ISSN: 2835-3730 Website: econferenceseries.com

KIBR JINOYATCHILIK

Iskandarova Nilufar Tohirovna
Ilmiy rahbar

Tohirova Iroda Murod qizi
SamDChTI Maktabgacha va boshlang‘ich ta’limda ingliz tili yônalishi talabasi

ANNOTATSIYA

Kiber jinoyatchilik internet va texnologiyalar rivojlanishining bir natijasi bo'lib, bu sohada o'zgarishlar katta ko'payib kelmoqda. Shunday qilib, har qanday insonning shaxsiy ma'lumotlarini himoyalash va kiber jinoyatchilikka qarshi qo'llanmalarga amal qilish kerak. Mamlakatlar kiber jinoyatchilikka qarshi qonunlar tuzish va xavfsizlik sohasida ishlovchi tashkilotlar yaratishga qaratilgan, bu esa internetdagi jinoyatni aniqlash va jazo qilish uchun zarur bo'lgan ko'rsatmalarni beradi. Biz hammasi bilan birga ishlaymiz va kiber jinoyatchilikka qarshi kurash uchun kerakli qo'llanmalarni o'rganib, ularni amalga oshirishga intilamiz.Bu orqali sizga yordam beramiz degan umiddamiz.

KALIT SÔZLAR: Kiber jinoyat , virus va Malware, phishing,cyberbullying, DDos hamyonligi, ID vafoti, pornografik jinoyatlar, xakerlik, E-mail va internet .

PRIDE CRIME

ABSTRACT

Cybercrime is a result of the development of the Internet and technology, and changes in this area are increasing. Thus, it is necessary to follow the guidelines to protect the personal information of any person and fight against cyber crime. Countries are aiming to create anti-cybercrime laws and security agencies that provide the guidelines needed to detect and punish cybercrime. We are working with everyone to learn and implement the necessary guidelines to combat cybercrime.

Keywords: Cyber crime, virus and Malware, phishing, cyberbullying, DDos wallet, ID death, pornographic crimes, hacking, E-mail and internet.

Hozirgi kunda bir qancha mamlakatlarda kiber jinoyatchilikka qarshi qonunlar bor. Bu qonunlar internetda jinoyat bilan kurashish uchun yangi asboblar ko'rsatib, internetdagi xavfsizlikni ta'minlash uchun eng yaxshi usullarni aniqlaydi va

foydalanuvchilarning shaxsiy ma'lumotlarini himoya qiladi. Bu qonunlarga muvofiq, kiber jinoyatchilikka qarshi kurash uchun xavfsizlik sohasida ishlovchi tashkilotlar va politsiya tashkil etiladi. Buning tufayli, internetdagi jinoyatchilikni aniqlash va jazo qilish imkoniyati kengayadi.

Kiber jinoyatchilikning tarixi o'zida qadimgi zamonlardan boshlab keladi, lekin shu sohada katta o'zgarishlar 1990-yillarda internet tuzilishi va ularga kirish imkonini berish bilan boshlandi. Internet bilan birga kiber jinoyatchilik ham ko'p yil mobaynida rivojlandi. 2000-yillardan boshlab kiber jinoyatlar, bank kartalari va kredit kartalari ma'lumotlariga to'g'ridan-to'g'ri xakkerlik kiradi. Bu xakkerliklar muvaffaqiyatsiz bo'lishsa, o'n mingdan ko'proq kart ma'lumotlari sotuvchi saytlarda chop etiladi.

2010-yillarda esa kiber jinoyatchilikning ko'p qismini botnet atakalari tashkil etdi. Botnetlar, odatda o'zida bir nechta kompyuterlarni biriktiradi va ularni xakkerlik va ddos atakalariga qo'shadi. Shunday qilib, botnetlar internet xizmatlarini yo'qotish va foydalanuvchilarning ma'lumotlarini olish uchun ishlatiladi.

Bugungi kunda kiber jinoyatchilik yuqori darajada rivojlanmoqda va har qanday insonning internetda shaxsiy ma'lumotlarining himoyalanganligini ta'minlashi kerak. Shu sababli, mamlakatlar kiber jinoyatchilikka qarshi qonunlar tuzish va xavfsizlik sohasida ishlovchi tashkilotlar yaratishga qaratilgan. Bular internetdagi jinoyatni aniqlash va jazo qilish uchun zarur bo'lgan ko'rsatmalarni beradi.

Internet tarmog'ida O'zbekiston Respublikasi IIV kiber jinoyatlarga qarshi kurashish bo'limi nomidan fuqarolarga «turli xil taqiqlangan materiallarni tarqatuvchi elementlar, shu jumladan zo'ravonlik, shafqatsizlik targ'ib etuvchi, pornografiyani o'z ichiga olgan» va h.k.lar bilan kurashish uchun bank kartasiga 240 ming so'm miqdorida pul o'tkazish zarurligini aytishadi.

Hurmatli fuqarolar! Ushbu turdagi xabarlarga tanqidiy munosabatda bo'lishingizni iltimos qilamiz. Ichki ishlar organlari fuqarolardan hech qanday hisob raqamiga pul o'tkazmalarini amalga oshirishni so'rashmaydi! Biz buni rasmiy ravishda e'lon qilamiz.

Agar sizga shunday mazmundagi xabarnoma kelsa, iltimos, yaqin atrofdagi ichki ishlar bo'limiga xabar bering.Bu sizning kiberjinoyatchilikka qarshi kurashga qo'shgan ulkan hissangiz bo'ladi.

Internet jinoyatchiligi - bu internet tarmog'i orqali amalga oshiriladigan jinoyatlar, bu jinoyatlar odatda internetda xarakter qiladi va internet tarmog'ini yordamida amalga oshiriladi. Internet jinoyatlari ko'p turli bo'lishi mumkin, misol uchun:

1. Internetda phishing (o'g'irlash) - shaxslar uchun yolg'onlik hisoblanadi, ularni shaxsiy ma'lumotlari yoki moliyaviy ma'lumotlari olish uchun yolg'onliklar bilan qo'llaniladi.
2. Identifikatsiya vafoti (ID vafoti) - bu jinoyat identifikatsiya ma'lumotlarini olish yoki o'zgartirish orqali shaxsiy ma'lumotlarni olishni maqsad qiladi.
3. Xakerlik - bu jinoyat internet tarmog'iga kirish yoki uni to'xtatish orqali moliyaviy foydalanuvchilarning ma'lumotlarini olishni maqsad qiladi.
4. DDoS hamyonligi - bu jinoyat internet saytlariga hujjatlarni yuborish orqali saytni to'xtatishni maqsad qiladi.
5. Pornografiya va seksual jinoyatlar - bu jinoyatlar internetda sharmandalik huquqini buzish, ziddiyat va boshqa seksual jinoyatlar bilan bog'liqdir.

Internet jinoyatlari kuchli qonunlar bilan qarshi kurashishni talab qiladi va ularga qarshi kurashish uchun xavfsizlik usullari bilan tanishish kerak. Internet tarmog'i orqali amalga oshiriladigan barcha faolliklar asosan kuzatilishi kerak, shuning uchun internetda foydalanuvchilar o'zlarining shaxsiy va moliyaviy ma'lumotlarini himoya qilish uchun juda ehtiyotkor bo'lishlari kerak.

6. Cyberbullying - bu jinoyat internet tarmog'i orqali boshqa odamlarga qarshi ziddiyat va nafsaniy tortishlarni olishni maqsad qiladi.
7. Foydalanuvchi ma'lumotlarini sotish - bu jinoyat shaxsiy ma'lumotlarni yoki moliyaviy ma'lumotlarni sotib olishni maqsad qiladi.
8. Phishing - bu jinoyat internet foydalanuvchilarini xavfsizlik maqsadida ko'p qatlamli yolg'onliklar bilan qo'llash orqali shaxsiy ma'lumotlarni olishni maqsad qiladi.
9. Virus va malware - bu jinoyat internet tarmog'i orqali virus va malware yordamida foydalanuvchilarning ma'lumotlarini olishni yoki xavfsizlikni buzishni maqsad qiladi.
10. Tovushli va video qayta ishlash - bu jinoyat internetda tovushli va video materiallarni o'zgartirish yoki yolg'onliklar bilan tahrirlashni maqsad qiladi.

Internet jinoyatlari foydalanuvchilar uchun katta xavfni tashkil etadi, shuning uchun foydalanuvchilar internetda xavfsizlikni ta'minlash uchun keng ko'lamli xavfsizlik usullaridan foydalanishlari kerak. Shuningdek, internet jinoyatlari bilan kurashish uchun qonunlar va xavfsizlik siyosatlaridan foydalanish kerak.

Foydalanuvchilar internetda xavfsizlikni ta'minlash uchun quyidagi usullardan foydalanishlari tavsiya etiladi:

1. Xavfsiz parol yaratish va uni muhafaza qilish.

2. Xavfsizlik dasturlaridan foydalanish, masalan, antivirys dasturlari va to'g'ridan-to'g'ri foydalanuvchi yoki tarmog'i xavfsizlikni ta'minlash uchun mo'ljallangan dasturlar.
3. Foydalanuvchilarning shaxsiy ma'lumotlarini ko'rsatmaydigan internet saytlaridan foydalanish.
4. E-mail va internet saytlariga kirishda ehtiyojli bo'lish, yolg'onlik xabarlarini ochib ko'rmagan holda.
5. Internetdagi shaxsiy ma'lumotlarni hamisha muhafaza qilish, masalan, foydalanuvchi tomonidan joylashtirilgan ma'lumotlarni va xabarlarini yozib olish.
6. Kirishingiz kerak bo'lgan internet saytlari va tarmog'lar haqida tez-tez yangilanayotgan ma'lumotlardan foydalanish.
7. Internetda xavfsizlikni ta'minlash uchun foydalanuvchilarning axborot texnologiyalari sohasida yetkinlik kazanishlari kerak.
8. Agar foydalanuvchi internetda jinoyat bilan qarshiga chiqqan bo'lsa, shunday qilib qilingan xavfli faoliyat haqida politsiyaga xabar berish kerak.

Internet jinoyatlari bilan kurashish uchun qonunlar va xavfsizlik siyosatlaridan foydalanish kerak. Foydalanuvchilarning internetdagi har qanday jinoyatlarni politsiyaga xabar berishlari va xavfsizlik sohasida ishlovchi tashkilotlar bilan hamkorlik qilishlari muhimdir.

So‘nggi paytlarda ijtimoiy tarmoqlarda saytlarni buzib kirish, virusli dasturlar tarqatish kabi holatlar haqida xabarlar ko‘paydi.Kiberj inoyatlar, ayniqsa, pandemiya vaqtida jiddiy muammolardan biriga aylandi. Jinoyat kodeksining bir qator moddalarida kompyuter texnikasi vositalaridan foydalanib sodir etiladigan jinoyatlar va ularga nisbatan javobgarlik ko‘zda tutilgan.

Jumladan, ushbu kodeksning 278^5-moddasiga ko‘ra, o‘zganing kompyuter uskunasini qasddan ishdan chiqarish, xuddi shuningdek kompyuter tizimini buzish (kompyuter sabotaji): 3 yilgacha muayyan huquqdan mahrum qilib, 66 mln 900 ming so‘mdan 89 mln 200 ming so‘mgacha miqdorda jarima; 2 yilgacha ozodlikni cheklash;2 yilgacha ozodlikdan mahrum qilish bilan jazolanadi. Shuningdek, mazkur harakatlarni guruh bo‘lib, takroran yoki xavfli retsidivist tomonidan sodir etish 3 yilgacha ozodlikdan mahrum qilish bilan jazolashga sabab bo‘lishi mumkin. Unutmang, qonunni bilmaslik javobgarlikdan ozod etmaydi!

FOYDALANILGAN ADABIYOTLAR

1. Akbarov D.Y.Axborot xavfsizligini ta'minlashningkriptografik usullari va ularning qo'llanilishi. – Toshkent, "O'zbekiston markasi" nashriyot, 2009-432 bet
2. Axborot xavfsizligiga oid atamalarning ruscha – o'zbekcha izohli lug'ati. 2-mashr. X.P.Xasanovning umumiy tahriri ostida. Toshkent, 2016 - 733 bet.
3. D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, U.Xolimtayeva. Kriptografiyaning matematik asoslari. O'quv qo'llanma. T: M.Ulug'bek nomidagi OzMU, 2018-144 bet.
4. Rakhimjon, H. (2022). 6 NEW PROGRAMMING LANGUAGES TO LEARN. Academicia Globe: Inderscience Research, 3(04), 126-135.
5. R.H.Ayupov, A.V.Kabulov. Kriptografiya va kriptovalyutalar. T: M.Ulug'bek nomidagi O'zMU, 2008-144 bet.