KIBERJINOYATCHILIK VA UNGA QARSHI KURASHISHNING ZAMONAVIY USULLARI

Umirzaqova Tursunoy Akramjon qizi

Andijon Davlat Texnika Instituti 1-bosqich talabasi

umirzaqovatursunoy7@gmail.com

Annotatsiya: Ushbu maqola kiberjinoyatchilik tushunchasi, uning turlari va zamonaviy tahdidlarini tahlil qilishga bag‘ishlangan. So‘nggi yillarda axborot texnologiyalarining jadal rivojlanishi bilan kiberjinoyatchilik ham murakkablashib bormoqda, bu esa unga qarshi kurashishning yangi va samarali usullarini ishlab chiqishni taqozo etadi. Maqolada kiberhujumlarning eng keng tarqalgan turlari o‘rganiladi hamda ularning iqtisodiyot, davlat boshqaruvi va fuqarolar xavfsizligiga ta’siri yoritiladi.Shu bilan birga, maqolaning asosiy qismi kiberjinoyatchilikka qarshi kurashishning zamonaviy usullariga qaratilgan. Bunda sun’iy intellekt va mashinani o‘qitish texnologiyalarining kiberxavfsizlikdagi o‘rni, raqamli dalillarni to‘plash va tahlil qilish, hamda xalqaro hamkorlikning ahamiyati ko‘rsatib o‘tilgan. Xulosa qilib aytganda, maqola kiberjinoyatchilikni bartaraf etish uchun faqat texnologik yechimlar emas, balki qonunchilikni takomillashtirish, mutaxassislarni tayyorlash va aholining raqamli savodxonligini oshirish muhimligini ta’kidlaydi.

Kalit so‘zlar: Kiberjinoyatchilik, kiberxavfsizlik, raqamli forenzika, kiberhujum, sun'iy intellekt, axborot xavfsizligi, kiber tahdidlar.

Annotation: This article is devoted to the analysis of the concept of cybercrime, its types and modern threats. With the rapid development of information technologies in recent years, cybercrime has also become more complex, which requires the development of new and effective methods of combating it. The article examines the most common types of cyberattacks and highlights their impact on the economy, public administration

and the security of citizens. At the same time, the main part of the article focuses on modern methods of combating cybercrime. The role of artificial intelligence and machine learning technologies in cybersecurity, the importance of collecting and analyzing digital evidence, and international cooperation are highlighted. In conclusion, the article emphasizes the importance of improving legislation, training specialists and increasing the digital literacy of the population in order to eliminate cybercrime.

Keywords: Cybercrime, cybersecurity, digital forensics, cyberattack, artificial intelligence, information security, cyber threats.

Аннотация: Статья посвящена анализу понятия киберпреступности, ее видов и современных угроз. В связи с бурным развитием информационных технологий в последние годы киберпреступность также стала более сложной, что требует разработки новых и эффективных методов борьбы с ней. В статье рассматриваются наиболее распространенные виды кибератак и выделяется их влияние на экономику, государственное управление и безопасность граждан. При этом основная часть статьи посвящена современным методам борьбы с киберпреступностью. Отмечается роль технологий искусственного интеллекта и машинного обучения в обеспечении кибербезопасности, важность сбора и анализа цифровых доказательств, а также международного сотрудничества. В заключение статьи подчеркивается важность совершенствования законодательства, подготовки специалистов и повышения цифровой грамотности населения в целях ликвидации киберпреступности.

Ключевые слова: Киберпреступность, кибербезопасность, цифровая криминалистика, кибератака, искусственный интеллект, информационная безопасность, киберугрозы.

Bugungi tezkor rivojlanayotgan raqamli dunyoda texnologiya inson hayotining ajralmas qismiga aylanib ulgurdi. Biz onlayn muloqot qilamiz, moliyaviy operatsiyalarni amalga oshiramiz, masofadan turib ishlaymiz, ijtimoiy tarmoqlarda faoliyat yoritamiz va

mobil bankchilik kabi qulayliklardan muntazam foydalanamiz. Bu qulayliklar hayotimizni sezilarli darajada soddalashtirib, vaqtni tejash imkonini berdi. Ammo, har bir yorug‘likning soyasi bo‘lganidek, raqamli taraqqiyotning o‘ziga xos salbiy tomoni ham borki, bu – **kiberjinoyatchilik**dir. Kiberjinoyatchilik deganda, kompyuterlar va internet orqali amalga oshiriladigan noqonuniy xatti-harakatlar tushuniladi. Bu jinoyatlar oddiy firibgarlikdan tortib, davlatning muhim infratuzilmalariga qilingan yirik hujumlargacha bo‘lgan keng doirani qamrab oladi. Kiberjinoyatchilikning tez sur'atlar bilan o‘sishi global miqyosda jiddiy muammoga aylanib bormoqda. Bu jinoyatlar nafaqat milliardlab dollarlik iqtisodiy yo‘qotishlarga olib kelmoqda, balki shaxsiy ma’lumotlar xavfsizligiga, biznes faoliyatiga, va hatto milliy xavfsizlikka ham bevosita tahdid solmoqda. Shu sababli, bu muammoga qarshi kurashishning zamonaviy, har tomonlama va samarali usullarini ishlab chiqish hamda joriy etish bugungi kunning eng dolzarb masalasidir. Ushbu maqolada kiberjinoyatchilikning asosiy turlari, uning ta’siri va unga qarshi kurashishning zamonaviy texnologik, huquqiy va ijtimoiy choralari batafsil tahlil qilinadi. Maqola kiberxavfsizlikning murakkab va o‘zgaruvchan dunyosini tushunishga yordam beradi.

Kiberjinoyatchilikning asosiy turlari va ularning salbiy ta’siri

Kiberjinoyatchilar o‘zlarining xavfli maqsadlariga erishish uchun turli xil usullardan foydalanishadi. Har bir hujum turi o‘ziga xos xususiyatlarga ega bo‘lib, turli darajadagi zararlar yetkazishga qaratilgan. Ushbu jinoyatlar tobora ommalashib, yangi shakllarga kirib bormoqda.

1. **Fishing (onlayn firibgarlik):** Bu eng keng tarqalgan kiberjinoyat turlaridan biri hisoblanadi. Unda jinoyatchilar o‘zlarini ishonchli tashkilotlar, masalan, yirik bank, pochta xizmati, mashhur ijtimoiy tarmoq yoki hukumat agentligi deb ko‘rsatishadi. Ular aldov yo‘li bilan shaxsiy ma’lumotlarni, masalan, parollar, kredit karta raqamlari, bank hisob raqamlari yoki ijtimoiy sug‘urta raqamlarini qo‘lga kiritishga urinishadi. Ko‘pincha bu shubhali havolalari bor elektron pochta yoki xabarlar orqali amalga oshiriladi. Fishing hujumlari nafaqat oddiy foydalanuvchilarga, balki yirik kompaniyalarning xodimlariga ham qaratilgan bo‘lishi mumkin. Birgina xodimning

ehtiyotsizligi butun kompaniyaning ma’lumotlar bazasiga kirish imkoniyatini ochib berishi mumkin. Bu esa kompaniya uchun katta moliyaviy va obro‘ga doir yo‘qotishlarga olib keladi.

2. **Zararli dasturlar (viruslar, troyanlar, ransomware):** Bu dasturlar zarar yetkazish maqsadida kompyuter tizimlariga ruxsatsiz kirib boradi. **Viruslar** boshqa dasturiy ta’minotlarga qo‘shilib, o‘zini nusxalash orqali keng tarqaladi. **Troyanlar** esa foydali dastur niqobi ostida tizimga kiradi, lekin aslida maxfiy ma’lumotlarni o‘g‘irlash yoki tizim ustidan nazorat o‘rnatishga xizmat qiladi. Eng xavfli turlardan biri esa **ransomware** (to‘lov talab qiluvchi dasturlar) bo‘lib, ular foydalanuvchining ma’lumotlarini shifrlab, ularni qayta ochish uchun katta miqdorda pul talab qiladi. Bunday hujumlar nafaqat shaxslarga, balki kasalxonalar, o‘quv yurtlari va yirik korxonalarga ham qilingan holatlar ko‘p uchraydi. Bu holatlar tizimning ishini to‘xtatib, odamlar hayotiga xavf solishi mumkin.

3. **DDoS (Distributed Denial-of-Service) hujumlari:** Bu hujumlar veb-sayt yoki onlayn-xizmatni sun’iy tarzda yuklab, uning ishlamay qolishiga olib keladi. Minglab, hatto millionlab kompyuterlardan bir vaqtning o‘zida bir manzilga so‘rovlar yuborilishi oqibatida tizim haddan tashqari yuklanib, xizmat ko‘rsatishni to‘xtatadi. Bu esa biznes uchun juda katta iqtisodiy yo‘qotishlarga sabab bo‘ladi. Masalan, onlayn-do‘kon sayti ishlamay qolsa, xaridlar to‘xtab, kompaniya daromadidan mahrum bo‘ladi va mijozlar ishonchi yo‘qoladi.

4. **Shaxsiy ma’lumotlarni o‘g‘irlash va o‘zgalar nomidan harakat qilish:** Jinoyatchilar ko‘pincha internetdagi turli ochiq manbalardan (ijtimoiy tarmoqlar, sizilgan ma’lumotlar bazalari) shaxsiy ma’lumotlarni to‘plab, o‘zgalar nomidan noqonuniy amallarni bajarishadi. Masalan, boshqaning nomidan kredit olish, bank hisob raqamlarini boshqarish, noqonuniy onlayn faoliyat yuritish yoki boshqa shaxsga tegishli mulkni o‘zgartirishga urinish. Bu jinoyat nafaqat moliyaviy zarar yetkazadi, balki

jabrlanuvchining obro‘siga ham katta putur yetkazib, uning ijtimoiy hayotiga salbiy ta’sir ko‘rsatadi.

Kiberjinoyatchilikka qarshi kurashishning zamonaviy usullari

Kiberjinoyatchilikka qarshi samarali kurashishda kompleks va muvofiqlashtirilgan yondashuv talab etiladi. Bu yondashuv uchta asosiy yo‘nalishni o‘z ichiga oladi: texnologik, huquqiy-tashkiliy va ijtimoiy choralar.

1. Texnologik yechimlar:

Sun’iy intellekt (AI) va mashinani o‘qitish (ML): Kiberxavfsizlik sohasida AI va ML tobora muhim rol o‘ynamoqda. An’anaviy usullar yangi turdagi hujumlarni aniqlashda qiyinchiliklarga duch kelayotgan bir paytda, AI tizimlari ma’lumotlar oqimini doimiy tahlil qilib, g‘ayritabiiy harakatlarni (anomaliyalarni) real vaqt rejimida aniqlay oladi. ML algoritmlari ilgari kuzatilmagan tahdidlarni ham o‘z-o‘zidan o‘rganib, ularga qarshi himoya mexanizmlarini yaratadi. Masalan, AI shubhali elektron pochta xabarlarini fishing ekanligini avtomatik aniqlab, ularni spam papkasiga yo‘naltirishi mumkin. Bu inson omiliga bog‘liq xavflarni kamaytiradi.

Raqamli forenzika: Bu ilmiy uslub kiberjinoyat sodir bo‘lganda, raqamli dalillarni (kompyuter xotirasidagi ma’lumotlar, tarmoq loglari, dastur fayllari) qonuniy va xolis tarzda to‘plash, saqlash va tahlil qilishga qaratilgan. Raqamli forenzika mutaxassislari hujumning manbasini, kim tomonidan amalga oshirilganini va hujum oqibatlarini aniqlashda muhim rol o‘ynaydi. Bu usul kiberjinoyatchilarni topish va ularni javobgarlikka tortish uchun ishonchli dalillar bazasini yaratadi. Raqamli forenzika jinoyatni tergov qilish jarayonining ajralmas qismiga aylandi.

Kuchli kiberhimoya tizimlari: Hozirgi kunda an’anaviy antivirus dasturlari yetarli emas. Zamonaviy kiberhimoya tizimlari ko‘p bosqichli himoyaga ega bo‘lishi kerak. Bunga ma’lumotlarni shifrlash (encryption), ikki faktorli autentifikatsiya (Two-Factor Authentication), xavfsizlik devorlari (firewalls) va tarmoq monitoringi kabi texnologiyalar kiradi. Shifrlash ma’lumotlarni ruxsatsiz foydalanishdan himoyalaydi, hatto ular

o‘g‘irlangan taqdirda ham. Ikki faktorli autentifikatsiya esa akkauntlarga kirish xavfsizligini sezilarli darajada oshiradi. Bulardan tashqari, korxonalar o‘z tizimlarining zaif tomonlarini topish uchun doimiy ravishda penetratsion testlar (tizimga kirishga urinishlar) o‘tkazishlari lozim.

2. Huquqiy va xalqaro hamkorlik:

Qonunchilikni takomillashtirish: Kiberjinoyatlar doimiy o‘zgarib turganligi sababli, milliy qonunchilikni ham yangi tahdidlarni hisobga olgan holda muntazam ravishda yangilab borish zarur. Jinoyatchilarning harakatlarini qonun bilan to‘g‘ri baholash, ular uchun jazo choralarini aniq belgilash va yangi texnologiyalar, masalan, kriptovalyuta orqali sodir etilgan jinoyatlar bilan bog‘liq huquqiy asoslarni yaratish muhimdir. Qonunlarning kechikishi jinoyatchilarga jazosiz qolish imkonini beradi.

Xalqaro hamkorlik: Kiberjinoyatlar chegarani tan olmaydi, jinoyatchi bir mamlakatda, jabrlanuvchi boshqasida bo‘lishi mumkin. Shu sababli, bu muammoga qarshi samarali kurashishda davlatlar o‘rtasida xalqaro hamkorlik juda muhim. Tezkor ma’lumot almashinuvi, kiberjinoyatchilarni birgalikda ta’qib qilish va transmilliy hujumlarga qarshi kurashish bo‘yicha kelishuvlar va konvensiyalar (masalan, Budapesht konvensiyasi) zarur. Interpol kabi xalqaro tashkilotlar bu jarayonda markaziy rol o‘ynaydi.

3. Ijtimoiy choralar:

Raqamli savodxonlikni oshirish: Kiberxavfsizlikdagi eng zaif bo‘g‘in ko‘pincha insonning o‘zi bo‘lib qoladi. Aholining raqamli savodxonligini oshirish kiberjinoyatchilikka qarshi kurashishning eng samarali usullaridan biridir. Maktablarda, oliy ta’limda va ish joylarida kiberxavfsizlik bo‘yicha doimiy ta’lim berish muhim. Odamlar kuchli parollar yaratishni, ikki faktorli autentifikatsiyadan foydalanishni, shubhali elektron xabarlarga ishonmaslikni, va o‘z ma’lumotlarini himoyalashni o‘rganishlari kerak. Jamiyatda bu bilimlar virusga qarshi immunitet kabi ishlaydi.

Mutaxassislarni tayyorlash: Kiberxavfsizlik sohasida yetuk mutaxassislarga bo‘lgan ehtiyoj yuqori. Oliy ta’lim muassasalarida bu yo‘nalishda maxsus dasturlar ochish, mutaxassislarni doimiy malaka oshirishga undash va soha uchun kadrlar bazasini yaratish

muhimdir. Kiberxavfsizlik bo‘yicha olimpiadalar va tanlovlar o‘tkazish ham yoshlarning bu sohadagi qiziqishini oshirishga yordam beradi.

Kompyuter va telefonni jinoyatchilardan himoyalashning oson yo'llari

Kiberjinoyatchilik haqida ko'p eshitamiz, lekin bu bizga taalluqli emas deb o'ylash kerak emas. Aslida, har birimiz internetdan foydalanar ekanmiz, xavf ostida bo'lishimizni unutmaslik kerak. Lekin qo'rqishga hojat yo'q! Oddiy, kundalik hayotda qiladigan ba'zi ishlar bilan o'zimizni osongina himoyalashimiz mumkin.

Onlayn firibgarlardan ehtiyot bo'lish kerak

Shubhali xabarlarga ishonmaslik kerak. Bankdan, pochta bo'limidan yoki boshqa tashkilotlardan kabi kelgan, "mukofot yutdingiz!" yoki "shoshilinch parolingizni yangilang" degan xabarlarga e'tibor bermaslik kerak. Bu firibgarlar usuli.

Havolalarga shoshilmaslik kerak. Xabardagi havolaga bosishdan oldin, sichqonchani uning ustiga olib borib (bosmasdan) va qayerga olib borishini tekshirish kerak. Agar manzil g'alati ko'rinsa, aslo ustiga bosmaslik kerak!

Ma'lumotlaringizni bermaslik kerak. Hech qachon bank karta raqam, parol yoki boshqa maxfiy ma'lumotlarni kimdir so'raganda yozib yuborish kerak emas.

3. Kompyuter va telefoninni toza tutish kerak

Dasturlarni doimiy yangilab turish kerak. Telefonyoki kompyuterdagi dasturlarni va operatsion tizimni yangilashni e'tibordan chetda qoldirmaslik kerak. Yangilashlar dasturlardagi xavfsizlikdagi zaifliklarni tuzatadi.

Antivirus dasturidan foydalanish kerak. Kompyuterga ishonchli antivirus dasturini o'rnatish kerak. U kompyuterni viruslardan himoyalaydi va xavfli saytlarga kirishdan ogohlantiradi.

Faqat rasmiy joylardan dastur yuklab olish kerak. Noma'lum veb-saytlardan dastur o'rnatmaslik kerak. Faqat Google Play, App Store yoki dastur yaratuvchisining rasmiy saytidan foydalanish kerak.

4. Ijtimoiy tarmoqlarda hushyor bo'lish kerak

Maxfiylik sozlamalarini tekshirish kerak. Ijtimoiy tarmoqdagi sahifangizni faqat do'stlaringiz ko'rishi uchun qilib qo'yish kerak.

Shaxsiy ma'lumotlarni e'lon qilmaslik kerak. Uyingiz manzili, telefon raqami yoki tug'ilgan kuningiz kabi ma'lumotlarni hammaga ko'rinadigan qilib qo'ymaslik kerak. Firibgarlar bu ma'lumotlardan foydalanishi mumkin.

Tanimagan odamlarni do'stingiz qatoriga qo'shmaslik kerak. Agar notanish odamdan do'stlik taklifi kelsa, uni qabul qilishdan oldin yaxshilab tekshirish yoki rad etish kerak.

Bu oddiy qoidalarga amal qilinsa, siz kiberjinoyatchilar uchun oson nishon bo'lmay qolasiz. Ehtiyotkor bo'lish va xavfsizlikni o'zingiz ta'minlash kerak!

Xulosa

Kiberjinoyatchilik zamonaviy jamiyat uchun jiddiy tahdid bo‘lib qolmoqda. Uning oldini olish va unga qarshi kurashish uchun faqatgina yangi texnologiyalarga tayanib qolish yetarli emas. Texnologik, huquqiy va ijtimoiy choralar birgalikda, kompleks yondashuv bilan qo‘llanilishi lozim. Faqatgina texnologiyalar emas, balki ularni qo‘llab-quvvatlaydigan kuchli qonunchilik va savodli jamiyat ham bo‘lishi kerak. Kelajakda kiberxavfsizlik bo‘yicha tadqiqotlarni davom ettirish, yangi texnologiyalarni amaliyotga joriy etish va barcha darajadagi ta’lim tizimlarida raqamli savodxonlikni oshirish ustuvor vazifa bo‘lishi shart. Faqat shunday keng qamrovli strategiyalar orqali biz o‘zimizni va raqamli mulkimizni kiberdunyo tahdidlaridan ishonchli himoya qila olamiz.

Foydalanilgan adabiyotlar va manbalar:

1. **Choriyev, A. & Xasanov, I.** (2022). *Kiberxavfsizlik asoslari*. Toshkent: O‘zbekiston Milliy universiteti nashriyoti.
2. **Kiberxavfsizlik markazi.** (2023). *O'zbekistonda kiberjinoyatchilikka qarshi kurashish bo'yicha hisobot*. Toshkent.

3. **Budapesht Konvensiyasi.** (2001). *Kiberjinoyatchilik to'g'risidagi konvensiya*. (https://www.coe.int/en/web/conventions/full-list/ /conventions/rms/0900001680081561)

4. **Shreyer, J. & Jons, M.** (2021). *Kiberxavfsizlikda sun'iy intellektning o'rni*. Nyu-York: Wiley nashriyoti.