elita.uz

Elektron Ilmiy Jurnal

№.1 (3)
2025

elita.uz

№ 1 (3) 2025

MUNDARIJA

elita.uz

№ 1 (3) 2025

KIBERJINOYATLARNI TERGOV QILISHNING O‘ZIGA XOS XUSUSIYATLARI

Nodirjon Xabibiddinov

n.xabibiddinov@tsul.uz

Toshkent davlat yuridik universiteti
Jinoyat-protsessual huquqi kafedrasi o‘qituvchi-yordamchisi
Magistratura va sirtqi ta’lim fakulteti
Kiber huquq yo‘nalishi talabasi

Annotatsiya. Zamonaviy raqamli texnologiyalarning jadal rivojlanishi natijasida kiberjinoyatlar soni va murakkablik darajasi sezilarli darajada ortib bormoqda. Ushbu tadqiqot kiberjinoyatlarni tergov qilishning o'ziga xos xususiyatlari, mavjud muammolar va ularning yechim yo'llarini tahlil qiladi. Maqolada kiberjinoyatlarning asosiy turlari, sodir etilish usullari, tergov jarayonida qo'llaniladigan zamonaviy texnologiyalar va xalqaro hamkorlik masalalari ko'rib chiqilgan. Tadqiqot natijalari raqamli dalillarni to'plash murakkabligi, maxsus texnik bilimlar zarurligini va kiberxavfsizlik sohasidagi mutaxassislarning yetishmasligini ko'rsatadi. Kiberjinoyatlarga qarshi samarali kurashish uchun normativ-huquqiy bazani takomillashtirish va xalqaro standartlarni joriy etish tavsiya etilgan.

Kalit so’zlar: kiberjinoyatlar, raqamli dalillar, kiberxavfsizlik, kompyuter-texnik ekspertiza, xalqaro hamkorlik, raqamli kriminalistika, kiberhujumlar, tergov metodikasi.

KIRISH

Zamonaviy axborot texnologiyalari jamiyat hayotining barcha jabhalariga kirib kelishi natijasida yangi turdagi jinoyatlar – kiberjinoyatlar paydo bo‘la boshladi. Global internet tarmog‘i va raqamli texnologiyalarning jadal rivojlanishi natijasida kiberjinoyatlar soni va ularning murakkablik darajasi yildan-yilga ortib bormoqda.

Kibermuhitda sodir etilgan jinoyatlar soni kompyuter tarmoqlaridan foydalanuvchilar soniga mutanosib ravishda o‘sib bormoqda va Xalqaro jinoyat politsiyasi tashkiloti – Interpol hisob-kitoblariga ko‘ra, global internet tarmog‘ida ushbu jinoyatchilikning o‘sish sur’ati sayyoramizda eng tezkor hisoblanadi[1].

Hozirgi vaqtda globallashuv va u olib keladigan muammolar kuchaymoqda. Bunday sharoitda transmilliy kiberjinoyatlarga qarshi kurashishda barchaning ishtirok etish masalasi juda muhim hisoblanadi. Kiberjinoyatlarga qarshi kurashishda kurashish vositalari va usullarini ishlab chiqishda jinoyatning latentlik darajasidan xabardor bo‘lishi kerak. Mutaxassislar taxminiga ko‘ra “kompyuter jinoyatlari”ning latentligi AQShda 80%ni, Buyuk Britaniyada - 85%ni, Germaniyada - 75%ni, Rossiyada - 90%ni tashkil qiladi[2].

Tahlillarga ko‘ra, dunyo bo‘ylab har yili 500 milliondan ortiq kiber hujumlar sodir etiladi. Har soniyada 12 nafar insondan biri virtual makonda sodir etilgan hujumlar qurboniga aylanadi. Amerika Qo‘shma Shtatlari, Angliya, Germaniya, Belgiya kabi rivojlangan davlatlarda jinoyatlarning 60-65 foizi kiber hujumlar orqali sodir etilmoqda[3]. O‘zbekistonda ham so‘nggi uch yilda bu turdagi jinoyatlar 25 baravarga ko‘paygan. 2023-yilning 11 oyida 5,5 mingta kiberjinoyat sodir etilgan[4]. Shundan 70 foizi bank kartalari bilan bog‘liq firibgarlik va o‘g‘irlik jinoyatlari hisoblanadi. Bundan tashqari, noqonuniy bank-moliya operatsiyalari orqali o‘zgalarning plastik kartadagi mablag‘larini o‘zlashtirish, zararli viruslar tarqatish, qimor va tavakkalchilikka asoslangan onlayn o‘yinlar, diniy aqidaparastlikka qaratilgan axborot xurujlari, onlayn savdo maydonidagi firibgarlik jinoyatlari ko‘payib bormoqda. Hozirda bunday jinoyatlarning oldini olish uchun profilaktik chora-tadbirlar bilan bir qatorda ularni fosh etish bo‘yicha qator tashkiliy-texnik tadbirlar amalga oshirilmoqda.

Kiberjinoyatlarning xavfliligi shundaki, ular nafaqat alohida shaxslarga, balki davlat organlari, bank tizimlari, ta’lim va sog‘liqni saqlash muassasalari kabi

muhim infratuzilma obyektlariga ham jiddiy zarar yetkazishi mumkin. So‘nggi yillarda O‘zbekistonda ham kiberjinoyatchilikka qarshi kurashish masalasiga alohida e’tibor qaratilmoqda. Xususan, “Kibexavfsizlik to‘g‘risida”gi qonun qabul qilinishi, kiberxavfsizlik markazi tashkil etilishi hamda huquqni muhofaza qiluvchi organlar tarkibida maxsus bo‘linmalar faoliyatining yo‘lga qo‘yilishi buning yaqqol dalilidir. Lekin, kiberjinoyatlarni tergov qilish jarayonida bir qator muammolar mavjud bo‘lib, ular:

- raqamli dalillarni to‘plash va saqlashning murakkabligi;

- kiberjinoyatlarning tranmilliy xususiyati tufayli xalqaro hamkorlikni talab etishi;

- maxsus texnik bilim va ko‘nikmalarning zarurligi;

- raqamli kriminalistika sohasidagi mutaxassislarning yetishmasligi;

- zamonaviy dasturiy-texnik vositalarning qimmatligi kabilardir.

Yuqoridagilardan kelib chiqib, ushbu maqolaning maqsadi kiberjinoyatlarni tergov qilishning o‘ziga xos xususiyatlarini o‘rganish, mavjud muammolarni aniqlash va ularning yechimiga qaratilgan taklif-tavsiyalar ishlab chiqishdan iborat. Tadqiqot doirasida quyidagi vazifalar belgilangan:

- kiberjinoyatlarning zamonaviy turlari va ularning sodir etilish usullarini tahlil qilish;

- xorijiy davlatlarning kiberjinoyatlarni tergov qilish tajribasini o‘rganish;

- kiberjinoyatlarni tergov qilish samaradorligini oshirish bo‘yicha amaliy tavsiyalar ishlab chiqish.

METODLAR

Adabiyotlar tahlili: Ushbu tadqiqot kiberjinoyatlarni tergov qilishning o‘ziga xos xususiyatlarini aniqlash maqsadida yetakchi nazariy va amaliy manbalarni tahlil qiladi. Bu jarayonda Google Scholar, Science Direct va Cyberleninka kabi ilmiy ma’lumotlar bazalaridan foydalanildi. Adabiyotlar tahlilida kiberjinoyatlarning texnik va huquqiy jihatlari, tergov usullari, shuningdek, xalqaro tajribalar e’tiborga olindi. Shu bilan birga, kiberjinoyatlarni tergov qilish, raqamli dalillarni yig‘ish va tahlil qilish haqidagi ilmiy maqolalar, kitoblar va konferensiya materiallari ko‘rib chiqildi.

Hodisani o‘rganish (case study): Toshkent davlat yuridik universiteti Kriminalistika va sud ekspertizasi kafedrasi tomonidan tashkil etilgan “Raqamli

kriminalistika” ilmiy to‘garagi doirasida namunaviy raqamli dalillar tahlil qilindi va bir nechta holatlar ko‘rib chiqildi. Ushbu holatlarda qo‘llanilgan tergov strategiyalari va raqamli kriminalistika usullarining samaradorligi o‘rganildi.

Kontent-tahlil: Kiberjinoyatlarni tergov qilishda foydalaniladigan raqamli vositalar haqida ma’lumot to‘plash maqsadida xalqaro kiberxavfsizlik tashkilotlarining veb-saytlari, tahliliy hisobotlar va tegishli hukumat portallari o‘rganildi.

Qiyosiy tahlil: Kiberjinoyatlarni tergov qilish jarayonida turli davlatlarda qo‘llanilgan usullar va yondashuvlarning samaradorligini qiyoslash uchun davlatlararo qiyosiy tahlil o‘tkazildi. Bunda tegishli tashkilotlarning kiberjinoyatlar bilan bog‘liq faoliyat ko‘rsatkichlari va xalqaro hamkorlik natijalari tahlil qilindi.

NATIJALAR

Ushbu tadqiqot natijalari kiberjinoyatlarni tergov qilishdagi asosiy qiyinchiliklarni, samarali strategiyalarning ahamiyatini yoritadi. Natijalar quyidagilarni o‘z ichiga oladi:

Asosiy qiyinchiliklar: Tahlil natijalariga ko‘ra, tergovchilarning ko‘pchiligida kiberjinoyatlarni tergov qilishda texnologik bilimlar yetarli emas va texnik infratuzilmaning kamchiliklari muammoli bo‘lib kelmoqda. Ayniqsa, IP-manzillarni aniqlash, ma’lumotlarni tiklash, va transmilliy jinoyatlarni tergov qilishda huquqiy chegaralar qiyinchilik tug‘dirmoqda.

Yangi texnologiyalarning qo‘llanilishi: Natijalar kiberjinoyatlarni tergov qilishda sun’iy intellekt, mashinani o‘rganish (machine learning), va katta ma’lumotlarni (big data) tahlil qilish texnologiyalari sezilarli yutuqlarni ta’minlayotganini ko‘rsatadi. Ayniqsa, raqamli kriminalistika vositalaridan foydalanish va kiberxavfsizlik dasturlari kiberjinoyatlarning izini topish va dalillarni to‘plashda katta hissa qo‘shmoqda.

Kiberjinoyatlar bo‘yicha xalqaro hamkorlik va huquqiy tartibga solish: Case study natijalariga ko‘ra, kiberjinoyatlarni tegov qilishda tergovchilardan zarur kompyuter-texnik bilimlarni bilish ham talab etiladi. Tergovchilar sodir etilgan kiberjinoyat kompyuter tizimining aynan qayerida sodir etilganligini aniqlashi, raqamli dalilni tahlil qila olish qobiliyatiga ega bo‘lishi kerak. Shu bilan birga, kiberxavfsizlik sohasi ham alohida ahamiyatga ega.

O‘zbekiston, kiberxavfsizlik sohasida OIT (ITU) va boshqa xalqaro tashkilotlar bilan hamkorlik qilmoqda. O‘zbekiston Kiberxavfsizlik markazi (CERT.uz) OIT bilan hamkorlik qilish va xalqaro standartlarni joriy qilishda muhim rol o‘ynaydi. Shu bilan birga, O‘zbekiston IT sohasida hamkorlikni rivojlantirish maqsadida xalqaro tashkilotlar bilan hamkorlik qilishni o‘z ichiga olgan holda kiberjinoyatlarni oldini olish uchun qo‘shimcha tashkilotlar bilan hamkorlik qilmoqda. Bunday hamkorliklar, O‘zbekiston kiberxavfsizlik sohasidagi faoliyatni yaxshilash, kiberjinoyatlarni tekshuruvga olish, maxfiylik sozlamalarini ta’minlash va kiberxavfsizlikning o‘rnatilishi bilan bog‘liq xizmatlarni takomillashtirishga yordam beradi. Shu bilan birga, O‘zbekiston kiberxavfsizlik sohasidagi ilmiy va amaliy yondashuvni rivojlantirish, yangiliklar almashish va hamkorliklarni rivojlantirish uchun xalqaro standartlarga rioya qilishga intiladi.

Natijalar shuni ko‘rsatadiki, internet va ijtimoiy tarmoqlarda kiberjinoyatlar haqida keng ma’lumotlarning mavjudligi va jamoatchilikni ogoh qilish choralari kiberjinoyatlarning oldini olishda muhim rol o‘ynaydi. Shu bilan birga, odamlar o‘z shaxsiy ma’lumotlarini himoya qilishda ehtiyotkor bo‘lishlari, shaxsiy xavfsizlik choralari ko‘rishlari talab etiladi.

MUHOKAMA

Hozirgi raqamli asrda yangi turdagi kiberjinoyatlarning kundan kunga ortib borayotganligi to‘g‘ridan-to‘g‘ri dalillarni yig‘ishni qiyinlashtirayotganligi bilan bog‘liq va bu ko‘pincha bir nechta texnologiyalardan foydalanishni talab qiladi. Bugungi kunga qadar tadqiqotchilar ushbu sohada ko‘plab ilmiy ishlarni taqdim etishgan. Ushbu maqolada kiberjinoyatlar, ularning turlari va klassifikatsiyasi, kiberjinoyatlarni sodir etish usullari va vositalarining tahlili bo‘yicha tegishli ilmiy ishlarni o‘rganib chiqish orqali yetarli ma’lumotlar mavzuni tahlil qilish va muhokama qilish uchun olindi.

Kiberjinoyatlar qonunbuzarliklarni sodir etish uchun raqamli texnologiyalardan foydalanadigan keng ko‘lamli noqonuniy faoliyatni o‘z ichiga oladi. Bu faoliyatlarga shaxsiy ma’lumotlarni o‘g‘irlash (identity theft), fishing (phishing), xakerlik (hacking), to‘lov dasturi hujumlari, onlayn firibgarlik (ransomware) kabilar kiradi, lekin bular bilan cheklanmaydi. Kiberjinoyatchilar tomonidan qo‘llaniladigan usullar oddiy fishing elektron pochta xabarlaridan

tortib, murakkab zararli dastur hujumlarigacha xilma-xil va doimiy ravishda rivojlanib boradi. Xuddi shunday, kiberjinoyatlarni sodir etishda foydalaniladigan vositalar ham har xil bo‘lib, jumladan, komputerlar, tarmoqlar va dasturiy ta’minot va boshqalarni o‘z ichiga oladi. Umuman olganda, komputerlar, kommunikatsiya qurilmalari, tarmoqlar, internet, jahon tarmoqlari va kibermaydonda sodir etiladigan jinoyatlarning barchasi kiberjinoyat deb ataladi[5].

Kompyuter yoki kommunikatsiya qurilmasi quyidagi maqsadlarda foydalanilishi mumkin:

(a) jinoyatning obyekti (xakerlik, fishing) sifatida;

(b) jinoyatni sodir etish vositasi sifatida (bolalar pornografiyasi);

(c) shaxsiy ma’lumotlarga kirish, savdo sirlarini qo‘lga kiritish yoki boshqa g‘arazli maqsadlarda.

Kiberxavfsizlik tushunchasi esa ma’lumotlar, qurilmalar, kompyuter resurslari, kommunikatsiya qurilmalarini va ularning ichida saqlangan ma’lumotlarni ruxsat etilmagan kirish, foydalanish, fosh etish, buzishdan himoya qilish degan ma’noni anglatadi[6].

Komputer tizimiga qaratilgan jinoyatlar:

a. ***Xakerlik (Hacking)*** – bu keng tushunchali atama hisoblanib, komputer tizimiga hech qanday ruxsatsiz kirishga erishgan holda tizimdagi ma’lumotlarning yo‘qolishi, o‘g‘irlanishiga sabab bo‘luvchi yoki ma’lumotlarni butunlay yo‘q qilish maqsadini ifodalovchi harakat hisoblanadi. Bu harakat maxfiy ma’lumotlarni (foydalanuvchi nomlari, parollar, IP manzillar va boshqalar) olish va ulardan komputer tizimiga kirish va/yoki boshqarish uchun foydalanish orqali amalga oshiriladi[7].

Xakerlik bilan zararli aloqa birinchi marta 1970-yillarda dastlabki komputerlashtirilgan telefonlar nishonga aylangan paytda ro‘yxatga olingan. **“Freakerlar”** nomi bilan tanilgan texnologiyani yaxshi biladigan odamlar bir qator kodlar orqali shaharlararo qo‘ng‘iroqlar uchun pul to‘lash yo‘lini topadilar. Ular uzoq masofali telefon vaqtini o‘g‘irlash uchun apparat va dasturiy ta’minotni o‘zgartirish orqali tizimdan qanday foydalanishni o‘rgangan birinchi xakerlar bo‘ladi. Ular odamlarni komputer tizimlari jinoiy faoliyatga zaif ekanligini va murakkab tizimlar qanchalik murakkab bo‘lsa, ular kiberjinoyatlarga shunchalik moyil bo‘lishini tushunishga majbur qilishgan[8].

b. ***Xizmatni rad etish hujumi (Denial or Distributed Denial-of-service, (DDoS)*** — bu ma'lum bir axborot tizimi va resurslarning ish faoliyatini vaqtinchalik to'xtatish maqsadida amalga oshiriladigan hujum turidir. DoS va DDoS hujumlarining ko'plab shakllari mavjud bo'lsada, eng keng tarqalganlari: tarmoq resurslarining tugashi, protokol resurslarining tugashi va dastur resurslarining tugashidir[9].

DoS hujumi odatda bir nechta tizimlar yordamida nishondagi tarmoq yoki serverga katta miqdordagi trafikni yuborish orqali amalga oshiriladi va bu orqali u tizimning butun qismini egallaydi va natijada halokatga olib keladi.

c. Viruslar va zararli dasturlarni tarqatish - bugungi kundagi eng katta kiberjonayatlarning turi hisoblanadi. Ular umumiy yoki ma'lum bir maqsadga yo'naltirilgan bo'ladi. Ular zararli kodni kiritilgan va tarqatishga mo'ljallangan viruslar, troyanlar, josuslik dasturlari, reklama dasturlari va rootkitlar kabi shakllarda kelishi mumkin. Ular jabrlanuvchining komputer tizimiga yashirincha o'rnatiladi va tizimga oid maxviy ma'lumotlarga kirish va uzatish uchun ishlatilishi mumkin. Ba'zi hollarda, zararlangan tizimlar davlatga qarshi urush olib borish yoki odamlar orasida terror tarqatish kabi boshqa kiberjinoyatlarni bajarish uchun vosita sifatida ham ishlatilishi mumkin.

j. Fishing/Farming (Phishing/Pharming) - odatda soxta pochta orqali, ***fishing*** qurbonni soxta veb-saytlarga yo'naltiradi yoki shaxsiy/biznes tafsilotlarini oshkor qilish uchun ularni aldaydi[10]. ***Farming*** - bu kredit karta raqamlari, parollar yoki PIN-kod kabi maxfiy ma'lumotlarni kiritish uchun foydalanuvchini aldashga yo'naltirilgan hujum turi hisoblanib, haqiqiy veb-saytlarni soxta veb-saytlarga aylantirish orqali amalga oshiriladi[11]. Bu fishingdan farq qiladi, chunki tajovuzkor hech qanday URL yoki havolaga tayanishi shart emas, aksincha, u veb-sayt trafigini qonuniy veb-saytdan soxta veb-saytga yo'naltirishining o'zi kifoya.

Kiberjinoyatlarni sodir etishda qo'llaniladigan usullar.

Kiberjinoyatlarni sodir etish usullari deganda, kiberjinoyatchilar tomonidan raqamli texnologiyalardan foydalangan holda noqonuniy faoliyatni amalga oshirish uchun foydalanadigan turli xil texnika va yondashuvlarni nazarda tutish mumkin. Ushbu usullar xilma-xil va doimiy ravishda rivojlanib boradi, ko'pincha dasturiy

ta’minot, apparat yoki inson xatti-harakatlaridagi zaifliklardan foydalanalib sodir etiladi.

Cracking - bu kimningdir komputer tizimiga parollar yoki litsenziyalarni chetlab o‘tish orqali yoki tizim xavfsizligini ataylab buzadigan boshqa usullar bilan kirish. Bu foyda olish uchun yoki zararli boshqa maqsadlarda amalga oshirilishi mumkin[12].

Ma’lumotlarni o‘zgartirish (Data Diddling)- bu jarayon ma’lumotlarni komputer tizimi qayta ishlashidan oldin va qayta ishlash tugagandan so‘ng o‘zgartirishni o‘z ichiga oladi.

Buffer overflow. Buferlar - bu boshqa joyga ketishi kerak bo‘lgan qo‘shimcha ma’lumotlarni o‘z ichiga olish uchun yaratilgan vaqtinchalik ma’lumotlarni saqlash joylari hisoblanadi. Agar dastur yoki jarayon saqlashga mo‘ljallanganidan ko‘proq ma’lumotni saqlashga harakat qilsa, u qo‘shni buferlarga to‘lib-toshib, ulardagi haqiqiy ma’lumotlarni buzadi yoki qayta yozadi. U esa tizim ma’lumotlarini yo‘q qilish uchun ishlatiladi[13].

Ijtimoiy muhandislik (Social Engineering) - bu tizim/tarmoq haqida maxsus ma’lumotlarni berish uchun odamlarni aldash va manipulyatsiya qilish uchun texnik bo‘lmagan tajovuz hisoblanadi. Misol sifatida do‘stlik so‘rovlarini yuborish va/yoki asal idishlari (honeypots)dan foydalanishni keltirishimiz mumkin[14].

Steganografiya usuli (Steganograph)- bu yashirin xabarlarni shunday yozishni o‘z ichiga oladiki, jo‘natuvchi va qabul qiluvchidan boshqa hech kim biron bir xabarning mavjudligidan shubhalanmaydi. Masalan, oddiy ko‘rinadigan Lohri yoki Id stikerida terror guruhlari o‘rtasida yashirin xabarlar almashinuvi mavjud bo‘lgan[15].

Kiberjinoyatlarni sodir etishda qo‘llaniladigan vositalar.

Kiberjinoyatlarni sodir etish vositalari bu kiberjinoyatchilar o‘zlarining noqonuniy faoliyatini amalga oshirish uchun foydalanadigan dasturiy yoki apparat (software yoki hardware) komponentlari hisoblanadi. Bu vositalar oddiy dasturiy ilovalardan tortib, raqamli tizimlardagi zaifliklardan foydalanish uchun mo‘ljallangan murakkab apparat qurilmalarigacha bo‘lishi mumkin.

Masofaviy kirish troyanlari (Remote Access Trojans (RATs). RATlar tajovuzkorga jabrlanuvchining komputerini masofadan boshqarish imkonini

beruvchi zararli dasturdir[16]. Ushbu vosita ko‘pincha maxfiy ma’lumotlarni o‘g‘irlash yoki tizimga ruxsatsiz kirish uchun ishlatiladi.

Keyloggerlar. Keyloggerlar komputerda tugmalar bosishlarini yozib oladigan dasturiy yoki apparat qurilmalari hisoblanadi. Ular parollar, kredit karta raqamlari va boshqa maxviy ma’lumotlarni olish uchun ishlatiladi[17].

Botnetlar (Botnets). Botnetlar - bu botmaster deb nomlanuvchi bitta tajovuzkor tomonidan boshqariladigan buzilgan komputerlar tarmoqlari. Ushbu tarmoqlar DDoS hujumlari yoki spam kampaniyalari kabi muvofiqlashtirilgan hujumlarni boshlash uchun ishlatiladi.

Umuman olganda, kiberjinoyatchilarni sodir etishda qo‘llaniladigan usullar va vositalar kundan kunga texnologiya rivojlangani sayin va yangi kiberjinoyatlarning turiga qarab o‘zgarib turadi. Kiberjinoyatlarning har xil turlarini va kiberjinoyatchilar tomonidan qo‘llaniladigan usullarni o‘rganish orqali biz raqamli tizimlardagi zaifliklarni bartaraf etish strategiyalarini ishlab chiqishimiz mumkin.

Kiberjinoyatlarni aniqlash bo‘yicha zamonaviy yondashuvlar.

Har qanday jinoyatning sodir qilish mexanizmini bilmay turib, uni tergov qilish va taktik harakatlarni olib borish xato hisoblanadi. Yuqorida biz kiberjinoyatlarni sodir etish usullari va vositalarini tahlilini amalga oshirish orqali kiberjinoyatlarning umumiy tavsifi, ularning turlari, qanday usul va vositalar orqali sodir etilishi va ularni aniqlash texnikalari haqida tushunchalarga ega bo‘ldik.

Kiberjinoyatlarga qarshi taktik harakatlarni o‘tkazish dalillarni to‘plash, jinoyatni tahlil qilish va jinoyatchilarni qo‘lga olish uchun tizimli yondashuvni o‘z ichiga oladi. Taktik harakatlarni o‘tkazishning umumiy tartibini izohlaydigan bo‘lsak, ma’lum bir turdagi kiberjinoyat aniqlangandan so‘ng, birinchi qadam zararlangan tizimlarni keyingi zararni oldini olish uchun himoya qilish hisoblanadi. Bu buzilgan tizimlarni tarmoqdan uzib qo‘yish yoki ularni o‘chirishni o‘z ichiga oladi. Undan so‘ng, ta’sir qilingan tizimlarning kriminalistik tasvirlarini yaratish orqali barcha potensial raqamli dalillarni saqlash kerak bo‘ladi. Bu asl dalillarning saqlanib qolishi va uni o‘zgartirmasdan tahlil qilinishini ta’minlaydi. Bundan keyin kiberjinoyatni sodir etishda qo‘llaniladigan usullar va vositalarni aniqlash uchun kriminalistik tasvirlarni tahlil qilish kerak bo‘ladi. Shu ketma-ketlikda qolgan zarur amallafr bajarilib boriladi.

Kiberjinoyatlarni aniqlash usullarini ishlab chiqish bo‘yicha ko‘plab yondashuvlar mavjud va hozirgi kungacha turlicha tadqiqotlar olib borilgan.

Hozirgi kunda AQSH, Germaniya, Latviya kabi davlatlar amaliyotida kiberjinoyatlarni oldini olish va ularga qarshi kurashishda mashinani o‘rganish **(Machine learning) va Sun’iy intelekt (AI)** orqali kiberjinoyatlarni aniqlash texnikasi yo‘lga qo‘yilgan.

Ushbu texnologiyalar kiberjinoyatlarning sodir etish usullarini aniqlashda katta hajmdagi ma’lumotlarni tahlil qilish uchun ishlatiladi. Mashinani o‘rganish algoritmlari tarmoq trafigida (network traffic), foydalanuvchi faoliyatida (user activity) yoki tizim jurnallarida (system logs) noodatiy xatti-harakatlarni aniqlay oladi.

Neyron tarmoqlar (Neural networks). Sun’iy intellektning bir shakli bo‘lgan neyron tarmoqlar murakkab usullarni o‘rganish qobiliyati tufayli kiberjinoyatlarni aniqlash uchun kuchli vosita bo‘lib xizmat qiladi. Neyron tarmoqlardan elektron pochta xabarlari va veb-saytlarni fishing hujumlari belgilarini tahlil qilish uchun foydalanish mumkin. Ular umumiy fishing taktikalarini tanib olishni va foydalanuvchilarni ogohlantirishni yoki zararli kontentni bloklashni amalga oshirishi mumkin. Masalan, xorijlik kiberxavfsizlik mutaxassislari Chjan va Yuan fishing hujumlarini aniqlash uchun neyron tarmoqdan foydalangan. Ular fishing hujumlarini aniqlashda 95% aniqlikka erishgan holda ko‘p qatlamli neyron tarmog‘idan foydalanganlar[18].

Blokcheyn texnologiyasi (Blockchain texnology). Blokcheyn texnologiyasi bu kompyuterlar tarmog‘i bo‘ylab tranzaksiyalarni qayd qiluvchi markazlashtirilmagan, taqsimlangan tizim hisoblanadi. Har bir tranzaksiya “blok”da saqlanadi, keyinchalik u bloklar zanjiriga qo‘shiladi va tranzaksiyalarning xronologik yozuvini yaratadi. Blokcheyn xavfsiz autentifikatsiya va identifikatsiyani boshqarish uchun ishlatilishi mumkin, bu esa maxviy ma’lumotlar va tizimlarga ruxsatsiz kirish xavfini kamaytiradi. Shu bilan birga, bu texnologiya kiberjinoyatlarni aniqlash va oldini olish bilan shug‘ullanadigan turli subyektlar o‘rtasida xavfsiz va markazlashmagan ma’lumotlar almashishni osonlashtiradi. Bu esa tahdidlar haqida ma’lumot almashish va kiberjinoyatlarni tergov qilish uchun hamkorlik qilishda muhim rol o‘ynaydi[19].

Shu bilan birga, **OSForensics, Access Data FTK Imager, Autospy** kabi dasturlar foydalanuvchilarga kompyuterlardan raqamli dalillarni tez va samarali ravishda olish imkonini beruvchi keng qamrovli raqamli kriminalistik vositalar hisoblanadi. Ushbu dasturlar raqamli tergovni olib borish uchun muhim bo‘lgan juda ko‘p funksiyalarga ega.

Umuman olganda, kiberjinoyatlarni aniqlashning zamonaviy yondashuvlari kiberhujumlarni aniqlash imkoniyatlarini oshirish va ularga qarshi samarali kurashish uchun davlat idoralari, xususiy tashkilotlar va kiberxavfsizlik bo‘yicha mutaxassislar o‘rtasidagi o‘zaro hamkorlikka asoslanadi.

XULOSA VA TAKLIFLAR

Xulosa qilib shuni aytish mumkinki, kiberjinoyatlarga qarshi keng qamrovli xalqaro darajadagi qonunlarning yo‘qligi va kiberjinoyatlarni sodir etish usullari va vositalarining tez o‘zgarishi va rivojlanib borishi kiberjinoyatlarga qarshi kurashni yanada murakkablashtirmoqda. Shuningdek, internetning anonim tabiati va kiberjinoyatchilar tomonidan anti-kriminalistik texnikalarning qo‘llanilishi, tergovga qarshi texnikani bilmaslik huquqni muhofaza qilish idoralari uchun jiddiy to‘siqlarni keltirib chiqarmoqda va ko‘pincha ularning kiberhujumlarga qarshi samarali kurashishiga to‘sqinlik qilmoqda va kiberjinoyatchilar tomonidan qo‘llaniladigan eng yangi qurilmalar, dasturiy ta’minot va aloqa usullaridan xabardor bo‘lishni qiyinlashtirmoqda.

Ushbu muammolarni hal qilish va kiberjinoyatlarning oldini olish va tergov harakatlarini yaxshilash uchun quyidagi takliflarni berish mumkin:

- ***raqamli ekspertizani ISO/IEC 27037 xalqaro standartlariga moslashtirish bo‘yicha normativ-huquqiy hujjatlar ishlab chiqish;***
- ***umumiy va nazariy asoslar, raqamli kriminalistik texnika va taktika va metodikadan iborat bo‘lgan darsliklar yaratish;***
- ***kiberjinoyatlarning har bir turlari bo‘yicha alohida tergov qilish uslubyotini yaratish zarur.***

Foydalanilgan adabiyotlar

1. *Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society (10-11).*
2. *Gupta, B. B., & Dahiya, A. (2021). Distributed denial of service (DDOS) attacks: Classification, attacks, challenges and countermeasures (4-6). CRC Press.*
3. *Ghazi‐Tehrani, A. K., & Pontell, H. N. (2021). Phishing Evolves: Analyzing the Enduring Cybercrime. Victims & Offenders, 16(3), 316–342.*
4. *Deckard, J. (2005). Buffer overflow attacks: Detect, exploit, prevent (7-9). Elsevier.*
5. *Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: a survey. Future Internet, 11(4), 89.*
6. *Garcia, N. (2018). Digital steganography and its existence in cybercrime (5-6). Scientific and Practical Cyber Security Journal..*
7. *Zaytsev, O. (2006). Rootkits, Spyware/Adware, keyloggers and backdoors: Detection and neutralization (25-27). BHV-Petersburg..*
8. *Al-Khater, W., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020b). Comprehensive review of Cybercrime detection techniques. IEEE Access, 8, 137293–137311.*
9. *Shinde, A. (2021). Introduction to cyber security: Guide to the world of cyber security (3-5). Notion Press.*

Internet saytlari:

1. *Google Scholar. https://scholar.google.com/*
2. *CyberLeninka. https://cyberleninka.ru/*
3. *Science Direct.https://www.sciencedirect.com/*
4. *ResearchGate. https://www.researchgate.net/*
5. *Osforensics. https://www.osforensics.com/*

---

[1] https://www.interpol.int/Crimes/Cybercrime

[2].Vardanyan A.V., Nikitina E.V. Rassledovanieprestuplenii v sferevyso-kikhtekhnologiiikomp'yuternoiinformatsii Investigation of Hi-Tech and Computer Information Crimes]. Moscow, Yurlitinform Publ.

[3] https://aag-it.com/the-latest-cyber-crime-statistics/

[4] https://kun.uz/news/2023/12/20/ozbekistonda-2023-yilda-55-mingta-kiberjinoyat-sodir-etildi
[5] Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. 10-11
[6] Shinde, A. (2021, pp. 3-5). *Introduction to cyber security: Guide to the World of Cyber Security*. Notion Press.
[7] Bothra, H. (2017,pp. 9-10). *Hacking: Be a Hacker with Ethics*. KHANNA PUBLISHING.
[8] https://www.pandasecurity.com/en/mediacenter/types-of-cybercrime/
[9] Gupta, B. B., & Dahiya, A. (2021, pp. 4-6). Distributed denial of service (DDOS) attacks: Classification,
Attacks, Challenges and Countermeasures. CRC Press.
[10] Ghazi‐Tehrani, A. K., & Pontell, H. N. (2021). Phishing Evolves: Analyzing the Enduring Cybercrime. Victims & Offenders, 16(3), 316–342. https://doi.org/10.1080/15564886.2020.1829224
[11] https://www.proofpoint.com/us/threat-reference/pharming
[12] https://www.avast.com/c-cracking
[13] Deckard, J. (2005, pp. 7-9). *Buffer overflow attacks: Detect, Exploit, Prevent*. Elsevier.
[14] Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: a survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089
[15] Garcia, Natasha, (2018, pp. 5-6). Digital steganography and its existence in cybercrime. Scientific and Practical Cyber Security Journal.
[16] https://www.malwarebytes.com/blog/threats/remote-access-trojan-rat
[17] Zaytsev, O. (2006, pp. 25-27). *Rootkits, Spyware/Adware, keyloggers and backdoors: Detection and neutralization*. БХВ-Петербург.
[18] Al-Khater, W., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020b). Comprehensive review of Cybercrime detection techniques. *IEEE Access*, *8*, 137293–137311. https://doi.org/10.1109/access.2020.3011259
[19] https://blog.merklescience.com/general/investigating-blockchain-crimes-using-blockchain-forensics