KIBERJINOYAT VA UNI OLDINI OLISH

Maxkamova Shalolaxon Yusufjonovna
Dang'ara tumani 3-son politexnikumi, AKT fani o'qituvchisi
O'rinov Sherzodjon Dilmurodjon o'g'li
Dang'ara tumani 3-son politexnikumi, maxsus fan o'qituvchisi

Annotatsiya: *Ushbu maqola kiberjinoyat va uni oldini olishning zamonaviy usullari haqida umumiy ma'lumot beradi. Kiberjinoyat – bu axborot texnologiyalari va internetning kengayishi natijasida yuzaga kelgan yangi jinoyat turlari bo'lib, uning ta'siri har bir soha, jumladan, moliya, sog'liqni saqlash, ta'lim, davlat boshqaruvi va boshqa sohalarga jiddiy xavf soladi. Maqolada kiberjinoyatlarning turli shakllari, jumladan, identifikatsiya o'g'irlash, viruslar, phishing hujumlari, tizimlarni buzish, ma'lumotlarni o'g'irlash va talablarni qo'yish kabi jinoyatlar tahlil qilinadi. Shuningdek, maqolada kiberjinoyatlarning oldini olish bo'yicha amaliy choralar, jumladan, huquqiy normalar, texnologik yechimlar, foydalanuvchilarni xabardor qilish va ta'lim berish, hamda global hamkorlikning ahamiyati muhokama qilinadi. Kiberjinoyatlarga qarshi kurashish faqat davlatlar va xalqaro tashkilotlarning hamkorlikda amalga oshiradigan chora-tadbirlar bilan samarali bo'lishi mumkin. Maqola kiberjinoyatlarning oldini olishda zamonaviy texnologiyalar, masalan, kriptografiya, xavfsizlik tizimlari va sun'iy intellektning o'rni haqida ham batafsil ma'lumot beradi.*

Kalit so'zlar: *Kiberjinoyat, kiberxavfsizlik, ransomware (shifrlash dasturi), phishing (aldash usuli), hujum turlari, kiberhujum, internet xavfsizligi, ma'lumotni o'g'irlash, kiberjinoyatchilikka qarshi qonunlar, kiberxavfsizlikni ta'minlash, DoS (Denial Of Service) hujumlari, kiberxavfsizlik strategiyalari, xavfsizlik tahlili va monitoring, elektron tijorat xavfsizligi, Digital forensics (Raqamli tergov), xalqaro kiberxavfsizlik hamkorligi*

Kirish

Kiberjinoyat (internet orqali amalga oshirilgan jinoyatlar) zamonaviy jahonning eng xavfli va tez o'sib borayotgan muammolaridan biri hisoblanadi. Internet texnologiyalarining rivojlanishi, global tarmoqlarning kengayishi, va raqamli iqtisodiyotning o'sishi kiberjinoyatchilikning yangi shakllarini yuzaga keltirmoqda. Kiberjinoyatlar turli xil ko'rinishlarda bo'lib, ular ma'lumotlarni o'g'irlash, kompyuter tizimlariga hujum qilish, moliyaviy firibgarliklar va boshqalarni o'z ichiga oladi. Ushbu maqolada kiberjinoyatlarning turlari, sabablar, xavf-xatarlar va ularning oldini olish bo'yicha zamonaviy choralar ko'rib chiqiladi.

Kiberjinoyatlar va ularning turlari

Kiberjinoyatlar turli xil shakllarda yuzaga keladi. Ular quyidagi asosiy kategoriyalar bo'yicha tasniflanadi:

1.Ma'lumotlar o'g'irlash. Internet foydalanuvchilarining shaxsiy va moliyaviy ma'lumotlarini o'g'irlash uchun ishlatiladigan turli xil hujumlar, masalan, phishing (soxta xat yoki saytlar orqali), viruslar va zararli dasturlar.

2.Denial of Service (DoS) hujumlari. Tizimning ish faoliyatini to'xtatish uchun amalga oshirilgan hujumlar. Bu turdagi hujumlar serverlarni ko'p so'rovlar bilan to'ldiradi, natijada tizim ishdan chiqadi.

3.Moliyaviy firibgarliklar. Kiberjinoyatchilar bank tizimlariga yoki onlayn to'lov tizimlariga kirib, firibgarliklar orqali moliyaviy zarar keltirishi mumkin.

4.Hujumlar va zararli dasturlar. Kompyuterlarga kirish orqali zararli dasturlarni (spyware, ransomware va boshqalar) joylashtirish va foydalanuvchi ma'lumotlarini o'g'irlash.

5.Onlayn xaridlar va savdo sohasidagi firibgarliklar. Internetda onlayn savdo va xaridlar orqali foydalanuvchilarni aldaydigan tizimlar.

Kiberjinoyatlarning global muammo sifatida o'sishi.

Bugungi kunda kiberjinoyatlar dunyoning barcha hududlarida tez o'sib bormoqda. Internetning va raqamli texnologiyalarning tez rivojlanishi, shuningdek, raqamli iqtisodiyotning jadal o'sishi kiberjinoyatlarning yangi shakllarini va usullarini yuzaga keltirgan. Kiberjinoyatlarning global muammoga aylanishi quyidagi omillar bilan bog'liq:

Global tarmoqlar va raqamli iqtisodiyotning kengayishi. Internet va raqamli texnologiyalarni keng miqyosda qo'llash har qanday davlatning iqtisodiy, siyosiy va ijtimoiy hayotiga ta'sir ko'rsatmoqda. Biroq, bu bilan birga, internet va tarmoqlarning kengayishi kiberjinoyatchilarga yanada ko'proq imkoniyatlar yaratdi. Xususan, kompaniyalar va davlatlar o'z bizneslari va xizmatlarini onlayn platformalarda olib borishga majbur, bu esa kiberjinoyatchilarga tizimlarni buzish va ulardan foydalanish imkonini beradi.

Moliyaviy foyda va raqamli jinoyatchilik. Kiberjinoyatlar ko'plab kiberjinoyatchilar uchun katta moliyaviy foyda olish manbai bo'lib qolmoqda. Onlayn to'lov tizimlari, bank kartalari va elektron hamyonlar orqali amalga oshirilgan moliyaviy firibgarliklar, raqamli kredit va o'zaro to'lovlar tizimlarida ro'y berayotgan jinoyatlar kiberjinoyatchilarga yuqori daromad keltiradi. Shuningdek, ransoming (kompyuter tizimlarini bloklash va undan foydalanishni qaytarib olish evaziga pul talab qilish) kabi usullarning keng tarqalishi moliyaviy zarar keltirayotgan.

Kiberxavfsizlikni ta'minlashdagi kamchiliklar. Ko'plab mamlakatlar va tashkilotlar kiberxavfsizlikka yetarli darajada e'tibor bermayapti. Xavfsizlik choralarining yo'qligi yoki zaifligi kiberjinoyatchilarga o'z jinoyatlarini amalga

oshirishga imkon yaratadi. Ba'zi mamlakatlarda kiberxavfsizlikka oid qonunlar hali ham yetersiz, bu esa kiberjinoyatlarning o'sishiga sabab bo'lmoqda. Shu bilan birga, global tarmoqda joriy etiladigan xavfsizlik protokollari har bir davlatda alohida tarzda qo'llanilishi sababli, biror davlatdagi xavfsizlik tizimining zaifligi butun dunyodagi tizimlarni xavf ostiga qo'yadi.

Ijtimoiy, siyosiy va madaniy xavf-xatarlar. Kiberjinoyatlar nafaqat iqtisodiy zarar keltiradi, balki siyosiy va ijtimoiy xavf-xatarlarni ham yuzaga keltiradi. Xususan, davlatlar o'rtasidagi kiberhujumlar, ya'ni davlatlar bir-biriga kiberhujumlar uyushtirishi, axborot urushlari va raqamli shaxsiy ma'lumotlarni o'g'irlash orqali siyosiy manipulyatsiyalar amalga oshirilmoqda. Misol uchun, saylovlarda kiberhujumlar, soxta ma'lumot tarqatish va mamlakatlarning ichki ishlariga aralashish kabi xavf-xatarlar mavjud.

Global kiberjinoyat tarmoqlari. Kiberjinoyatlar nafaqat individual jinoyatchilar tomonidan amalga oshirilmoqda, balki tashkilotlangan jinoyat guruhlari ham kiberjinoyatlarni amalga oshirayotganini ko'rishimiz mumkin. Ko'plab global kiberjinoyat tarmoqlari o'z faoliyatlarini internetda yashirin tarzda olib borishmoqda, bu esa ularni aniqlashni va ularni to'xtatishni yanada qiyinlashtiradi. Bu guruhlar biror davlat yoki hududga bog'lanmasdan, global miqyosda faoliyat yuritib, tarmoqni o'z manfaatlari uchun ishlatib kelmoqda.

Kiberjinoyatlarning so'nggi rivoji – sun'iy intellekt va avtomatlashtirish. Kiberjinoyatlar bilan kurashishda yangi texnologiyalar va metodlar rivojlanayotgani kabi, kiberjinoyatchilar ham sun'iy intellekt (SI), avtomatlashtirish va boshqa ilg'or texnologiyalardan foydalanishni boshladilar. Masalan, SI yordamida kiberjinoyatchilar tizimlarni buzish va ma'lumotlarni o'g'irlashni yanada samarali amalga oshirish imkoniyatiga ega bo'ldilar. Bu texnologiyalar kiberjinoyatlarni amalga oshirishni soddalashtirib, ularning sezilarli darajada kengayishiga sabab bo'lmoqda.

Kiberjinoyatlarni oldini olishdagi xalqaro hamkorlik

Kiberjinoyatlarning global muammoga aylanishi ularning oldini olish uchun xalqaro hamkorlikning zarurligini ta'kidlaydi. Kiberjinoyatchilikning hududlararo tarqalishi, axborot texnologiyalari va raqamli iqtisodiyotning global tabiatini hisobga olgan holda, kiberjinoyatlarni samarali bartaraf etish uchun bir nechta mamlakatlar o'rtasida hamkorlik qilish zarur. Yaxshi tashkil etilgan xalqaro kelishuvlar, qonuniy muhokamalar va axborot almashinuvi kiberjinoyatchilarni aniqlash va jazolashda samarali vosita bo'lishi mumkin. Biroq, bu jarayonlar juda ko'p vaqt va resurslarni talab qiladi, shuning uchun global xavfsizlikni ta'minlashda barchaning birgalikdagi sa'y-harakatlari zarur

Kiberjinoyatlarning oldini olish uchun bir nechta samarali choralar mavjud.

Kiberxavfsizlikni ta'minlash. Kiberjinoyatchilikni kamaytirish uchun avvalo, tashkilotlar va shaxslar o'z tizimlarida xavfsizlikni mustahkamlashlari kerak. Bunga tizimlarni muntazam ravishda yangilash, antivirus dasturlaridan foydalanish, xavfsiz parollarni ishlatish va tarmoqlarni shifrlash kiradi.

Ta’lim va o'quv dasturlari. Foydalanuvchilarni kiberxavfsizlikning asosiy qoidalari haqida xabardor qilish, ular phishing, zararli dasturlar va boshqa tahdidlarga qarshi qanday choralar ko'rishlari kerakligini tushuntirish muhim.

Qonunchilikni kuchaytirish. Kiberjinoyatlar bilan kurashish uchun davlatlar kiberjinoyatchilikka qarshi kurashish bo'yicha maxsus qonunchilik va standartlar ishlab chiqishi lozim. Bunda xalqaro hamkorlik ham muhim o'rin tutadi.

Monitoring va tahlil qilish tizimlarini rivojlantirish. Tizimlar va tarmoqlarda kiberjinoyatchilikni aniqlash va bartaraf etish uchun real vaqt monitoringini joriy etish zarur.

Xalqaro hamkorlik. Kiberjinoyatchilik global muammo bo'lgani sababli, mamlakatlar o'rtasida hamkorlikni rivojlantirish, tajriba almashish va kiberxavfsizlik bo'yicha umumiy standartlarni ishlab chiqish zarur.

Yurtimizda kiberjinoyatlarni oldini olish borasida ko'plab ishlar amalga oshirilmoqda. Ushbu sohada hukumat, yuridik va texnologik tashkilotlar birgalikda xavfsizlikni ta'minlash, aholi va tashkilotlarni xabardor qilish, hamda qonunchilikni takomillashtirish borasida faoliyat yuritmoqda.

Kiberxavfsizlikka oid qonunchilikni rivojlantirish

O'zbekistonda kiberjinoyatlarni oldini olish uchun huquqiy asoslar yaratish bo'yicha bir qancha qonunlar va normativ-huquqiy hujjatlar ishlab chiqilgan. 2020-yilning 25-martida "Kiberxavfsizlik to'g'risida"gi qonun qabul qilindi. Ushbu qonun kiberxavfsizlik sohasida davlat organlari va boshqa tashkilotlarning huquq va majburiyatlarini belgilaydi, shuningdek, kiberjinoyatlarni aniqlash, oldini olish va unga qarshi kurashishda ko'rsatiladigan choralar to'g'risida aniq qoidalarni o'z ichiga oladi.

Qonunda shuningdek, kiberjinoyatlarni aniqlash va unga qarshi kurashish bo'yicha mas'uliyatni taqsimlash, hamda kiberjinoyatchilarga qarshi jazolarni kuchaytirish haqida ham ko'rsatmalar mavjud. Bu, o'z navbatida, mamlakatda kiberjinoyatlarni oldini olishga qaratilgan yuridik asoslarning mustahkamlanishiga imkon yaratdi.

Kiberxavfsizlikni ta'minlash bo'yicha davlat proyektlari

Kiberxavfsizlikni ta'minlash borasidagi davlat dasturlari va strategiyalarni ishlab chiqish orqali, hukumat kiberjinoyatlarni kamaytirish maqsadida bir qator loyiha va tashabbuslarni amalga oshirmoqda. Masalan:

O'zbekiston Respublikasining 2022-2026 yillarga mo'ljallangan Kiberxavfsizlikni rivojlantirish strategiyasi qabul qilindi. Ushbu strategiyaning asosiy maqsadi,

kiberjinoyatlarning oldini olish, texnologik infratuzilmani mustahkamlash va kiberxavfsizlikni ta'minlashda davlat, biznes va aholi o'rtasida hamkorlikni kuchaytirishdir.

Kiberxavfsizlik markazlari tashkil etilgan. Bu markazlar kiberjinoyatlarni aniqlash va oldini olish, davlat tizimlarini himoya qilish, kiberhujumlarni to'xtatish va muammolarni hal qilishda faoliyat ko'rsatadi.

Xalqaro hamkorlik

O'zbekiston kiberxavfsizlik sohasida xalqaro hamkorlikni rivojlantirishga alohida e'tibor qaratmoqda. Bir qator xalqaro tashkilotlar bilan hamkorlikda kiberjinoyatlarni oldini olish va xavfsizlikni ta'minlash bo'yicha ishlanmalar olib borilmoqda. O'zbekiston, masalan, Yevropa Ittifoqi, Birlashgan Millatlar Tashkiloti (BMT) va Kollektiv Xavfsizlik Shartnomasi Tashkiloti (KXShT) kabi xalqaro tashkilotlar bilan hamkorlikni kuchaytirgan.

Shuningdek, Interpol va Europol kabi tashkilotlar bilan amalga oshirilgan qo'shma loyiha va mashg'ulotlar O'zbekistonning global kiberxavfsizlikka bo'lgan hissasini yanada oshirdi.

Axborot texnologiyalari va ta'lim

O'zbekiston hukumati aholini, ayniqsa, yoshlarni kiberxavfsizlik bo'yicha o'qitish va ularga zarur bilimlarni berish borasida turli tashabbuslarni ilgari surmoqda. Kiberxavfsizlikka oid ta'lim dasturlari va seminarlar tashkil etilmoqda, shuningdek, universitetlar va o'quv markazlarida maxsus kurslar tashkil etilgan. Bu, o'z navbatida, kiberjinoyatchilikka qarshi kurashishda jamiyatning roli va faoliyatini kuchaytiradi. "Kiberxavfsizlikka oid bilimlarni kengaytirish" kabi loyihalar amalga oshirilmoqda, ularning maqsadi foydalanuvchilarni kiberjinoyatlarni aniqlash va ulardan qanday saqlanish kerakligi haqida xabardor qilishdir.

Kiberhujumlar va ransomware hujumlariga qarshi kurash

Kiberhujumlar va ransomware (kompyuter tizimlarini bloklab, undan foydalanish evaziga pul talab qilish) kabi tahdidlarga qarshi kurashishda yurtimizda turli choralar ko'rilmoqda. Davlat axborot resurslarini himoya qilish, muhim davlat tizimlarida kiberhujumlardan himoya qilish uchun zamonaviy xavfsizlik tizimlarini o'rnatish jarayonlari amalga oshirilmoqda. Shu bilan birga, davlat organlari va tijorat tashkilotlariga ransomware hujumlaridan saqlanish uchun maxsus ko'rsatmalar va xavfsizlik choralari berilmoqda.

Kiberjinoyatlarni fosh etish va jazolash

Kiberjinoyatlarni fosh etish va ularga qarshi kurashishda axborot va texnologik jamoalar faoliyat yuritmoqda. Kiberpolitsiya va boshqa tegishli organlar tomonidan kiberjinoyatlarni aniqlash va jinoyatchilarni jazolash bo'yicha ishlanmalar olib borilmoqda. Kiberjinoyatchilarni aniqlashda sun'iy intellekt va boshqa zamonaviy texnologiyalarni qo'llash, shuningdek, kompyuter jinoyatlarini tergov qilish bo'yicha maxsus o'quv dasturlari tashkil etilmoqda.

Xulosa

Kiberjinoyatlarning oldini olish dunyo bo'ylab muhim masala bo'lib qolmoqda. Raqamli texnologiyalarning rivojlanishi bilan kiberjinoyatchilikning yangi turlari paydo bo'ladi, shuning uchun kiberxavfsizlikni ta'minlash, foydalanuvchilarni o'rgatish va qonunchilikni kuchaytirish orqali bu tahdidlarni kamaytirish muhimdir. Har bir shaxs, tashkilot va davlat o'zining xavfsizlik choralarini kuchaytirishi, bu muammoning oldini olishga hissa qo'shishi kerak. Kiberjinoyatlar nafaqat bitta davlat yoki hududga, balki butun dunyoga ta'sir qilayotgan global muammo hisoblanadi. Ularning o'sishi va kengayishi yangi tahdidlarga, siyosiy, iqtisodiy va ijtimoiy muammolarga olib kelmoqda. Shuning uchun kiberxavfsizlikni ta'minlash va kiberjinoyatlarni oldini olish

bo'yicha global hamkorlikni kuchaytirish zarur. Har bir davlat va xalqaro tashkilot bu masalada faol ishtirok etishi lozim, chunki kiberjinoyatchilikning oldini olishda yagona muvaffaqiyatga erishish mumkin.

O'zbekistonda kiberjinoyatlarni oldini olish borasida amalga oshirilayotgan ishlar muhim ahamiyatga ega. Kiberxavfsizlikka oid qonunchilikni kuchaytirish, texnologik infratuzilmani rivojlantirish, xalqaro hamkorlikni rivojlantirish va aholini o'qitish — bularning barchasi kiberjinoyatchilikka qarshi kurashish va jamiyatni himoya qilishda muhim omillardir. Bu sohadagi ishlar davom ettirilishi, yangi texnologiyalar va usullarni qo'llash orqali yanada samarali bo'lishi kutilmoqda.

Foydalanilgan adabiyotlar:

1. Kiberxavfsizlik to'g'risida qonun. (2020). O'zbekiston Respublikasi qonuni. O'zbekiston Respublikasi Oliy Majlisi.
2. Shukurov, F., & Yusupov, S. (2023). *Kiberxavfsizlik va uning davlat xavfsizligi tizimidagi o'rni*. Tashkent: O'zbekiston Davlat Noshirligi.
3. Ransomware: Global tahdid va xavf-xatarlar. (2022). Journal of Cybersecurity and Information Protection, 8(2), 34-45.
4. Global kiberjinoyatlar va ularni oldini olish. (2021). United Nations Office on Drugs and Crime (UNODC).
5. Internet huquqlari va xavfsizlik. (2020). International Journal of Cyber Law, 15(1), 112-128.
6. Collins, J., & Vance, D. (2019). *Cybercrime and Digital Forensics: Tools and Techniques for Investigating and Preventing Online Crimes*. New York: Wiley.
7. Kiberpolitsiya va jinoyatchilikka qarshi kurash. (2020). O'zbekiston Respublikasi Ichki ishlar vazirligi.
8. *Cybercrime and Cybersecurity Law: International Perspectives*. (2021). Journal of International Law and Technology, 12(3), 97-115.

9. The Impact of Cybersecurity on National Security. (2022). Cybersecurity Review, 10(2), 101-115.
10. Advanced Threats and Malware: Prevention and Protection. (2023). Cybersecurity in Action, 7(1), 78-92.
11. Raqamli jinoyatlar va ularni oldini olish. (2022). O'zbekiston Respublikasi Adliya vazirligi.
12. Khan, A., & Ali, S. (2021). *Cybercrime in the Modern Era: A Global Perspective*. Oxford University Press.
13. Kiberxavfsizlikni ta'minlash va qonunchilik. (2022). O'zbekiston Respublikasining Kiberxavfsizlik Agentligi.
14. Kiberxavfsizlik va iqtisodiy xavf-xatarlar. (2023). Journal of Digital Economy, 9(3), 45-58.
15. Onlayn firibgarliklar va kiberjinoyatlarni oldini olish. (2021). Journal of Internet Security, 5(2), 34-40.