KIBERJINOYATCHILIKKA QARSHI KURASHISH MUAMMOLARI

Mo'minova Dilnoza Muhiddin qizi
Buxoro davlat universiteti
Yurisprudensiya kafedrasi o'qituvchisi
e-mail: mominovad99@gmail.com
https://doi.org/10.5281/zenodo.22033744

ANNOTATSIYA

Ushbu maqolada, davlatimizda sodir etilayotgan kiberjinoyatlar, mavjud muammolar va kiberjinoyatlarga qarshi kurashish masalalari, kiberjinoyatlarning turlari, ular aholining qaysi qatlami orasida ko'proq sodir bo'layotganligi, ulardan himoyalanish usullari, kiber jinoyatchilikka qarshi aholining huquqiy ongi va madaniyatini oshirish, fuqarolarga kiber jinoyatchilikning tashqi belgilari va ulardan qanday himoyalanish mumkinligi haqidagi masalalar tahlil qilingan.

Kalit so'zlar: Kiberjinoyat, kiberxavfsizlik, xalqaro hamkorlik, himoyalanish choralari, axborot xavfsizligi, global muammo.

ABSTRACT

This article analyzes cybercrimes occurring in the country, existing challenges, and issues related to combating cybercrime. It examines the types of cybercrimes, the demographic groups most frequently targeted, methods of protection, and ways to raise public legal awareness and culture regarding cybercrime. Additionally, it addresses the need to inform citizens about the indicators of cybercrime and how to protect themselves against it.

Keywords: Cybercrime, cybersecurity, international cooperation, protective measures, information security, global problem.

АННОТАЦИЯ

В статье анализируются киберпреступления, совершаемые в стране, а также существующие вызовы и проблемы, связанные с борьбой с киберпреступностью. Рассматриваются виды киберпреступлений, наиболее уязвимые группы населения, методы защиты, а также способы повышения правовой осведомленности и культуры граждан в данной сфере. Кроме того, освещается необходимость информирования населения о признаках киберпреступлений и мерах защиты от них.

Ключевые слова: киберпреступность, кибербезопасность, международное сотрудничество, защитные меры, информационная безопасность, глобальная проблема.

KIRISH

Davrimizning fan va texnika sohasidagi yutuqlari kundalik ijtimoiy hayotimizga yanada qulay imkoniyatlarni taqdim etmoqda. Biroq ana shu afzalliklar bilan bir qatorda, ayrim salbiy holatlar ham yuzaga kelmoqdaki, bunga ham ko'z yumib bo'lmaydi.

Shulardan biri kiber jinoyatchilikdir. Kiber jinoyatchilik — bu kompyuter, kompyuter tarmog'i yoki tarmoq qurilmasidan suiiste'mol qilishga qaratilgan jinoiy faoliyat hisoblanadi. Ularning aksariyati kiber jinoyatchilar yoki xakerlar tomonidan noqonuniy daromad orttirish maqsadida sodir etiladi.

Mamlakatimizda kiber jinoyatchilikka qarshi kurashish samaradorligini oshirish va kiber muhitdagi jinoyatlarning oldini olishga qaratilgan keng ko'lamli ishlar amalga oshirilmoqda. Shunga qaramay, so'nggi yillarda yurtimizda kiberjinoyatlarning turi 18 tadan

62 taga ko’paygan. Ayniqsa, zararli fayllarni tarqatish, bank kartalari bilan bog’liq firibgarlik holatlari bugungi kunda aholini jiddiy xavotirga solmoqda.

Prezidentimizning 2025-yil 30-apreldagi tegishli qarori bu yo’nalishdagi chora-tadbirlarning mustahkam huquqiy asosini yaratib berdi. Ushbu hujjatda Ichki ishlar vazirligi barcha mas’ul tashkilotlar faoliyatini muvofiqlashtirish bo’yicha vakolatli organ etib belgilanib, ichki ishlar organlari mas’ul bo’linmalari so’roviga asosan shubhali pul o’tkazma amaliyotlariga aloqador bank kartalarini tezkorlik bilan bloklashga oid choralarni ko’rishni nazarda tutgan.

Vazirlik, Bosh prokuratura va Markaziy bank o’rtasida kiberjinoyatlarga qarshi kurashishda tezkorlik bilan ma’lumotlar uzatish va tushgan murojaatlar bo’yicha tez choralarni ko’rish maqsadida elektron ma’lumotlar almashinuv platformasini ishga tushirish kabi tadbirlar belgilangan.

MATERIAL VA METODLAR

Mazkur maqola tahliliy tadqiqot sifatida qonun hujjatlari va ilmiy-nazariy manbalar tahlilini o’z ichiga oladi. Ushbu maqolada sohaga oid ilmiy tushunchalar, nazariyotchi olimlarning qarashlari asosida kiberjinoyat va kiber jinoyatchilik tushunchasi, kiberjinoyatlarning turlari, mazkur jinoyatlarga qarshi kurashish usullari, himoya choralari tahlil qilingan.

Tadqiqot ishini amalga oshirishda tizimli hamda qiyosiy-huquqiy tahlil qilish, shuningdek, analiz, sintez, induksiya, deduksiya, tarixiy-huquqiy va statistik ma’lumotlar tahlili kabi usullardan foydalanilgan. Davlatimizda olib borilayotgan sud-huquq islohotlari va kiber jinoyatchilikka qarshi kurashish sohasidagi qonunchilikni takomillashtirishga oid tahlillar tadqiqot ishining metodologik asosini tashkil qiladi.

TADQIQOT NATIJALARI

Bugun texnologiyalar tobora rivojlanib borgani sari jinoyatchilar ham ulardan foydalanib, noqonuniy xatti-harakatlarni sodir etmoqda. Xususan, odamlar kartochkalaridan pulni o'marish sezilarli darajada oshdi. Tabiiyki, huquqni muhofaza qiluvchi organlar tomonidan bu jinoyatchilar aniqlanib, tegishli jazo choralari ko'rilmoqda va jarblanuvchilarga zarar undirib berilmoqda.

Kiberjinoyatni butunlay yo’q qilish va to’liq internet xavfsizligini ta’minlash imkoni bo’lmasa-da, korxonalar, tizimlar, tarmoqlar va ma’lumotlar xavfsizligini ta’minlashga chuqur mudofaa yondashuvidan foydalangan holda samarali kiberxavfsizlik strategiyasini qo’llab-quvvatlash orqali uning ta’sirini kamaytirishga erishish mumkin. Kiberjinoyat xavfini quyidagi usullar bilan kamaytirish mumkin: biznes va xodimlar uchun aniq siyosat va tartiblarni ishlab chiqish; tizimlar va korporativ ma’lumotlarni himoya qilish bo’yicha amaldagi xavfsizlik choralarini belgilash; ikki faktorli autentifikatsiya ilovalari yoki jismoniy xavfsizlik kalitlaridan foydalanish; xodimlarni kiberxavfsizlik siyosati va tartib qoidalari hamda xavfsizlik buzilgan taqdirda nima qilish kerakligi haqida doimiy ravishda ogohlantirib turish; ransomware hujumi yoki ma’lumotlar buzilgan taqdirda zararni kamaytirish uchun ma’lumotlarni muntazam ravishda zaxiralash.

Kiberjinoyat hujumlariga qarshilik mahalliy qattiq disklar va elektron pochta platformalarini shifrlash, virtual xususiy tarmoq va xavfsiz domen nomlari tizimi serveridan foydalanish orqali ham yaratilishi mumkin.

Bugungi kunda jamiyatda kiberjinoyatlarning bir qancha turlari mavjud. Ularga birma-bir to’xtalib o’tamiz:

Fishing – firibgarlarning soxta elektron pochta xabarlari, veb-saytlar yoki xabarlar orqali foydalanuvchilarning shaxsiy va moliyaviy ma’lumotlarini qo‘lga kiritish usulidir. Fishing hujumlari quyidagi shakllarda amalga oshirilishi mumkin: 1.**Elektron pochta**

fishingi – foydalanuvchilarga soxta elektron pochta xabarlari yuboriladi, unda ular login va parollarini kiritishga undaladi;

2.Vishing (ovozli fishing) – telefon qo‘ng‘iroqlari orqali foydalanuvchilarni aldab, ularning shaxsiy yoki moliyaviy ma’lumotlarini olishga harakat qilinadi;

3.SMS fishing – soxta SMS xabarlar orqali foydalanuvchilar fishing havolalariga bosishiga undaladi;

4.Spear fishing – aniq bir shaxs yoki tashkilotni nishonga olgan fishing hujumi, bunda maxsus tayyorlangan xabarlar va shaxsiylashtirilgan ma’lumotlar ishlatiladi.

Fishing hujumlaridan himoyalanish uchun foydalanuvchilar shubhali xabarlarga ishonmasligi, elektron pochta yoki SMS orqali kelgan havolalarga bosishdan oldin ularning haqiqiyligini tekshirishi lozim. Shuningdek, ikki bosqichli autentifikatsiya va xavfsizlik dasturlaridan foydalanish ham fishingga qarshi samarali choradir.

Zararli dasturlar (Malware) – bu foydalanuvchilarning kompyuter tizimlariga zarar yetkazish, shaxsiy ma’lumotlarini o‘g‘irlash yoki noqonuniy maqsadlarda foydalanish uchun maxsus ishlab chiqilgan dasturlar to‘plamidir. Ular quyidagi turlarga bo‘linadi:

Kompyuter viruslari – o‘zini boshqa fayllarga qo‘shib oladigan va ularni buzadigan dasturlar.

Troyan dasturlari – foydalanuvchi tizimiga foydali dastur ko‘rinishida kirib, zarar yetkazuvchi kodlarni o‘z ichiga olgan zararli dasturlar.

Josuslik dasturlari (Spyware) – foydalanuvchining faoliyatini kuzatish va shaxsiy ma’lumotlarni yashirincha yig‘ish uchun mo‘ljallangan dasturlar.

Keyloggerlar – klaviatura bosishlarini qayd qilib, foydalanuvchi parollari va shaxsiy ma’lumotlarini o‘g‘irlovchi dasturlar.

Zararli dasturlar odatda xabarlari, shubhali havolalar yoki yolg‘on dasturlar orqali tarqaladi. Ulardan himoyalanish uchun ishonchli antivirus dasturlarini o‘rnatish, dasturlarni faqat rasmiy manbalardan yuklab olish va shubhali havolalarga bosmaslik muhimdir.

Kiberjosuslik – bu davlatlar, tashkilotlar yoki xususiy shaxslarning maxfiy ma’lumotlarini noqonuniy ravishda yig‘ish va ulardan foydalanish uchun amalga oshiriladigan kiberjinoyat turidir. Kiberjosuslik ko‘pincha hukumat agentliklari, yirik korporatsiyalar va harbiy sektorga qarshi amalga oshiriladi. Ushbu hujumlar orqali raqobatchilar yoki dushman kuchlar maxfiy ma’lumotlarga ega bo‘lish, strategik rejalarni buzish yoki muhim axborot tizimlariga kirish imkoniyatini qo‘lga kiritishadi. Kiberjosuslikning oqibatlari jiddiy bo‘lib, davlat xavfsizligi, iqtisodiy barqarorlik va tijorat sirlarining buzilishiga olib kelishi mumkin. Ushbu tahdidlardan himoyalanish uchun quyidagi choralarga rioya qilish lozim:

Tizimlar va dasturlarni muntazam yangilab borish – zaifliklar orqali kirishning oldini olish uchun xavfsizlikni doimiy ravishda kuchaytirish.

Ikki bosqichli autentifikatsiya va kuchli parollardan foydalanish – kirish huquqlarini himoya qilish.

Shubhali xabarlar va havolalardan ehtiyot bo‘lish – fishing va spear xurujlarining oldini olish.

Kuchli shifrlash texnologiyalaridan foydalanish – maxfiy ma’lumotlarni himoya qilish uchun shifrlash tizimlarini joriy etish.

Xodimlarni kiberxavfsizlik bo‘yicha o‘qitish – ichki tahdidlardan himoyalanish uchun har bir xodimning axborot xavfsizligi bo‘yicha xabardorligini oshirish.

Kiberjosuslikning oldini olish uchun davlat va xususiy sektor hamkorlikda ish olib borishi lozim. Xalqaro darajada kiberxavfsizlik choralari mustahkamlanmoqda va tashkilotlar o‘z tizimlarini yanada kuchli himoya qilish uchun yangi texnologiyalardan foydalanmoqda.

Kiberjinoyatlar nafaqat oddiy foydalanuvchilarga, balki yirik biznes vakillari va davlat muassasalariga ham jiddiy zarar yetkazadi. Ular iqtisodiy yo'qotishlar, shaxsiy ma'lumotlarning oshkor bo'lishi, odamlarning onlayn xizmatlarga nisbatan ishonchsizligining ortishi, davlatlar o'rtasidagi kiberhujumlar natijasida milliy xavfsizlikka jiddiy tahdid solinishi, kiberjinoyatlar tufayli kompaniyalar katta zarar ko'rib, ishchilarni qisqartirishga majbur bo'lishi, kiber jinoyat qurbonlari depressiya, stress va psixologik muammolarga duch kelish shakllarida namoyon bo'ladi.

Kiberjinoyat qurboni bo'lib qolmaslik uchun bir nechta **himoyalanish choralari** mutaxasislar tomonidan ishlab chiqilgan. Ushbu ehtiyot choralariga quyidagilar kiradi:

1.Kuchli parollar ishlatish. Foydalanuvchilar o'z hisoblarini himoya qilish uchun murakkab va takrorlanmas parollardan foydalanishlari kerak. Shuningdek, parolni muntazam yangilab turish muhim hisoblanadi. Kuchli parol quyidagi xususiyatlarga ega bo'lishi kerak: kamida 12-16 belgidan iborat bo'lishi, katta va kichik harflar, raqamlar hamda maxsus belgilar qo'llanilishi; har bir akkaunt uchun alohida parol ishlatilishi; oldindan taxmin qilib bo'lmaydigan bo'lishi ya'ni foydalanuvchi ismi, tug'ilgan sanasi va oddiy so'zlar kiritilmasligi lozim.

Kuchli parollarni yaratish va saqlash uchun quyidagi usullardan foydalanish tavsiya etiladi: parol menejer dasturlaridan foydalanish; parollarni har 3-6 oyda yangilash va avval ishlatilgan parollardan qayta foydalanmaslik; fishing va boshqa firibgarlik usullari orqali parollarni qo'lga kiritishga urinishlardan ehtiyot bo'lish zarur.

Ikki bosqichli autentifikatsiya. Ikki bosqichli autentifikatsiya foydalanuvchi akkauntiga ruxsatsiz kirishning oldini olish uchun qo'shimcha xavfsizlik darajasini ta'minlaydi. Ushbu tizim foydalanuvchining parolidan tashqari, yana bir qo'shimcha xavfsizlik qatlamini talab qiladi va kirish paytida foydalanuvchining telefoniga yoki elektron pochtasiga maxsus tasdiqlash kodi yuboriladi.

Ikki bosqichli autentifikatsiyaning afzalligi shundaki, agar xaker foydalanuvchining parolini qo'lga kiritsa ham, qo'shimcha autentifikatsiyani talab qiladi va soxta saytlarga parol kiritilganda ham, qo'shimcha tasdiqlash kodisiz akkaunt buzilmaydi.

Antivirus dasturlaridan foydalanish. Antivirus dasturlar va tarmoq xavfsizlik devorlaridan foydalanish zararli dasturlarni oldindan aniqlash va bartaraf etishga yordam beradi. Antivirus dasturi foydalanuvchi qurilmalarini doimiy ravishda kuzatib borib, zararli dasturlarni aniqlaydi va bloklaydi; topilgan zararli fayllarni izolyatsiya qilib, ularning tizimga zarar yetkazishining oldini oladi.

Antivirus dasturlaridan to'g'ri foydalanish kiberjinoyatlardan himoyalanishning eng muhim choralardan biri bo'lib, u zararli dasturlarning oldini olish va ma'lumotlarning xavfsizligini ta'minlashga yordam beradi.

Shubhali havolalardan ehtiyot bo'lish. Elektron pochta xabarlarida va ijtimoiy tarmoqlarda shubhali havolalarga bosishdan saqlanish lozim. Firibgarlar ko'pincha yolg'on xabarlar yoki soxta veb-saytlar orqali foydalanuvchilarning shaxsiy ma'lumotlarini qo'lga kiritishga harakat qilishadi. Quyidagi tavsiyalar shubhali havolalardan ehtiyot bo'lishga yordam beradi: manbani tekshirish – havolani bosishdan oldin uning haqiqiyligini tekshirish; qisqartirilgan havolalarga ehtiyot bo'lish; shubhali elektron pochta va xabarlarni ochmaslik; ijtimoiy tarmoqdagi havolalarga ehtiyotkorlik bilan yondashish lozim.

Kiberjinoyat qurboni bo'lish har qanday foydalanuvchi uchun og'ir holat hisoblanadi. Kiberjinoyat nishoniga aylangan shaxs quyidagi choralarni ko'rishi mumkin:

1. Parollarni darhol o'zgartirish.
2. Bank kartalarini bloklash va moliyaviy muassasaga xabar berish.
3. Qurilmalarda antivirus tekshiruvini o'tkazish.
4. Huquq-tartibot organlariga murojaat qilish.

XULOSA

Xulosa qilib aytganda, kiberjinoyatlar zamonaviy dunyoning eng muhim muammolaridan biri bo'lib, ulardan himoyalanish har bir inson va tashkilot uchun dolzarb vazifadir. Kuchli parollar ishlatish, ikki bosqichli autentifikatsiya, antivirus dasturlaridan foydalanish kabi choralarga rioya qilish orqali xavfsizlikni ta'minlash mumkin. Kiberjinoyatlarga qarshi kurash faqat texnologik himoyaning o'zi bilan cheklanmay, balki foydalanuvchilarning ongli va ehtiyotkor bo'lishini ham talab qiladi.

Texnologik rivojlanish bilan birga, kiberjinoyatlar ham takomillashmoqda, shuning uchun himoya choralarini doimiy ravishda yangilanib borishi lozim.

Kelajakda texnologik taraqqiyot bilan birga kiberjinoyatlar ham yanada rivojlanishi mumkin, shuning uchun har bir inson va tashkilot o'z xavfsizligini ta'minlashga doimiy ravishda e'tibor qaratishi lozim. Kiberjinoyatlar bilan samarali kurashish uchun ham texnologik, ham huquqiy jihatdan harakat qilish zarur bo'lib, har bir foydalanuvchi o'zining axborot xavfsizligiga mas'uliyat bilan yondashishi lozim. Kelajakda texnologik taraqqiyot bilan birga kiberjinoyatlar ham rivojlanishi mumkin, shuning uchun har bir inson va tashkilot o'z xavfsizligini ta'minlashga doimiy ravishda e'tibor qaratishi lozim. Hukumatlar, xususiy sektor va xalqaro hamkorlik kiberjinoyatlarga qarshi kurashishning muhim omillaridir. Har bir foydalanuvchi o'zining axborot xavfsizligiga mas'uliyat bilan yondashishi lozim.

REFERENCES

1. https://tashviqot.uz/index.php/2022/10/04/2506/
2. https://library-tsul.uz/viktimologiya-rustambayev-m-x-niyozova-s-s-2021
3. https://www.jigsawacademy.com/blogs/cyber-security/major-causes-of-cyber-crimes-you-must-be-aware-of/
4. https://earthweb.com/cybercrime-statistics/
5. https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime
6. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
7. https://zamon.uz/detail/ozbekistonda-songgi-3-yilda-kiberjinoyatlar-keskin-oshgan-ozbekiston
8. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
9. Convention on Cybercrime, Article
10. https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/
11. https://base.garant.ru/4089723/9db18ed28bd6c0256461e303941d7e7a/#block 3701
12. https://tass.ru/politika/4782506