

KIBER BEZORILIK FENOMENI: HUQUQIY TABIATI, TERGOV QILISH XUSUSIYATLARI VA JINOIY JAVOBGARLIKNI MUSTAHKAMLASH MASALALARI

Ibragimov Sirojiddin Bakpo'latovich

Huquqni muhofaza qilish akademiyasi magistraturasi

"Tergov faoliyati" mutaxassisligi tinglovchisi

Email: ibragimov.sirojiddin.7070@gmail.com

Annotatsiya

Mazkur ilmiy maqolada informatsion-telekommunikatsiya tarmoqlari orqali sodir etiladigan bezorilik (kiber bezorilik) fenomenining huquqiy tabiati, uning kriminalistik xususiyatlari, tergov qilish amaliyotida yuzaga keladigan muammolar hamda mazkur xatti-harakatlar uchun jinoiy javobgarlikni mustahkamlash istiqbollari tahlil qilinadi. Raqamli texnologiyalarning jadal rivojlanishi jinoiy faoliyatning elektron muhitga ko'chishiga sabab bo'lmoqda, bu esa an'anaviy bezorilik jinoyati doirasiga kirmaydigan yangi xatti-harakat turlarining paydo bo'lishiga olib keldi. Tadqiqotda kiber bezorilikning doktrinal tushunchasi asoslangan, uning asosiy ko'rinishlari tasniflangan va O'zbekiston Respublikasi qonunchiligidagi bo'shliqlar aniqlangan. Shuningdek, MDH davlatlari hamda Yevropa mamlakatlari qonunchiligining qiyosiy tahlili asosida mazkur soha tartibga solinishining xalqaro tajribasi umumlashtirilgan. Maqolaning amaliy qismida raqamli dalillar — videokuzatuv yozuvlari, mobil aloqa ma'lumotlari va ijtimoiy tarmoq materiallari bilan ishlash taktikasi yoritilgan. Yakunda kiber bezorilik uchun jinoiy javobgarlikni mustahkamlash bo'yicha ikki muqobil qonunchilik varianti va bosqichma-bosqich yondashuv taklif etilgan.

Kalit so'zlar: kiber bezorilik, jamoat tartibi, raqamli dalillar, informatsion-telekommunikatsiya tarmoqlari, tergov taktikasi, 277-modda, kvalifikatsiya, ijtimoiy tarmoqlar.

ФЕНОМЕН КИБЕР-ХУЛИГАНСТВА: ПРАВОВАЯ ПРИРОДА, ОСОБЕННОСТИ РАССЛЕДОВАНИЯ И ВОПРОСЫ УСТАНОВЛЕНИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ

Ибрагимов Сироджиддин Бакпулатович

Студент магистратуры Академии правоохранительных органов

по специальности «Следственная деятельность»

Email: ibragimov.sirojiddin.7070@gmail.com

Аннотация

В настоящей научной статье анализируются правовая природа хулиганства, совершаемого посредством информационно-телекоммуникационных сетей (кибер-хулиганство), его криминалистические особенности, проблемы, возникающие в следственной практике, а также перспективы установления уголовной ответственности за подобные деяния. Стремительное развитие цифровых технологий обуславливает перемещение преступной деятельности в электронную среду, что привело к появлению новых видов деяний, не охватываемых традиционным составом хулиганства. В исследовании обосновано доктринальное понятие кибер-хулиганства, классифицированы его основные формы и выявлены пробелы в законодательстве Республики Узбекистан. На основе сравнительно-правового анализа законодательства стран СНГ и европейских государств обобщён международный опыт

правового регулирования данной сферы. В практической части статьи освещена тактика работы с цифровыми доказательствами — записями видеонаблюдения, данными мобильной связи и материалами социальных сетей. В завершение предложены два альтернативных законодательных варианта установления уголовной ответственности за кибер-хулиганство и поэтапный подход к их реализации.

Ключевые слова: кибер-хулиганство, общественный порядок, цифровые доказательства, информационно-телекоммуникационные сети, тактика расследования, статья 277, квалификация, социальные сети.

THE PHENOMENON OF CYBER-HOOLIGANISM: LEGAL NATURE, PECULIARITIES OF INVESTIGATION AND ISSUES OF ESTABLISHING CRIMINAL LIABILITY

Ibragimov Sirojiddin Bakpolatovich

Master's Student at the Academy of Law Enforcement,
specializing in 'Investigative Activities'

Email: ibragimov.sirojiddin.7070@gmail.com

Annotation

This scientific article analyses the legal nature of hooliganism committed through information and telecommunications networks (cyber-hooliganism), its criminalistic features, problems arising in investigative practice, and the prospects for establishing criminal liability for such acts. The rapid development of digital technologies has caused the migration of criminal activity into the electronic environment, resulting in the emergence of new types of conduct not covered by the traditional composition of hooliganism. The study substantiates the doctrinal concept of cyber-hooliganism, classifies its main manifestations, and identifies gaps in the legislation of the Republic of Uzbekistan. Based on a comparative legal analysis of the legislation of CIS countries and European states, the international experience of legal regulation in this area is summarised. The practical part of the article highlights the tactics of working with digital evidence — video surveillance records, mobile communication data, and social network materials. In conclusion, two alternative legislative options for establishing criminal liability for cyber-hooliganism and a phased approach to their implementation are proposed.

Keywords: cyber-hooliganism, public order, digital evidence, information and telecommunications networks, investigation tactics, Article 277, qualification, social networks.

Kirish

XXI asrning ikkinchi choragiga kirib kelganimiz sari axborot-kommunikatsiya texnologiyalarining jamiyat hayotiga ta'siri tobora kengayib bormoqda. Internet, ijtimoiy tarmoqlar va messenjerlar bugungi kunda kundalik muloqotning, kasbiy faoliyatning va ijtimoiy munosabatlarning ajralmas qismiga aylanib ulgurdi. Biroq mazkur jarayon bilan bir qatorda jinoiy faoliyat shakllarining ham elektron muhitga ko'chishi kuzatilmoqda. Jamoat tartibiga qarshi qaratilgan eng keng tarqalgan jinoiy qilmishlardan biri bo'lgan bezorilik bundan mustasno emas: internet maydonida jinoyat alomatlariga ega, jamiyatga nisbatan ochiq hurmatsizlik ko'rsatuvchi va virtual muhitning xavfsizligini izdan

chiqaruvchi yangi xatti-harakatlar paydo bo'layotgani bugungi kunning dolzarb muammolaridan biri hisoblanadi.

2022–2026 yillarga mo'ljallangan “Yangi O'zbekistonning Taraqqiyot strategiyasi”da qonun ustuvorligini ta'minlash va inson qadrini huquqiy jarayonlarning asosiy mezon sifatida belgilash vazifasi ko'rsatib o'tilgan. Raqamli iqtisodiyot va elektron davlatni qurish davrida ushbu vazifani ijro etish fuqarolarning huquq va manfaatlarini nafaqat fizik, balki virtual muhitda ham samarali himoya qilishni taqozo etadi.

So'nggi yillar ichki ishlar organlari amaliyotini tahlil qilish shuni ko'rsatadiki, internet va ijtimoiy tarmoqlar vositasi orqali sodir etilayotgan bezorilik alomatlariga ega bo'lgan xatti-harakatlar soni sezilarli darajada ortib bormoqda. Bunga muvoziy ravishda, respublikada an'anaviy bezorilik ko'lemi ham yuqori darajada saqlanib qolmoqda: O'zbekiston Respublikasi Ichki ishlar vazirligi ma'lumotlariga ko'ra, 2024-yilda respublika bo'yicha 2 369 ta, 2025-yilda 2 255 ta bezorilik jinoyati qayd etilgan, 100 ming aholiga nisbatan ko'rsatkich mos ravishda 6,44 va 6,01 ni tashkil etgan¹. Ommaviy haqoratlash, guruhiy kiberta'qib, jamoat tartibini buzish harakatlarini suratga olib internetga joylashtirish, ijtimoiy tarmoqlarda behayolik mazmunidagi materiallarni ommalashtirish — bularning hammasi virtual muhitning zamonaviy ma'nodagi "jamoat maydoni"ga aylanib ulgurganini ko'rsatadi. Ayni paytda esa amaldagi O'zbekiston Respublikasi Jinoyat kodeksining 277-moddasi dispozitsiyasi, asosan, an'anaviy "ko'chadagi" bezorilikka yo'naltirilgan bo'lib, internet-muhitdagi xatti-harakatlarni to'liq qamrab olmaydi. Bu esa huquqni muhofaza qiluvchi organlar oldida kvalifikatsiya qiyinchiligini hamda dalillar bazasini shakllantirishdagi protsessual muammolarni keltirib chiqaradi.

Maqolaning ilmiy dolzarbligi aynan ushbu qonunchilik va amaliyot bo'shliqlarini tadqiq qilish, "kiber bezorilik" tushunchasini doktrinal jihatdan asoslash, unga oid tergov taktikasining o'ziga xos jihatlarini yoritish hamda mazkur sohani huquqiy tartibga solishni takomillashtirish bo'yicha aniq takliflarni ishlab chiqishdan iborat.

Tadqiqot natijalari

Kiber bezorilik tushunchasi va uning huquqiy tabiati

Zamonaviy jinoyatchilik tuzilmasining tahlili shuni ko'rsatadiki, elektron muhit jinoiy faoliyat uchun yangi "maydon" sifatida tobora ko'proq foydalanilmoqda. V.A. Meshcheryakov elektron dalillar tushunchasini ilk bor tizimli ravishda tadqiq qilgan olimlardan biri sifatida ularni "raqamli ko'rinishda, elektron qurilmalar xotirasida yoki ma'lumotlar uzatish tizimlarida saqlanadigan, ish holatlarini aniqlashda ahamiyatga ega bo'lgan ma'lumotlar" deb ta'riflaydi². Mazkur nuqtai nazar jinoyat qonunchiligi va kriminalistika fani oldida yangi metodologik masalalarni qo'ygan bo'lib, ularning yechimi bezorilik jinoyatining zamonaviy talqiniga ham to'g'ridan-to'g'ri tegishlidir.

Kiber bezorilik tushunchasini ilmiy-huquqiy jihatdan asoslash uchun, avvalo, uning mohiyatini ochib beruvchi mezonlarni aniqlash lozim. O'zbekiston Respublikasi Jinoyat kodeksining 277-moddasi dispozitsiyasi mazmunidan kelib chiqib, bezorilikning ikki asosiy belgisi ajratiladi: birinchidan, jamiyatda o'rnatilgan yurish-turish qoidalarini qasddan mensimaslik; ikkinchidan, jamoat tartibini

¹O'zbekiston Respublikasi Ichki ishlar vazirligining 2024–2025-yillar davomida qayd etilgan jinoyatchilik dinamikasi bo'yicha ma'lumotnomasi. — T., 2026.

²Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования: дис. ... д-ра юрид. наук. — Воронеж, 2001. — С. 92.

qo'pol ravishda buzish va jamiyatga nisbatan ochiq hurmatsizlik ko'rsatish. Mazkur belgilarning har ikkalasi ham virtual muhitda to'laqonli namoyon bo'lishi mumkin, garchi ularning aniqlash mexanizmi va huquqiy rasmiylashtirish tartibi o'ziga xos xususiyatlarga ega bo'lsa ham.

Ushbu pozitsiyadan kelib chiqib, kiber bezorilikka quyidagicha ta'rif berish mumkin: bu informatsion-telekommunikatsiya tarmoqlari va resurslari orqali, jamiyatda qabul qilingan yurish-turish qoidalarini qasddan mensimaslik shaklida namoyon bo'luvchi, jamoat tartibini qo'pol ravishda buzuvchi va jamiyatga nisbatan ochiq hurmatsizlik ko'rsatuvchi xatti-harakatlar majmuidir. Mazkur ta'rifda asosiy urg'u "jamoat tartibiga qarshi qaratilganlik" belgisiga qaratiladi — aynan shu element kiber bezorilikni shaxsga qarshi boshqa internet-jinoyatlardan (haqorat, tuhmat, qo'rqitish) ajratib turuvchi tashqi chegara rolini o'ynaydi.

Kiber bezorilikning tipik ko'rinishlari

Amaliyot va ilmiy tahlil asosida kiber bezorilikning quyidagi asosiy ko'rinishlarini ajratib ko'rsatish mumkin: internet-muhitda noma'lum va aniqlanmagan fuqarolar doirasiga qarshi ommaviy haqoratlash va jamiyatga nisbatan ochiq hurmatsizlik ko'rsatish; ijtimoiy tarmoqlar yoki messenjerlar orqali shaxsga yoki guruhga nisbatan qo'rqituv xarakteridagi xabarlar yuborish; ma'lum bir shaxsga qarshi ommaviy, uyushtirilgan kibermobbing tashkil etish; axloqqa zid va behayolik mazmunidagi materiallarni ommaviy tarqatish; bezorilik harakatlarini suratga olib, internetga joylashtirib, ularni ommaviy namoyish qilish orqali jamoat tartibini ikkilamchi ravishda buzish; internet-muhitda jinoyatga undovchi yoki tahrikchilik xarakteridagi xabarlar va videomateriallarni tarqatish. Har bir ko'rinish o'ziga xos subyektiv va obyektiv belgilarga ega bo'lib, ularni kvalifikatsiya qilishda individual yondashuvni talab qiladi.

M.X. Rustambayevning bezorilik jinoyatining subyektiv belgilariga oid fundamental ta'limotiga ko'ra, aybdor shaxsning o'z xatti-harakatlariga qasddan, ongli ravishda munosabatda bo'lishi, jamiyatda o'rnatilgan yurish-turish qoidalariga nisbatan hurmatsizlik ko'rsatishi bezorilik tarkibining asosiy subyektiv elementini tashkil etadi³. Mazkur nazariy yondashuv internet-muhitda sodir etiladigan bezorilik holatlariga ham to'liq tatbiq etilishi mumkin, chunki aybdor ijtimoiy tarmoq orqali o'z xatti-harakatlari ommaning keng doirasiga ko'zga tushishini va jamoat tartibiga ta'sir ko'rsatishini aniq tasavvur qiladi. Demak, kiber bezorilikning subyektiv jihati an'anaviy bezorilikdan printsipial farq qilmaydi — mazmunan u ham shunday ongli va qasddan sodir etiladigan qilmishdir.

Shuni ta'kidlash lozimki, yuqorida keltirilgan xatti-harakatlarning barchasi jamoat tartibiga qarshi qaratilganlik belgisiga ega bo'ladi faqat, ular ommaviy xarakterga ega bo'lgan, noaniq doiradagi shaxslar ko'ziga tushadigan va jamiyatning huquqiy-axloqiy tartibiga izdan chiqaruvchi ta'sir ko'rsatadigan taqdirdagina. Bu ajratuv kvalifikatsiya amaliyotida nihoyatda muhim — u kiber bezorilikni shaxsga qarshi jinoyatlardan ajratishning asosiy mezoni hisoblanadi.

Amaldagi qonunchilikdagi holat va undagi bo'shliqlar

O'zbekiston Respublikasi Jinoyat kodeksining joriy redaksiyasida "kiber bezorilik" atamasi yoki unga tegishli alohida jinoiy javobgarlik normasi mavjud emas. JK 277-moddasining dispozitsiyasi an'anaviy "jismoniy" bezorilik holatlariga yo'naltirilgan bo'lib, internet-muhitda sodir etilayotgan qilmishlarni to'laqonli tarzda qamrab olish imkoniyatiga ega emas. Amaliyotda bunday xatti-harakatlar, odatda, bir

³Rustambayev M.X. O'zbekiston Respublikasi jinoyat-huquq kursi. V tom. Maxsus qism: Darslik. – T., 2018. – B. 207–209.

nechta moddalar bo'yicha kvalifikatsiya qilinmoqda: tuhmat (JK 139-moddasi), haqorat (JK 140-moddasi), o'ldirish yoki sog'lig'iga og'ir shikast yetkazish bilan qo'rqitish (JK 112-moddasi), shuningdek, Ma'muriy javobgarlik to'g'risidagi kodeksning tegishli moddalari.

Biroq ushbu normalar kiber bezorilikning jamoat tartibiga qarshi qaratilgan tabiatini to'liq aks ettira olmaydi. Tuhmat va haqorat — shaxsga qarshi jinoyat turlari bo'lib, ularning obyektini aniq shaxsning sha'ni va or-nomusidir. JK 277-moddasi esa jamoat tartibini himoya qilishga yo'naltirilgan. Aynan jinoyatning obyektini va ijtimoiy xavflilik darajasidagi mazkur farq kiber bezorilikning mustaqil institutsional o'rnini asoslashning nazariy poydevori hisoblanadi.

Mavjud qonunchilik bo'shlig'i tergov amaliyotida quyidagi muammolarni keltirib chiqaradi. Birinchidan, mavjud moddalar bo'yicha kvalifikatsiya qilinayotgan qilmishlar uchun belgilangan jazo hamisha ham jinoyatning haqiqiy ijtimoiy xavfliligiga mutanosib kelmaydi. Ikkinchidan, ijtimoiy tarmoqlarda tarqalayotgan bezorilik mazmunidagi video va postlarga aniq va izchil huquqiy baho berish qiyin. Uchinchidan, internet-provayderlar va ijtimoiy tarmoq platformalari bilan tergov organlari o'rtasidagi hamkorlik uchun yetarli qonuniy asos yo'q. To'rtinchidan, kiber bezorilikka qarshi profilaktika tizimining samarali ishlashi qiyinlashmoqda.

Xorijiy davlatlar qonunchiligining qiyosiy-huquqiy tahlili

Jahon huquqshunoslik tajribasini o'rganish kiber bezorilik bo'yicha milliy qonunchilikni takomillashtirish uchun qimmatli material beradi. Mustaqil Davlatlar Hamdo'stligi davlatlarining jinoyat qonunchiligi ushbu yo'nalishda quyidagi umumiy xususiyatlarga ega: Rossiya Federatsiyasining JKsi (213-moddasi), Qozog'iston Respublikasining JKsi (293-moddasi), Belarus Respublikasining JKsi (339-moddasi), Qirg'iziston Respublikasining JKsi (280-moddasi), Tojikiston Respublikasining JKsi (237-moddasi) bezorilik uchun javobgarlikni yagona, uch qismli moddalar shaklida belgilaydi. Biroq ushbu davlatlarning hech birida internet-muhitda yoki raqamli vositalar yordamida sodir etiladigan bezorilik uchun alohida qonun normasi joriy etilmagan. Bu holat O'zbekiston Respublikasi uchun mintaqaviy miqyosda qonunchilik tashabbusini ilgari surish imkonini yaratadi.

Romano-german huquq oilasi davlatlari qonunchiligi printsiplial jihatdan boshqacha yondashuvni namoyon etadi. Germaniya Federativ Respublikasida "bezorilik" (Hooliganismus) tushunchasi yaxlit jinoyat-huquqiy kategoriya sifatida mavjud emas; uning funksional ekvivalentlari bir nechta maxsus normalar orqali qamrab olingan. Germaniya Jinoyat kodeksining § 125-moddasi "Landfriedensbruch" (jamoat tinchligini buzish) eng yaqin ekvivalent hisoblanadi. V.D. Fechnerning qayd etishicha, Germaniyada bezorilikning yaxlit normasi yo'qligi huquq-siyosiy tanlov natijasi bo'lib, individual zarar turlariga aniq yondashish tamoyili asosida shakllangan⁴.

Germaniya qonunchiligining kiber bezorilik masalasidagi ilg'or yondashuvi alohida e'tiborga loyiq. 2021-yilda StGBga § 126a-moddasi "Gefährdendes Verbreiten personenbezogener Daten" (shaxsiy ma'lumotlarni xavf tug'diradigan tarzda tarqatish — "doxing") kiritildi. Bu norma internet orqali amalga oshiriladigan shaxsga tajovuz uchun maxsus javobgarlik belgilaydi. Bundan tashqari, Germaniya huquqiy tizimidagi eng muhim hujjatlardan biri — 2017-yilda qabul qilingan "Tarmoq Huquqiy Qo'llab-quvvatlash qonuni" (NetzDG) hisoblanib, u ijtimoiy tarmoq platformalariga noqonuniy kontentni 24

⁴Fechner V.D. Die Strafvorschriften zum Landfriedensbruch — Grenzen und Konturen von § 125 StGB // Die Kriminalpolizei. — 2019. — März. — S. 14–18.

soat ichida o'chirish majburiyatini yuklaydi. Bu xorijiy qonunchilik tajribasi milliy qonun chiqaruvchi uchun muhim manba bo'lishi mumkin.

Fransiya Respublikasi qonunchiligi esa bezorilikka tegishli vazifani bir nechta maxsus moddalar vositasida bajaradi: Fransiya Jinoyat kodeksining R.623-1 va R.623-2 moddalari (tunda va haqoratli shovqin ko'tarish), 222-33-2-moddasi (onlayn ta'qib qilish — "harcèlement moral"), 322-1 va keyingi moddalari (mulkka shikast yetkazish). 2020-yilda qabul qilingan "Loi Avia" qonuni internet orqali tahdid va ta'qib qilish masalalarini tartibga solishga qaratilgan ilk muhim qadam bo'ldi, garchi keyinchalik uning ba'zi qoidalari Konstitutsiyaviy Kengash tomonidan bekor qilingan bo'lsa ham.

Xulosa sifatida ta'kidlash joizki, tahlil qilingan davlatlarning hech birida "kiber bezorilik" nomli alohida jinoyat-huquqiy norma mavjud emas. Germaniya va Fransiya kiber-muhtdagi shaxsga qarshi tajovuzlarni alohida normalar (doxing, onlayn ta'qib) orqali qamrab olgan bo'lsalar-da, bu normalar "jamoat tartibiga qarshi jinoyatlar" guruhiga kirmaydi — ular shaxsga qarshi jinoyatlar guruhiga tegishlidir. Demak, O'zbekiston Respublikasi ushbu masalada qonunchilik tashabbusini ilgari surish orqali MDH mintaqasida va keng xalqaro doirada ilg'or huquqshunoslik an'anasining asoschisi bo'lish imkoniga ega.

Kiber bezorilik ishlarini tergov qilish xususiyatlari

Kiber bezorilik ishlarini tergov qilishning o'ziga xos xususiyatlari, birinchi navbatda, uning kriminalistik tavsifida namoyon bo'ladi. N.P. Yablokovning kriminalistika nazariyasiga ko'ra, har bir jinoyat turi uchun kriminalistik tavsif elementlari (sodir etish usuli, vaziyat va joyi, izlar tizimi, jinoyatchi va jabrlanuvchi shaxsi) bir-biri bilan korrelyatsion aloqada bo'ladi — ma'lum bir elementdagi belgilar boshqa elementlar haqida asosli xulosa chiqarish imkonini beradi⁵. An'anaviy bezorilikdan farqli ravishda, kiber bezorilik jismoniy shakldagi jinoyat joyiga ega emas — uning "hodisa joyi" virtual muhitda, ya'ni ma'lum bir internet-sayt, ijtimoiy tarmoq platformasi, messenjer yoki forum doirasida shakllanadi. Bu vaziyat voqea joyini ko'zdan kechirish institutining zamonaviy sharoitda qayta ma'nolashtirilishini taqozo etadi.

Kiber bezorilikka xos izlar tizimi o'ziga xos xususiyatlarga ega: ma'lumotlarni saqlash serverlaridagi log-fayllar, IP-manzillar, foydalanuvchi akkauntlari metadata'si, kontent-joylashtirish vaqti va davomiyligi, platformaning texnik xabarlar, foydalanuvchilar o'rtasidagi o'zaro ta'sir tarixi — bularning barchasi kiber bezorilik ishining elektron dalillar bazasini tashkil etadi. Bu izlarning an'anaviy moddiy izlardan farqli o'laroq, jismoniy shaklga ega emasligi, osonlikcha nusxa olinishi, o'zgartirilishi yoki yo'q qilinishi mumkinligi, shuningdek, saqlash muddati platforma va servis-provaydarning siyosatiga bog'liqligi alohida taktik yondashuv zaruratini keltirib chiqaradi.

Kiber bezorilik subyektining shaxsiy xususiyatlari ham an'anaviy bezorilikdan farq qiladi. Agar an'anaviy bezorilik aksariyat hollarda 18–35 yoshdagi erkak subyektlar tomonidan, ko'pincha alkohol yoki narkotik vositalar ta'siri ostida sodir etilsa, kiber bezorilik uchun bunday umumlashtirilgan tipologiya qo'llanilishi qiyin. Kiber bezorilik subyektlari orasida voyaga yetmaganlar ulushi ancha yuqori bo'ladi, shuningdek, anonimlik va masofadan turib harakat qilish imkoniyati an'anaviy jinoyatchi ijtimoiy portretidan sezilarli farqlar beradi.

L.Ya. Drapkinning tergov vaziyatlari nazariyasiga ko'ra, tergov vaziyati jinoyat ishi tergovining ma'lum bosqichida mavjud bo'lgan axborot va imkoniyatlar majmui bo'lib, u tergovchi tomonidan qabul

⁵Яблоков Н.П. Криминалистика: учебник. — 4-е изд., перераб. и доп. — М.: Норма: ИНФРА-М, 2014. — С. 482.

qilinadigan taktik qarorlar mazmunini belgilaydi⁶. Ushbu nazariy poydevordan kelib chiqib, kiber bezorilik ishlari bo'yicha tergov vaziyatlarini axborot to'liqligi va jinoyatchi aniqlanganlik darajasiga ko'ra uch asosiy toifaga bo'lish mumkin: birinchi vaziyat — jinoyatchi aniq, uning akkaunti va shaxsiy ma'lumotlari to'liq ma'lum; ikkinchi vaziyat — akkaunt aniq, biroq uning egasi soxta ma'lumotlar bilan ro'yxatga olingan yoki shaxsi aniqlanmagan; uchinchi vaziyat — jinoyatchining izi ham (anonimayzerlar, VPN xizmatlari yoki hakerlik vositalaridan foydalanish sababli) aniq emas. Har bir vaziyat tergovning o'ziga xos taktikasini, maxsus bilim va texnik vositalardan foydalanishni talab qiladi.

Raqamli dalillar bilan ishlash taktikasi

Kiber bezorilik ishlarini muvaffaqiyatli tergov qilish uchun raqamli dalillar bilan ishlashning samarali taktikasiga asosiy e'tibor qaratilishi lozim. Ushbu taktikaning uch asosiy yo'nalishi ajratiladi: videokuzatuv yozuvlari va skrinshotlar bilan ishlash; mobil aloqa ma'lumotlarini olish va tahlil qilish; ijtimoiy tarmoqlar va messengerlardagi materiallar bilan ishlash.

Videokuzatuv yozuvlari va skrinshotlar kiber bezorilik ishlarida asosiy dalil turlaridan biri hisoblanadi. Ularning protsessual qiymatini ta'minlash uchun quyidagi tartibda olinishi tavsiya qilinadi: skrinshot sana, vaqt va aniq URL-manzil aks etgan holda saqlanadi; mutaxassis yoki guvohlar ishtirokida raqamli muhitda voqea joyini ko'zdan kechirish bayonnomasi tuziladi; olingan materiallar autentifikatsiyasini tasdiqlaydigan tizimli bayonnoma rasmiylashtiriladi; zarur hollarda kompyuter-texnik ekspertiza tayinlanadi. Ushbu tartibga rioya qilinmaganda sudda dalillarning maqbulligi masalasida bahslar yuzaga kelishi mumkin.

Videokuzatuv yozuvlari bilan ishlashning asosiy muammosi — saqlash muddatining cheklangan ekanligidir. Xususiy videokuzatuv tizimlari odatda 7–30 kun ichida eski yozuvlarni o'chirib, ularning ustiga yangilarini yozadi. Davlat tizimlari yozuvi esa, qoidaga ko'ra, 30 kun atrofida saqlanadi. Bu holat tergovchidan yozuvlarni olish masalasini eng yuqori darajadagi tezkorlik bilan hal etishni talab qiladi. Amaliyotda shunday hollar uchrashi mumkinki, dalillar tushirilib ketgunga qadar olish imkoniyati yo'qoladi — bu esa ishning dalil bazasini jiddiy zaiflashtiradi.

Mobil aloqa ma'lumotlari kiber bezorilik ishlarida jinoyatchining harakatlarini qayta tiklash, shaxsini aniqlash va jinoyat sheriklari bilan aloqalarini aniqlashda muhim dalil manbai vazifasini bajaradi. O'zbekiston Respublikasida faoliyat yuritayotgan mobil operatorlar tomonidan saqlanadigan ma'lumotlar bu borada muhim ahamiyatga ega. Qo'ng'iroqlar va SMS-xabarlar yozuvlari (CDR — Call Detail Records), bazaviy stansiya ma'lumotlariga asoslangan joylashuv xizmatlari, telefon qurilmasining o'zidan olinadigan ma'lumotlar (qo'ng'iroq tarixi, messenger xabarlar, foto va videolar, GPS-navigatör tarixi, internet-brauzer tarixi, ijtimoiy tarmoq ilovalari) — hammasi kompleks tergov harakatlari vositasida olinadi.

Shu o'rinda shuni ta'kidlash lozimki, shifrlangan messengerlar (WhatsApp, Telegram, Signal) ma'lumotlarini olish katta texnik va huquqiy qiyinchiliklar bilan bog'liq. Ko'plab jinoyatchilar VPN xizmatlari orqali o'zlarining asl joylashuvini yashirishi, bir martalik yoki soxta SIM-kartalardan foydalanishi tergov jarayonini murakkablashtiradi. Bu muammolarning yechimi faqat kompleks — huquqiy, texnik va xalqaro hamkorlik — yondashuvni taqozo etadi.

Ijtimoiy tarmoqlar va messengerlardagi materiallar bilan ishlashning ikki asosiy yo'nalishi mavjud: ochiq manbalardan ma'lumot yig'ish (OSINT — Open Source Intelligence) va yopiq ma'lumotlarni

⁶Драпкин Л.Я. Основы теории следственных ситуаций. — Свердловск: Изд-во Уральского ун-та, 1987. — С. 17.

platforma-operatorlardan rasmiy so'rov orqali olish. Dastlabki bosqichda tergovchi maxsus ruxsatsiz ochiq profillardan, kanallardan va postlardan ma'lumotlarni to'plashi mumkin. Bu materiallar screenshot vositasida yoki maxsus dasturiy vositalar yordamida saqlanadi va protsessual tarzda rasmiylashtiriladi. Yopiq ma'lumotlar bilan ishlash ancha murakkab: xorijiy serverlarda joylashgan platformalardan (Meta, X, TikTok, YouTube) rasmiy so'rov orqali ma'lumot olish xalqaro huquqiy yordam tartibidan foydalanishni taqozo etadi, bu esa bir nechta oy davom etishi mumkin bo'lgan jarayondir.

Raqamli dalillarni ekspertiza qilish maqsadida quyidagi maxsus ekspertiza turlari qo'llaniladi: video-texnik ekspertiza (yozuvning haqiqiyli, manipulyatsiya qilinmaganligi, yozib olingan sanasi va vaqtini aniqlash); kompyuter-texnik ekspertiza (raqamli qurilmalardagi ma'lumotlarni texnik o'rganish, o'chirilgan fayllarni tiklash); fonoskopik ekspertiza (audio yozuvlardagi ovozni identifikatsiya qilish); kriminalistik portret ekspertizasi (videokameradagi shaxs yuzini gumon qilinuvchi bilan qiyoslash); lingvistik ekspertiza (matn yoki nutqdagi so'zlarning semantik mazmunini, haqorat, tahdid, behayolik alomatlarini baholash). Kiber bezorilik ishlarida ayniqsa lingvistik va kompyuter-texnik ekspertizalar muhim o'rin egallaydi.

Jinoiy javobgarlikni mustahkamlash bo'yicha qonunchilik takliflari

Yuqorida keltirilgan tahlillar asosida kiber bezorilik uchun jinoiy javobgarlikni mustahkamlash bo'yicha ikki muqobil qonunchilik variantini taklif etish mumkin.

A varianti — O'zbekiston Respublikasi Jinoyat kodeksiga yangi 277¹-modda ("Kiber bezorilik") kiritish. Bu variantning afzalliklari shundaki, yangi modda kiber bezorilikning o'ziga xos xususiyatlarini (internet-muhit, anonimlik, virtual tarzda ko'p shaxslarga ta'sir qilish) to'laqonli ravishda aks ettira oladi, kvalifikatsion belgilar aniq belgilanishi mumkin, jazo tizimi jinoyatning haqiqiy ijtimoiy xavfililigiga mutanosib tarzda ajratib taqdim etiladi va qonuniy aniqlik yuqori darajada ta'minlanadi. Variantning kamchiliklari esa Jinoyat kodeksi tarkibining kengayishi va boshqa moddalar (139, 140, 112-modda) bilan kvalifikatsiyada mumkin bo'lgan ziddiyatlar hisoblanadi.

B varianti — amaldagi JK 277-moddasiga yangi band yoki qism kiritish orqali kiber bezorilik alomatini kvalifikatsion belgi sifatida mustahkamlash. Buning ikki shakli mumkin: 2-qismga yangi band (masalan, "f" bandi — informatsion-telekommunikatsiya tarmoqlari, shu jumladan internet tarmog'i orqali sodir etilgan bezorilik) qo'shish yoki alohida 4-qism sifatida kiritish. B variantining afzalliklari — mavjud qonunchilik tuzilmasini saqlash, minimal o'zgarishlar orqali huquqiy takomillashtirishni amalga oshirish, mavjud Oliy sud Plenumi qarori (9-sonli, 2002-yil 14-iyun) asosiy holatda qo'llanilishi imkoniyati va kvalifikatsiya amaliyotining uzluksizligi. Kamchiliklari esa kiber bezorilikning o'ziga xos xususiyatlarining to'liq aks ettirilmasligi va internet-muhitda sodir etilishining avtomatik ravishda "jamiyatga ochiq hurmatsizlik" belgisini ta'minlamasligi bo'lishi mumkin.

Ikki variantni qiyosiy baholashga asoslanib, quyidagi bosqichma-bosqich yondashuv tavsiya etiladi. Qisqa muddatli (1–2 yil) strategiyada — B variantini amalga oshirish maqsadga muvofiq. Bu qadam amaliy muammolarning aksariyat qismini tez hal etish imkonini beradi. O'rta muddatli (3–5 yil) strategiyada esa to'plangan amaliyot tajribasi asosida A variantiga o'tish — alohida 277¹-modda kiritish taklif etiladi. Mazkur yondashuv kiber bezorilikning mustaqil huquqiy institut sifatida shakllanishini ta'minlaydi va qonunchilik tizimini zamonaviy talablarga muvofiqlashtiradi.

Har ikki variantni amalga oshirishda O'zbekiston Respublikasi Oliy sudi Plenumining 2002-yil 14-iyundagi 9-sonli qaroriga muhim tushuntirishlar kiritish zarur, xususan: "jamoat tartibini qo'pol

ravishda buzish" tushunchasining internet-muhitga tatbiqi; kiber bezorilikning mayda huquqbuzarlikdan ajratish mezonlari; raqamli dalillarni baholash mezonlari; ijtimoiy tarmoqlardan olingan materiallarga protsessual baho berish bo'yicha. Bundan tashqari, Jinoyat-protsessual kodeksiga "Elektron dalillar bilan ishlash tartibi" alohida bobini kiritish, raqamli dalil tushunchasining qonuniy ta'rifini, ularni olish tartibini, mustahkamlashning texnik talablari va platforma-operatorlar bilan hamkorlik tartibini belgilash tavsiya etiladi. Mazkur huquqiy takomillashtirishlar Germaniya qonunchiligining StPO § 100a–100g moddalarini va NetzDG qonuni tajribasini namuna sifatida hisobga olgan holda ishlab chiqilishi maqsadga muvofiqdir.

Xulosa

O'tkazilgan tadqiqot natijalari asosida quyidagi asosiy xulosalar ilgari surilishi mumkin. Birinchidan, axborot-kommunikatsiya texnologiyalarining rivojlanishi bezorilik jinoyatining yangi, o'ziga xos ko'rinishi — kiber bezorilikning paydo bo'lishiga olib keldi. Ushbu fenomen jamoat tartibiga qarshi qaratilgan tabiati bilan xarakterlanadi va an'anaviy bezorilikdan faqat sodir etish muhiti va vositalari jihatidan farq qiladi.

Ikkinchidan, kiber bezorilik tushunchasi informatsion-telekommunikatsiya tarmoqlari va resurslari orqali jamiyatda qabul qilingan yurish-turish qoidalarini qasddan mensimashda namoyon bo'luvchi, jamoat tartibini qo'pol ravishda buzuvchi va jamiyatga nisbatan ochiq hurmatsizlik ko'rsatuvchi xatti-harakatlar majmui sifatida ta'riflanishi mumkin. Ushbu ta'rifda markaziy o'rinni "jamoat tartibiga qarshi qaratilganlik" belgisi egallaydi — aynan shu element kiber bezorilikni shaxsga qarshi boshqa internet-jinoyatlardan ajratib turuvchi mezondir.

Uchinchidan, O'zbekiston Respublikasi Jinoyat kodeksining joriy redaksiyasi kiber bezorilik uchun alohida javobgarlik normasini nazarda tutmaydi. Amaldagi moddalar (139, 140, 112-moddalarini) ushbu xatti-harakatlarning jamoat tartibiga qarshi qaratilgan tabiatini to'liq aks ettira olmaydi. Bu qonunchilik bo'shlig'i tergov va kvalifikatsiya amaliyotida jiddiy muammolar keltirib chiqaradi.

To'rtinchidan, MDH va romano-german huquq oilasi davlatlari qonunchiligining qiyosiy tahlili tahlil qilingan barcha mamlakatlarda kiber bezorilik uchun alohida jinoyat-huquqiy norma mavjud emasligini ko'rsatdi. Bu holat O'zbekistonga mintaqaviy va kengroq xalqaro miqyosda qonunchilik tashabbusini ilgari surish imkonini yaratadi.

Beshinchidan, kiber bezorilik uchun jinoiy javobgarlikni mustahkamlash bo'yicha ikki muqobil variant taklif etilgan: A varianti — JKga alohida 277¹-modda kiritish; B varianti — amaldagi 277-moddaga yangi band yoki qism qo'shish. Bosqichma-bosqich yondashuv optimal deb e'tirof etiladi: qisqa muddatda B variantini, o'rta muddatda A variantini amalga oshirish.

Oltinchidan, kiber bezorilik ishlarini tergov qilish raqamli dalillar bilan kompleks ishlashni, maxsus ekspertiza turlarini (video-texnik, kompyuter-texnik, fonoskopik, lingvistik) qo'llashni, shuningdek, xalqaro hamkorlik mexanizmlarini samarali tashkil etishni taqozo etadi. Ushbu sohada huquqni muhofaza qilish akademiyasi va ichki ishlar bo'linmalari kadrlarining raqamli kriminalistika bo'yicha malakasini oshirish, texnik ta'minotni yangilash alohida ahamiyatga ega.

Yettinchidan, O'zbekiston Respublikasi Prezidenti tomonidan ilgari surilayotgan jamoat xavfsizligini mustahkamlash va inson qadrini himoya qilishga yo'naltirilgan strategik maqsadlar kiber bezorilikka qarshi kurashni ham qamrab olishi lozim. Zamonaviy bezorilik — faqat ko'chadagi emas, balki virtual maydondagi jamoat tartibini ham izdan chiqaruvchi qilmishdir va unga qarshi samarali kurashish uchun qonunchilik hamda tergov metodikasi doimiy takomillashtirib borilishi kerak.

Tadqiqot natijalari nazariy jihatdan kriminalistika va jinoyat huquqi fanini rivojlantirishga, amaliy jihatdan huquqni muhofaza qiluvchi organlar samaradorligini oshirishga, shu orqali fuqarolarning jamoat tartibi sohasidagi huquq va manfaatlarini samarali himoya qilishga xizmat qilishi kutilmoqda.

Ibragimov Sirojiddin Bakpolatovich

Foydalanilgan adabiyotlar

1. O'zbekiston Respublikasi Jinoyat kodeksi (1994-yil 22-sentabrdagi 2012-XII-sonli Qonun bilan tasdiqlangan). // URL: <https://lex.uz/uz/docs/111453>
2. O'zbekiston Respublikasi Jinoyat-protsessual kodeksi (1994-yil 22-sentabrdagi 2013-XII-sonli Qonun bilan tasdiqlangan). // URL: <https://lex.uz/uz/docs/111460>
3. "2022–2026 yillarga mo'ljallangan Yangi O'zbekistonning Taraqqiyot strategiyasi". // Qonunchilik ma'lumotlari milliy bazasi.
4. O'zbekiston Respublikasi Oliy sudi Plenumining 2002-yil 14-iyundagi "Bezorilikka oid ishlar bo'yicha sud amaliyoti haqida"gi 9-sonli qarori (keyingi tahrirlari bilan). // URL: <https://lex.uz/mact/-1452654>
5. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования: дис. ... д-ра юрид. наук. — Воронеж, 2001. — 317 с.
6. Rustambayev M.X. O'zbekiston Respublikasi jinoyat-huquq kursi. V tom. Maxsus qism: Darslik. – T., 2018. – B. 207–209.
7. Яблоков Н.П. Криминалистика: учебник. — 4-е изд., перераб. и доп. — М.: Норма: ИНФРА-М, 2014. — 768 с.
8. Драпкин Л.Я. Основы теории следственных ситуаций. — Свердловск: Изд-во Уральского ун-та, 1987. — 163 с.
9. Fechner V.D. Die Strafvorschriften zum Landfriedensbruch — Grenzen und Konturen von § 125 StGB // Die Kriminalpolizei. – 2019. – März. – S. 14–18.
10. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. — Ст. 213 Хулиганство. // URL: http://www.consultant.ru/document/cons_doc_LAW_10699/
11. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V. — Ст. 293 Хулиганство. // URL: <https://adilet.zan.kz/rus/docs/K1400000226>
12. Уголовный кодекс Республики Беларусь от 9 июля 1999 года № 275-З. — Ст. 339 Хулиганство. // URL: https://kodeksy-by.com/ugolovnyj_kodeks_rb/339.htm
13. Strafgesetzbuch der Bundesrepublik Deutschland (StGB) — §§ 125, 125a, 126a, 130. // URL: <https://www.gesetze-im-internet.de/stgb/>
14. Netzwerkdurchsetzungsgesetz (NetzDG) vom 1. September 2017. // URL: <https://www.gesetze-im-internet.de/netzdg/>
15. Code pénal de la République française. — Art. R.623-1, R.623-2, 222-33-2, 322-1. // URL: <https://www.legifrance.gouv.fr/>
16. O'zbekiston Respublikasi Ichki ishlar vazirligining 2024–2025-yillar davomidagi jinoyatchilik dinamikasi bo'yicha rasmiy ma'lumotnomalari. – Toshkent, 2025–2026.