and Innovations of the Republic of Uzbekistan.

Agreed-upon price.

Publication Officer:
O. Choriev

Editors:
Y. Makhmudov, M. Sharifova,
Sh. Beknazarova, Y. Yarmolik, E. Mustafaev
Proofreader:
S. Rasulova
Technical editor:
U. Sapaev
Designer:
D. Rajapov

Editorial office address:
100047. Tashkent city,
Sayilgokh street, 35.

Phone: (0371) 233-66-36,
233-41-09.
Fax: (0371) 233-37-48.
Website: www.ccj.tsul.uz
E-mail: criminologyjournal@tsul.uz

Subscription index: 1386.

Publishing license
№ 174625, 29.11.2023.

The journal is submitted to the Printing house on 23.06.2025.
Paper size: A4.
Cond.p.f: 6.
Units: 100. Order: № 115.

Printing house license
№ 174626, 29.11.2023.

Published in the Printing house of Tashkent State University of Law.
100047. Tashkent city, Sayilgokh street, 37.

ISSN 2181-2179
DOI: 10.51788/tsul.ccj.

2025-YIL 2-SON
VOLUME 5
ISSUE 2 / 2025

MUNDARIJA

12.00.07 – SUD HOKIMIYATI. PROKUROR NAZORATI. HUQUQNI MUHOFAZA QILISH FAOLIYATINI TASHKIL ETISH. ADVOKATURA

12.00.08 – JINOYAT HUQUQI. JINOYAT-IJROIYA HUQUQI

12.00.09 – JINOYAT PROTSESSI. KRIMINALISTIKA, TEZKOR-QIDIRUV HUQUQ VA SUD EKSPERTIZASI

СОДЕРЖАНИЕ

12.00.07 – СУДЕБНАЯ ВЛАСТЬ. ПРОКУРОРСКИЙ НАДЗОР. ОРГАНИЗАЦИЯ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ. АДВОКАТУРА

12.00.08 – УГОЛОВНОЕ ПРАВО. УГОЛОВНО-ИСПОЛНИТЕЛЬНОЕ ПРАВО

12.00.09 – УГОЛОВНЫЙ ПРОЦЕСС. КРИМИНАЛИСТИКА, ОПЕРАТИВНО-РОЗЫСКНОЕ ПРАВО И СУДЕБНАЯ ЭКСПЕРТИЗА

ISSN 2181-2179
DOI: 10.51788/tsul.ccj.

CONTENTS

12.00.07 – JUDICIAL BRANCH. PROSECUTOR'S CONTROL. ORGANIZATION OF LAW ENFORCEMENT. ADVOCACY

12.00.08 – CRIMINAL LAW. CRIMINAL-EXECUTIVE LAW

12.00.09 – CRIMINAL PROCEEDINGS. FORENSICS, INVESTIGATIVE LAW AND FORENSIC EXPERTISE

Kelib tushgan / Получено / Received: 15.05.2025
Qabul qilingan / Принято / Accepted: 13.06.2025
Nashr etilgan / Опубликовано / Published: 23.06.2025

DOI: 10.51788/tsul.ccj.5.2./PZZZ7518
UDC: 343.9:004(045)(575.1)

KIBERJINOYATLARNING TURLARI VA ULARNING O‘ZIGA XOS XUSUSIYATLARI

Mirzakarimova Dilafruz Doniyorjon qizi,
Farg‘ona davlat universiteti
Huquq ta’limi kafedrasi o‘qituvchisi
ORCID: 0009-0001-6043-0323
e-mail: dilafruzmirzakarimova80@gmail.com

Annotatsiya*. Ushbu maqolada kiberjinoyatlar, ularning turlari, kelib chiqishi va rivojlanish tarixi haqida ma’lumotlar berilgan. Avvalo, kiberjinoyat deganda qanday jinoyatlar tushunilishi, ularning tasnifi va xususiyatlari talqin qilingan. Bundan tashqari, zamonaviy raqamli dunyoda kiberjinoyatlarning o‘sish sabablari va unga qarshi kurashish uchun ko‘riladigan chora-tadbirlar muhokama qilindi. Kiberjinoyatlarning sodir etilishi sabablari, ularga zamin yaratayotgan xavfsizlik tizimidagi bo‘shliqlar, kiberjinoyatlar uchun javobgarlik masalasi, shuningdek, bu boradagi ishlarning hozirgi holati muhokama qilindi. Maqolada, shuningdek, nusxa olish metodidan foydalanilgan. Ya’ni kiberjinoyatlar bilan bog‘liq ma’lumotlar, kiberjinoyatlar sodir etilgan holatlar, ularni aniqlash va tergov qilish, javobgarlik choralarini belgilash kabi masalalar xorijiy davlatlar tajribasidan kelib chiqib o‘rganilgan. Kiberjinoyatchilikka qarshi kurashishda hamkorlik va axborot almashish hal qiluvchi ahamiyatga ega. Kiberjinoyatlarni tergov qilish usullari raqamli dalillarni to‘plash, tarmoq faolligini tahlil qilish, kriminalistik tahlil, shaxsiy ma’lumotlarni tekshirish va ekspertlar bilan hamkorlikni o‘z ichiga oladi. Bu usullar jinoyatlarni aniqlash va ularning oldini olishda muhim ahamiyatga ega. Shu bilan birga, joriy vaziyatni yaxshilash, kiberjinoyatchilikning oldini olish va buning uchun javobgarlikni belgilashga qaratilgan qonunchilik bo‘yicha takliflar kiritildi.*

Kalit so‘zlar: *kiberjinoyat, internet firibgarligi, shaxsiy ma’lumotlar, kiberhujumlar, xakerlik, virus, zararli dasturlar*

ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ И ИХ ОСОБЕННОСТИ

Мирзакаримова Дилафруз Дониёржон кизи,
преподаватель кафедры правового образования
Ферганского государственного университета

Аннотация. *В данной статье представлена информация о киберпреступлениях, их разновидностях, происхождении и истории развития. В первую очередь рас-*

сматриваются понятие киберпреступления, его классификация и характерные особенности. Кроме того, проанализированы причины роста киберпреступности в современном цифровом мире, а также меры, предпринимаемые для борьбы с ней. Особое внимание уделено причинам совершения киберпреступлений, пробелам в системе кибербезопасности, создающим условия для таких преступлений, вопросам ответственности за киберпреступления и текущему состоянию работы в данной сфере. В статье использован метод заимствования. В частности, вопросы, связанные с киберпреступлениями, – сведения о них, случаи совершения, методы выявления и расследования, а также меры ответственности – изучены с учётом опыта зарубежных стран. Подчёркивается, что сотрудничество и обмен информацией имеют решающее значение в борьбе с киберпреступностью. Методы расследования киберпреступлений включают сбор цифровых доказательств, анализ сетевой активности, криминалистический анализ, проверку персональных данных и взаимодействие с экспертами. Эти методы играют важную роль в выявлении преступлений и предотвращении их совершения. Также предложены законодательные инициативы, направленные на улучшение текущей ситуации, предупреждение киберпреступности и установление ответственности за совершение таких преступлений.

Ключевые слова: *киберпреступление, интернет-мошенничество, персональные данные, кибератаки, хакерство, вирус, вредоносные программы*

TYPES OF CYBERCRIMES AND THEIR CHARACTERISTICS

Mirzakarimova Dilafruz Doniyorjon kizi,
Teacher at the Department of Legal Education,
Fergana State University

Abstract. *This article provides information about cybercrimes, their types, origin, and history of development. First of all, what crimes are meant by cybercrime, their classification and characteristics are interpreted. In addition, the reasons for the growth of cybercrime in the modern digital world and measures to combat it were discussed. The reasons for the commission of cybercrimes, the gaps in the security system that create the basis for them, the issue of responsibility for cybercrimes, as well as the current state of affairs in this area were discussed. The article also uses the copying method. That is, information related to cybercrimes, cases of cybercrimes, their detection and investigation, and the establishment of liability measures were studied based on the experience of foreign countries. Cooperation and information exchange are crucial in the fight against cybercrime. Methods for investigating cybercrimes include collecting digital evidence, analyzing network activity, forensic analysis, verifying personal data, and collaborating with experts. These methods are important for detecting and preventing crimes. At the same time, proposals were made on legislation aimed at improving the current situation, preventing cybercrime, and establishing responsibility for it.*

Keywords: *cybercrime, Internet fraud, personal data, cyberattacks, hacking, virus, malicious programs*

Kirish

Kiberjinoyat – xakerlar yoki boshqa jinoyatchilar tomonidan raqamli qurilmalar va tarmoqlardan noqonuniy maqsadlarda foydalanish yoki ularga hujum qilish ostida sodir etiluvchi jinoyat turi. Kiberjinoyatlar turli shakllarda namoyon bo‘lib, ularning oldini olish muhim ahamiyat kasb etmoqda. Ko‘pgina davlatlarda ushbu tahdidlarga qarshi yangi strategiyalar ishlab chiqilmoqda. Bu borada ta’lim va xabardorlik muhim rol o‘ynaydi. Ommaviy axborot vositalari va ijtimoiy tarmoqlarda firibgarlik, fishing, zararli dasturlar va boshqa kiberjinoyatlarning ko‘payishi foydalanuvchilarning ehtiyotkorligini oshirishga yordam beradi. Ba’zi kiberjinoyatchilar texnik jihatdan juda malakali bo‘lib, har jihatdan puxta tashkil etilgan va murakkab usullardan foydalanadilar. Mamlakatning moliyaviy, siyosiy xavfsizligiga tahdidlar yoki kiberterrorizm kompyuterlarga iqtisodiy, shaxsiy va siyosiy hujumlarni o‘z ichiga olgan kiberjinoyatlar bunga misol bo‘la oladi [1].

So‘nggi yillarda ommaviy axborot vositalarida “kiberjinoyat” tushunchasiga tobora ko‘proq duch kelayotgan bo‘lsak-da, ushbu tushunchaga sinonim sifatida mamlakatimizda “kompyuter jinoyatlari” yoki “axborot texnologiyalari sohasidagi jinoyatlar” tushunchalari qo‘llanadi. Ammo aksariyat mualliflar “kiberjinoyat” tushunchasini “kompyuter jinoyatlari” tushunchasidan farq qilishini, ushbu tushuncha axborotlashtirish sohasidagi barcha jinoyatlarni qamrab olishini va shu orqali “kompyuter jinoyatlari”ga nisbatan kengroq tushuncha ekanligini ta’kidlashgan. Bundan ko‘rinadiki, kiberjinoyat kompyuterdan foydalanish yoki global tarmoq orqali sodir qilinadigan jinoyatdir [2].

Kiberjinoyatlarning turli shakllarini tushunish shaxslarga, tashkilotlarga va siyosatchilarga sodir bo‘lishi kutilgan tahdidlarning oldini olish, unga qarshi kurashishdagi asosiy vazifalarni belgilash, samarali xavfsizlik choralarini ishlab chiqish va tegishli qonunchilik normalarini shakllantirishga yordam beradi.

Mazkur tadqiqot ishining asosiy maqsadi fishing, identifikator o‘g‘irlash, kiberbulling va zararli dastur hujumlari kabi kiberjinoyatlarning har xil turlarini o‘rganish va tasniflash, ularning o‘ziga xos xususiyatlari hamda ishlash usullarini tahlil qilishdan iborat. Shuningdek, mazkur jinoyatlarning mohiyati, ta’siri, oldini olish yoki ularga qarshi samarali kurashish yo‘llari haqida xabardorlikni oshirishga qaratilgan. Bu bilimlar xavfsizroq onlayn muhitni yaratish va jamiyatda kiber barqarorlikni oshirishda muhim ahamiyat kasb etadi. Ushbu maqolada kiberjinoyatlarning turlari, ularning o‘ziga xos xususiyatlari, kiberjinoyatlarni tahlil qilish, ularga nisbatan javobgarlik choralarini belgilash kabi masalalar o‘rganiladi va ko‘rsatilgan ma’lumotlardan kelib chiqqan holda qonunchilikka takliflar beriladi.

Material va metodlar

Mazkur maqolada kiberjinoyatlarning turlari, ularni kvalifikatsiya qilish, kiberjinoyatlar va ularga nisbatan javobgarlik choralarini belgilash bilan bog‘liq qonunchilikdagi bo‘shliqlar o‘rganilgan va mavjud muammolarga muqobil yechimlar taqdim etilgan.

Har yili millionlab odamlar xakerlik, firibgarlik, shaxsiy ma’lumotlarni o‘g‘irlash va boshqa kiberjinoyatlar natijasida zarar ko‘rmoqda. Jumladan, O‘zbekiston

ISSN 2181-2179
DOI: 10.51788/tsul.ccj.

Respublikasida ham yaqin yillarda kiberjinoyatlar soni ko‘paydi. Ayni paytda kiberjinoyatlarning turlari va javobgarlik choralari, tergov va raqamli dalillarni to‘plash bilan bog‘liq masalalar qonunchilikda to‘liq aks etmagan. Shuning uchun, birinchi navbatda, bu sohada ilg‘or xorijiy mamlakatlarning tajribalarini o‘rganish muhim ahamiyat kasb etadi [3]. Ushbu maqolada nusxa olish metodidan foydalanilgan. Ya’ni kiberjinoyatlar bilan bog‘liq ma’lumotlar, kiberjinoyatlar sodir etilgan holatlar, ularni aniqlash va tergov qilish, javobgarlik choralarini belgilash kabi masalalar xorijiy davlatlar tajribasidan kelib chiqib o‘rganilgan.

Xorijiy tajribani o‘rganishning afzalligi shundaki, biz amaliyot bilan yaqindan tanishgan holda ularda mavjud kamchiliklarni bartaraf etishimiz mumkin. Bundan tashqari, kiberjinoyatlar bilan bog‘liq ilmiy maqolalar, keyslar, qo‘llanma va normativ-huquqiy hujjatlar to‘planib, ularning tahlili maqolada batafsil keltirilgan. Shu bilan birga, kiberjinoyatlarni tadqiq qilish bilan bog‘liq cheklovlar, qonunchilikdagi mavjud bo‘shliqlar, joriy holatda ko‘rsatilgan muammolar va ularga yechimlar taqdim etilgan [4]. Shuningdek, ushbu muammolarni hal qilish yuzasidan qonunchilikka bir qator takliflar ham tavsiya etilgan.

Tadqiqot natijalari

Sohaga oid muammolarni hal qilish texnologik innovatsiyalarni keng qo‘llash va jamiyat rivojlanishini ta’minlash uchun zarurdir. Bir qator Yevropa olimlari D. Rebovich hamda J. Byrnelarning fikricha, so‘nggi yillarda kiberjinoyat va kiberxavfsizlik muammolari jadal sur’atlar bilan o‘sib bordi va bu yangi ilmiy izlanishlar yo‘nalishini shakllantirishga olib keldi (Bossler va Berenblum, 2019; Herath va boshq., 2022). Kiberjinoyat va kiberxavfsizlik ham insoniy, ham texnologik jihatlarni o‘z ichiga olganligini hisobga olsak, ushbu sohalardagi tadqiqotchilar fanlararo yondashuvni qo‘llashlari kerak, afsuski, bu sohalardagi adabiyotlar cheklangan hisoblanadi. Huquq sohasidagi olimlar – birinchi navbatda kriminologlar ko‘pincha kiberjinoyatlarning tarqalishi va dinamikasini qo‘llash va sinovdan o‘tkazish orqali tekshiradilar. Aksincha, kiberjinoyatlarning kelib chiqish sabablarini o‘rganayotgan olimlar, asosan, kiberjinoyat va kiberxavfsizlik bo‘yicha tadqiqotlarning son-sanoqsiz mavzularini o‘rganishdi, lekin ular an’anaviy ravishda e’tiborni qaratishdi (Brands & Van Doorn, 2022). Huquqni muhofaza qilish organlarining tashkiliy innovatsiyalari, transformatsiyasi nuqtayi nazaridan kiberjinoyatlarga javoban moslashish borasida Nowacki va Willitsning fikrlari shundan iboratki, bugungi kunda huquq-tartibot idoralari o‘rtasida kiberjinoyatchilikka qarshi kurashish bo‘linmalari 2013–2023-yillar davomida ‘‘uch baravar’’ ko‘payganini hamda kiberjinoyatchilik muammosining o‘sishini ta’kidlaydi. Muammoga javoban moslashish uchun davlat va mahalliy huquqni muhofaza qilish idoralari o‘rtasidagi sa’y-harakatlar qonunchilik doirasida kiberjinoyatlarni tergov qilish uchun ko‘proq resurslarni ajratishga qaratilishi lozimligi aytilgan. Shunday qilib, kiberjinoyatchilik bo‘linmalari o‘z-o‘zidan umumiy ko‘rsatkich bo‘lishi mumkin emas. Kiberjinoyatchilikka qarshi kurashishdagi salohiyatli kadrlar va mahalliy huquqni muhofaza qilish organlarining imkoniyatlarini kengaytirish lozim.

1996-yilda Yevropa Kengashi AQSh, Kanada va Yaponiya hukumati vakillari bilan birgalikda kompyuter jinoyatlarini qamrab oluvchi dastlabki xalqaro shartnoma loyihasini ishlab chiqdi [5]. Butun dunyo bo‘ylab fuqarolik libertar guruhlari shartnomadagi Internet-provayderlardan (ISP) o‘z mijozlarining tranzaksiyalari haqidagi ma’lumotlarni saqlash va bu ma’lumotni taomilga ko‘ra topshirishni talab qiluvchi qoidalarga darhol norozilik bildirishdi. Shartnoma ustida ishlash shunga qaramay davom etdi va 2001-yil 23-noyabrda Yevropa Kengashining Kiberjinoyatchilik to‘g‘risidagi konvensiyasi (Budapesht konvensiyasi) 30 ta davlat tomonidan imzolandi. Konvensiya 2004-yilda kuchga kirdi. Terrorchilik faoliyati, irqchilik va ksenofobik kiberjinoyatlarni qamrab oluvchi qo‘shimcha protokollar 2002-yilda taklif qilingan va 2006-yilda kuchga kirgan [6].

Yuqoridagilardan ko‘rishimiz mumkinki, kiberjinoyatlarning asosiy obyekti bu kompyuter axborotidir. Kompyuter axboroti, taqdim etilish shaklidan qat’i nazar axborot hisoblash tizimlari, tarmoqlari va ularning tarkibiy qismlaridagi ma’lum bir xos matnda aniq ma’noga ega bo‘lgan tushunchalarni ichiga oluvchi shaxs, predmet, dalil, voqea, hodisa kabi obyektlar haqidagi bilimlar, ma’lumotlardir. Ushbu turdagi jinoyatlar axborot texnologiyalaridan qonuniy, xavfsiz foydalanishni ta’minlovchi munosabatlarga tajovuz qiladi. Jinoyat obyektining to‘rt bo‘g‘inli tuzilishga ega ekanligi haqidagi nazariyaga asoslanadigan bo‘lsak, axborot texnologiyalaridan g‘ayriqonuniy foydalanish bilan bog‘liq jinoiy tajovuzning umumiy obyektini jinoyat qonuni bilan muhofaza etiladigan barcha ijtimoiy munosabatlar majmui, maxsus obyektini jamoat xavfsizligi va jamoat tartibi, turdosh obyektini axborot texnologiyalaridan qonuniy va xavfsiz foydalanish borasidagi ijtimoiy munosabatlar majmui tashkil qiladi. Bevosita obyekti esa muayyan moddaning nomi va dispozitsiyasidan kelib chiqib aniqlanadi [8].

Tadqiqot natijalari tahlili

Yangi texnologiyalar har bir sohaga ko‘plab qulayliklar taqdim etish bilan birgalikda yangi jinoiy imkoniyatlarni ham vujudga keltiradi. Shubhasiz, bitta farq raqamli qurilmalardan foydalanishdir, ammo jinoiy faoliyatning turli sohalari o‘rtasida mavjud bo‘lishi mumkin bo‘lgan har qanday farq uchun texnologiyaning o‘zi yetarli emas. Jinoyatchilarga firibgarlik, bolalar pornografiyasi va intellektual mulk savdosi, shaxsning ma’lumotlarini o‘g‘irlash yoki kimningdir shaxsiy hayoti daxlsizligini buzish uchun raqamli qurilma kerak emas. Bu faoliyatlarning barchasi “kiber” prefiksi hamma joyda paydo bo‘lishidan oldin mavjud edi. Kiberjinoyat, ayniqsa, Internet bilan bog‘liq, ba’zi yangi noqonuniy harakatlar bilan bir qatorda mavjud jinoiy xatti-harakatlarning kengayishini anglatadi.

Aksariyat kiberjinoyatlar jismoniy shaxslar, korporatsiyalar yoki hukumatlar haqidagi ma’lumotlarga hujumlardan iborat bo‘ladi. Hujumlar moddiy muhitda sodir bo‘lmasa-da, ular shaxsiy yoki korporativ virtual muhitda sodir bo‘ladi, bu Internetdagi odamlar va muassasalarni belgilaydigan axborot atributlari to‘plamidir [9]. Boshqacha qilib aytganda, raqamli asrda bizning virtual identifikatorlarimiz kundalik hayotning muhim elementlari hisoblanadi. Biz hukumatlar va korporatsiyalarga tegishli bo‘lgan bir nechta kompyuter ma’lumotlari bazalarida raqamlar va identifikatorlar to‘plamaymiz. Kiberjinoyat bizning hayotimizda tarmoqqa ulangan raqamli

ISSN 2181-2179
DOI: 10.51788/tsul.ccj.

qurilmalarning markaziy o‘rinni egallaganligini, shuningdek, shaxsiy identifikatsiya kabi ishonchli ko‘rinadigan faktlarning xavfsizligi yaxshi ta’minlanmaganligini ko‘rsatadi. Kiberjinoyatning muhim jihati cheksizligidir, ya’ni harakatlar juda katta masofalar bilan ajratilgan yurisdiksiyalarda sodir bo‘lishi mumkin. Bu huquqni muhofaza qilish organlari uchun jiddiy muammolarni keltirib chiqaradi, chunki ilgari mahalliy yoki milliy jinoyatlar endi xalqaro hamkorlikni talab qiladi. Sayyorani qamrab oluvchi tarmoq sifatida Internet jinoyatchilarga real dunyoda ham, tarmoqning o‘zida ham bir nechta yashirinish joylarini taklif etadi. Biroq yerda yurgan odamlar o‘zlaridan iz qoldirishi kabi kiberjinoyatchilar ham izlarini yashirish uchun barcha sa’y-harakatlariga qaramay, o‘zlarining shaxslari va joylashgan yerlari haqida izlar qoldiradilar. Bunday izlar “artifaktlar” deb ataladi. Quyida kiberjinoyatlarning sodir etilish sabablari keltirilgan:

Zaif qurilmalar. Yuqorida aytib o‘tganimizdek, samarali xavfsizlik choralarining yo‘qligi kiberjinoyatchilar uchun oson nishon bo‘lgan zaif qurilmalarning keng doirasining mavjudligi;

Shaxsiy motivatsiya. Kiberjinoyatchilar ba’zida o‘zlari yomon ko‘rgan yoki muammosi bo‘lgan odamlardan qasos olish uchun kiberjinoyat sodir etishadi;

Moliyaviy motivatsiya. Kiberjinoyatchilar va xakerlik guruhlarining eng keng tarqalgan motivatsiyasi, bugungi kunda aksariyat hujumlar ulardan moddiy foyda olishga qaratilgan [10].

Kiberjinoyat turli xil faoliyat turlarini qamrab olib, raqamli qurilmalarda saqlanadigan ma’lumotlarning yaxlitligiga tajovuz va noqonuniy ravishda olingan raqamli ma’lumotlardan firma yoki jismoniy shaxsni ta’qib qilish, zarar yetkazish yoki shantaj qilish uchun foydalanish kabi shaxsiy yoki korporativ maxfiylikning asosiy buzilishini o‘z ichiga olgan jinoyatlar hisoblanadi. Turli kompaniyalar raqamli qurilmalarga josuslik dasturlari, qurilmaning joylashuv yeri, qurilma egasining ma’lumotlarini ko‘rsatuvchi dasturlarni o‘rnatishmoqda. Bunda kompaniyalar ushbu dasturlar faqatgina jinoyatlarning oldini olish, jinoyatchilarni ta’qib qilish maqsadida foydalanishini aytib o‘tishgan. Shunga qaramay, shaxsiy ma’lumotlarni o‘g‘irlashi mumkin bo‘lgan smartfonga biriktirilgan josuslik dasturi hukumatlar tomonidan siyosatchilar, hukumat rahbarlari, huquq himoyachilari, dissidentlar va jurnalistlarni kuzatish uchun yashirin ravishda keng qo‘llangan [11]. Kompyuter jinoyatga qo‘shimcha vosita sifatida qo‘llanadigan jinoyatlar, masalan, noqonuniy olingan ma’lumotlarni saqlash uchun kompyuterdan foydalanish. Raqamli qurilma va dasturlar rivojlangan sari ularning turlari ham ko‘payib bormoqda. Quyida kiberjinoyatlarning eng keng tarqalgan turlari, ularning sodir etilish usullari bilan tanishishingiz mumkin.

Internetdagi firibgarlik

Internetda ijtimoiy tarmoq foydalanuvchilarining aldash usullari ko‘payib bormoqda. Ulardan biri Internet firibgarligi hisoblanadi. Internetdagi firibgarlik qurbonlarni aldash yoki ekspluatatsiya qilish uchun Internetga kirish imkoniga ega onlayn xizmatlar va dasturlardan foydalanishni o‘z ichiga oladi. “Internet firibgarligi” atamasi, odatda, Internet yoki elektron pochta orqali sodir bo‘ladigan kiberjinoyatchilik faoliyatini, jumladan, shaxsiy ma’lumotlarni o‘g‘irlash, “phishing”

va odamlardan pul undirish uchun mo‘ljallangan xakerlik faoliyatini o‘z ichiga oladi. Onlayn xizmatlar orqali jabrlanuvchilarni nishonga olgan internet firibgarliklari tufayli har yili millionlab dollar zarar ko‘rilmoqda. Internetdan foydalanishning kengaygani va kiberjinoyatchilik texnikasi yanada murakkablashgani sari bu raqamlar ortib bormoqda. Internet firibgarligining bir nechta turlari mavjud bo‘lib, ular quyidagilardan iborat [12]:

– “Phishing”: shaxsiy ma’lumotlar, login ma’lumotlari va moliyaviy ma’lumotlarni almashishda qurbonlarni aldash uchun elektron pochta va onlayn xabar almashish xizmatlaridan foydalanish.

– Ma’lumotlarning buzilishi: maxfiy, himoyalangan ma’lumotlarni xavfsiz joydan o‘g‘irlash va ularni ishonchsiz muhitga ko‘chirish. Bunga foydalanuvchilar va tashkilotlardan o‘g‘irlangan ma’lumotlar kiradi.

– Xizmatni rad etish (DoS): jinoyat sodir etish uchun onlayn xizmatga, tizimga yoki tarmoqqa trafik kirishini to‘xtatish.

– Zararli dasturiy ta’minot: foydalanuvchilarning qurilmalariga zarar yetkazish, ma’lumotlarni o‘chirish, ularni o‘g‘irlash uchun zararli dasturlardan foydalanish.

Cyberstalking. “Cyberstalking” – veb-saytlar, qidiruv tizimlari, ijtimoiy tarmoqlar orqali ta’qib qilish. Ushbu jinoyat odatda shaxsning ijtimoiy tarmoqlaridagi sahifalari e-mail manzili, shaxsiy yozishmalaridan tashqari juda xavfli ta’qib qiluvchi dasturlar orqali ham amalga oshirilishi mumkin. Masalan, “key logging” dasturlari. Bu ta’qib qiluvchi eng kuchli dasturlardan biri hisoblanadi. Ya’ni bunda ushbu dastur o‘rnatilgan qurilmada amalga oshirilgan yozishmalar, ilovalarga berilgan qidiruv buyruqlari, xullas, barcha yozuvlarni onlayn ravishda kuzatish imkoniyati mavjud bo‘ladi.

Kiberterrorizm. Kiberterrorizm – tahdid yoki qo‘rqitish orqali siyosiy yoki mafkuraviy yutuqlarga erishish uchun tahdid qiluvchi zo‘ravonlik harakatlarini amalga oshirishga da’vat qilish uchun Internetdan foydalanish. Kompyuter viruslari, kompyuter “worms”, “phishing”, zararli dasturlar, dasturlash skriptlari kabi vositalar yordamida kompyuter tarmoqlarini, xususan, Internetga ulangan raqamli qurilmalarni qasddan, keng miqyosda buzish harakatlari kiberterrorizmning sodir etilish shakllari bo‘lishi mumkin [13].

Bolalar pornografiyasi. Bolalar pornografiyasi voyaga yetmagan shaxslarning jinsiy aloqa qilishi bilan bog‘liq tasvirlar, rasmlar, videolarni internetda tarqatishdan iborat jinoyat hisoblanadi. Ushbu jinoyatni sodir etuvchilarning 98,9 foizi erkaklar bo‘lib, ularning o‘rtacha yoshi 41 ni tashkil etadi. AQSh da ushbu jinoyatni sodir etganlar soni 2022-yilda 1435 tani tashkil etib, ulardan 98,7 foizi ozodlikdan mahrum qilish jazosiga hukm etilgan. Ijtimoiy muhandislik – shaxsiy ma’lumotlarga kirishda inson xatolaridan foydalanish uchun mo‘ljallangan manipulyatsiya usuli. Xakerlar soxta identifikatsiya va turli xil psixologik hiylalar yordamida sizni aldab, shaxsiy yoki moliyaviy ma’lumotlarni oshkor qilishlari mumkin. Bunga erishish uchun ular “phishing” firibgarliklari, spam elektron pochta yoki tezkor xabarlar va hatto soxta veb-saytlarga tayanishi mumkin [14].

Parollarni buzish. Xakerlar parollarni olishning turli usullaridan foydalanadilar. Bunda xakerlar kirish uchun barcha mumkin bo‘lgan parollar kombinatsiyani taxmin

ISSN 2181-2179
DOI: 10.51788/tsul.ccj.

qilishga urinadilar. Xakerlar parol birikmalarini aniqlashga kirisjganda harflar, raqamlar va belgilarning turli kombinatsiyalarini yaratish uchun oddiy algoritmlardan ham foydalanishlari mumkin. Yana bir usul lug‘at hujumi sifatida tanilgan bo‘lib, bu dastur parol maydonlariga umumiy so‘zlarni kiritib, ulardan birortasi ishlashi yoki yo‘qligini ko‘rish imkonini beradi.

Zararli dasturlar bilan zararlangan qurilmalar. Xakerlar zararli dasturlarni o‘rnatish uchun foydalanuvchi qurilmasiga kirib borishi mumkin. Ular potensial qurbonlarni elektron pochta, tezkor xabarlar va veb-saytlar yoki yuklab olinadigan tarkibga ega bo‘lgan tarmoqlar, dasturlar orqali nishonga olishlari mumkin [15].

Botnetlar. Botnet – bu kiberjinoyatning bir turi bo‘lib, unda jinoyatchi bir nechta kompyuterlarni egallab oladi va ularni jinoiy faoliyatni amalga oshirish uchun birlashtiradi. Botnetlarda jinoyatchilar yuzlab yoki hatto millionlab qurilmalarga ulanishlari mumkin, bu esa ushbu jinoyatlarni to‘xtatishni qiyinlashtiradi. Ya’ni bu holatda, botnetdagi qurilmalarning joylashuv hududi turli davlatlarni ko‘rsatishi mumkin. Bu holatda ko‘rsatilgan manzillarning hammasini tekshirib chiqish ko‘p vaqt talab qiladi. Bu vaqt ichida jinoyatchi o‘z maqsadiga erishib ulgurgan bo‘ladi. Shuning uchun ham ushbu jinoyat eng xavfli kiberjinoyat turi hisoblanadi.

Xulosalar

Ushbu maqolada kiberjinoyatlar tushunchasi, ularning tahlili, turlari, sodir etilish usullari, ularga belgilangan javobgarlik choralari ko‘rsatilgan. Kiberjinoyatlarning soni raqamli dunyo rivojlangan sari oshib bormoqda. Bugungi kunda, raqamli qurilmalar, dasturlarga bo‘lgan ehtiyojning yuqoriligi, odamlar hayotining bir qismi raqamli dunyoga ko‘chganligi hisobiga kiberjinoyatlarni sodir etish yanada qulaylashib bormoqda. Hukumatlar, huquqni muhofaza qilish organlarining asosiy maqsadi sodir etilayotgan kiberjinoyatlarga taalluqli normativ-huquqiy hujjatlarni ishlab chiqish, qonunchilikdagi bo‘shliqlarni bartaraf etish, amaliyotda yangi vujudga kelishi mumkin bo‘lgan kiberjinoyatlarning oldini olish va ularga nisbatan javobgarlik belgilanishini ta’minlash, aholini kiberjinoyatlarning turlari va ularni sodir etish usullari bilan tanishtirgan holda fuqarolarni ogohlikka chorlash hisoblanadi.

O‘zbekiston Respublikasida kiberjinoyatlar yangi turdagi jinoyatlar hisoblanib, jinoyat qonunchiligi ushbu jinoyatlarni to‘liq qamrab olmagan. Avvalo, kiberjinoyatlarning eng keng tarqalgan asosiy turlarini Jinoyat kodeksiga kiritish va ularga nisbatan javobgarlik choralarini belgilash lozim. Kiberjinoyatlarni tergov qilish, jinoyatchilarni aniqlash bo‘yicha O‘zbekiston Respublikasida muayyan normativ-huquqiy hujjatlar mavjud emas. Jinoyat-protsessual kodeksida bu sohada juda katta bo‘shliq mavjud bo‘lib, ushbu bo‘shliqni to‘ldirish uchun, avvalo, raqamli dalillarga mustaqil dalil sifatida maqom berilishi lozim. Kiberjinoyatlar boshqa jinoyatlardan o‘z xususiyatlari bilan farq qiladi. Demak, ularni tergov qilish ham odatiy jinoyatlarnikidan farqli bo‘lishi lozim. Kiberjinoyatlarni tergov qilish bo‘yicha xorijiy davlatlar tajribasini o‘rganish, ularni Jinoyat-protsessual kodeksiga kiritish, bu sohadagi xalqaro konvensiya va shartnomalarni ratifikatsiya qilish mavjud muammolarni hal qilishga yordam berishi mumkin.

Mazkur tadqiqot yuzasidan quyidagi takliflar berildi:

1. Kiberjinoyatlar profilaktikasining asosiy tamoyillari raqamli xavfsizlikni ta'minlash, risklarni baholash va boshqarish bo'yicha zamonaviy nazariyalar bilan muvofiq bo'lishi kerak. Bu tamoyillar, xususan, ISO/IEC 27001 va NIST modellari asosida ularning amaliyotda qo'llanishini ta'minlashi lozim.

2. Kiberjinoyatlar uchun intellektual va texnik usullar bilan jinoyatni profilaktika qilish bo'yicha qonun hujjatlarini ishlab chiqish, murakkab va global texnologik jinoyatlarga nisbatan qat'iy jazo va javobgarlik choralarini belgilash zarur.

3. Kiberxavfsizlikni nazorat qilish va profilaktikasi uchun akademik va muhandislik ilmiy-tadqiqot markazlarini tashkil etish, raqamli xavfsizlik model va algoritmlarini ishlab chiqish kerak.

REFERENCES

1. Borodkina T.N., Pavlyuk A.V. Kiberprestupleniya: ponyatiye, soderzhaniye i mery protivodeystviya [Cybercrime: concept, content and countermeasures]. *Social and political sciences*, 2018, vol. 1, pp. 135–137.

2. Salayev N.S., Ro'ziyev R.N. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar [National and international standards for combating cybercrime]. Tashkent, TSUL Publ., 2018, p. 139.

3. Toraxodjayeva I. O'zbekistonda Internet tarmog'i orqali sodir etiladigan jinoyatchilikka qarshi kurashish muammolari [Problems of combating crime committed through the Internet in Uzbekistan]. Tashkent, *Review of Law Sciences*, 2019, vol. 03, pp. 128–132.

4. Kochkina L. Definition of the concept "cybercrime". Selected types of cybercrime. *Siberian Criminal Procedure and Forensic Readings*, 2017, vol. 3 (17), pp. 2, 37–40.

5. Kibermakonda sodir etilgan jinoyatlarga qarshi kurashish: muammolar va yechimlar [Combating crimes committed in cyberspace: problems and solutions]. Proceedings of the Republican Scientific and Practical Conference. Academy of the Ministry of Internal Affairs of Uzbekistan Publ., 2022, pp. 253–259.

6. Technology Briefing Internet: S.E.C. *Issues Warning On Fraud* 2022, pp. 89–100. Available at: https://www.nytimes.com/2002/06/26/business/technology-briefing-internet- sec-issues-warning-on-fraud

7. Sherri G. Cyberstalking: Definition, Signs, Examples, and Prevention, 2023 pp. 233–237. Available at https://www.verywellmind.com/what-is-cyberstal-king-5181466

8. Rustamboyev M.H. O'zbekiston Respublikasi Jinoyat huquqi kursi. Maxsus qism. Jamoat xavfsizligi va jamoat tartibiga qarshi jinoyatlar. Harbiy xizmatni o'tash tartibiga qarshi jinoyatlar [Criminal Law Course of the Republic of Uzbekistan. Special Part. Crimes against public safety and public order. Crimes against the procedure for military service]. Tashkent, ILM ZIYO Publ., 2011, pp. 34–40.

ISSN 2181-2179
DOI: 10.51788/tsul.ccj.

9. Ro‘ziyev R.N., Salayev N.S. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar [National and international standards for combating cybercrime]. Tashkent, TSUL Publ., 2018, pp. 133–140.

10. Fayziyev O.R., Xusainov D.K. Axborot texnologiyalari sohasidagi jinoyatlar [Crimes in the field of information technology]. Tashkent., TSIL Publ., 2009, p. 63.

11. G‘aniyev S.K., G‘aniyev A.A. Elektron hisoblash mashinalari va tarmoqlari [Electronic computing machines and networks]. TSUL Publ., ILM ZIYO Publ., 2016, pp. 67–70.

12. Axborot-kommunikatsiya texnologiyalari izohli lug‘ati [Explanatory Dictionary of Information and Communication Technologies]. UNDP Office in Uzbekistan, 2010, pp. 70–77.

13. Kalamkaryan R.A., Migachev Yu.I. Mezhdunarodnoye pravo [International law]. Moscow, Eksmo Publ., 2004, pp. 45–60.

14. Niyozova S.S. Kiberjinoyatchilik. Tashkent, TSUL Publ., 2024, pp. 14–17. Available at: https://library-tsul.uz/kiberjinoyatchilik-niyozova-s-2024/

15. Anorboyev A.U. Kiberjinoyatchilik, unga qarshi kurashish muammolari va kiberxavfsizlikni ta’minlash istiqbollari [Cybercrime, problems of combating it and prospects for ensuring cybersecurity]. Tashkent, National Guard Institute Publ., 2020, p. 324.

KRIMINOLOGIYA
VA JINOIY ODIL SUDLOV

ILMIY-AMALIY JURNAL

2025-yil 2-son