KIBERJINOYATLARNI KELTIRIB CHIQARUVCHI OMILLAR VA ULARNI OLDINI OLISH USULLARI

https://doi.org/10.5281/zenodo.7883858

Azimjonov Muslimbek Dilmurodjon O`G`Li
O'zbekiston Respublikasi IIV Akademiyasi kursanti

Annotatsiya: *Zamonaviy jamiyat har kuni turli xil o'zgarishlarni boshdan kechirmoqda: odamlar ilgari hech qachon bo'lmagan harakatlar, siyosat va muassasalarni kuzatishi mumkin. Atrof-muhit muammolari, ishsizlikning o'sishi, migratsiya va ijtimoiy beqarorlik - bularning barchasi jamoalar va mamlakatlar rivojlanishiga ta'sir qiladi. Kiberxavfsizlik kiberkmakondan kelayotgan xavflarni tanqidiy baholaydi. Kiberjinoyat sohasi, uning jamiyatga tahdid solayotgan tahdidlari va kelajakda odamlarga ta'sir qilishi mumkin bo'lgan oqibatlari bilan bog'liq.*

Annotation: *Modern society is experiencing various changes every day: people can observe actions, policies and institutions that have never existed before. Environmental problems, rising unemployment, migration and social instability all affect the development of communities and countries. Cybersecurity is a critical assessment of threats from cyberspace. The field of cybercrime is concerned with the threats it poses to society and the consequences it may have on people in the future.*

Аннотация: *Современное общество каждый день переживает различные изменения: люди могут наблюдать действия, политику и институты, которых раньше никогда не было. Экологические проблемы, растущая безработица, миграция и социальная нестабильность — все это влияет на развитие сообществ и стран. Кибербезопасность — это критическая оценка угроз из киберпространства. Область киберпреступности связана с угрозами, которые она представляет для общества, и последствиями, которые она может иметь для людей в будущем.*

Kalit so`zlar: *Kiberjinoyat, kiberxavfsizlik, kibermakon, kompyuter jinoyatchiligi, axborot xavfsizligi, operatsion tizim, kiberjinoyat omillari.*

Key words: *Cyber crime, cyber security, cyber space, computer crime, information security, operating system, cyber crime factors*

Ключевые слова: *Киберпреступность, кибербезопасность, киберпространство, компьютерная преступность, информационная безопасность, операционная система, факторы киберпреступности.*

Internetda sodir bo'layotgan dolzarb jarayonlar muhokama qilinmoqda. 2020-yil juda ko'p kiber hodisalarga ega bo'lib, tahlil va mulohaza yuritish uchun juda ko'p savollar va sabablarni taklif qildi. Vaqt o'tishi bilan ularning soni ortib boradi. Innovatsion texnologiyalar va kibermexanizmlarning kiritilishi bilan internet

jinoyatchilari har qachongidan ham kuchliroq bo'lib bormoqda. Ular doimiy ravishda internet olamiga hujum qilib, maxfiy ma'lumotlarni buzishadi. Ta'kidlanishicha, kiberjinoyatlarning aksariyati moliyaviy va mafkuraviy sabablarga ko'ra xakerlar tomonidan sodir etilgan. Mubolag'asiz aytish mumkinki, ko'pchilikning hayoti kompyuterlarda saqlanadi: qarindoshlar, do'stlar va tanishlar ro'yxati, video va fotosuratlar, odamlar qaerda bo'lganligi, ular nimani yoqtirishi va yoqtirmasligi haqidagi ma'lumotlar va maxfiylik. Jamiyatning axborot-kommunikatsiya texnologiyalariga tobora ko‘proq qaram bo‘lib borayotganini inobatga oladigan bo‘lsak, ushbu texnologiyalarni himoya qilish va ulardan foydalanish imkoniyati milliy manfaatlar uchun muhim nuqta va hayotiy mavzuga aylanib bormoqda. Individual darajada, kiber-hujum shaxsiy ma'lumotlarni o'g'irlashdan tortib pul undirish yoki qimmatbaho ma'lumotlarni, masalan, oilaviy fotosuratlarni yo'qotishgacha bo'lgan turli oqibatlarga olib kelishi mumkin. Jamiyat va tizimlar elektr stantsiyalari, shifoxonalar va moliyaviy xizmatlar kompaniyalari kabi muhim infratuzilmalarga bog'liq. Bu va boshqa tashkilotlarning himoyasi jamiyatimizni saqlab qolish, davlatlar va xalqaro tashkilotlar o‘rtasidagi munosabatlarni qo‘llab-quvvatlash uchun zarurdir.

Ekstremistik va terroristik jamoalarning onlayn muloqot faoliyati soni jadal sur'atlar bilan o'sib bormoqda. Texnologiya odamlarning hayotini yanada qulayroq qiladi, ammo xavf har qanday joydan kelishi mumkin. Kiberjinoyatchilar keyinchalik taqsimlangan xizmatni rad etish (DDoS) hujumlarida foydalanish uchun Narsalar Interneti (IoT) dan bot.netlarni faol ravishda yaratmoqda. Kibertahdid holatlari barcha darajalarda oldindan aytib bo'lmaydigan siyosiy oqibatlarga olib kelishi mumkin. Aksariyat kiberjinoyatlar kiberjinoyatchilarga foyda keltirish maqsadida amalga oshirilgan bo'lsa-da, ba'zi kiberjinoyatlar to'g'ridan-to'g'ri kompyuterlar yoki qurilmalarga zarar etkazish yoki o'chirish uchun amalga oshiriladi. Boshqa zararli dasturlar noqonuniy ma'lumotlar, tasvirlar yoki boshqa materiallarni tarqatish uchun kompyuterlar yoki tarmoqlardan foydalanadilar. Ba'zi kiberjinoyatlar ikkalasini ham, ya'ni kompyuterlarni maqsadli ravishda ularga kompyuter virusi bilan yuqtirishni maqsad qilib qo'yadi, keyinchalik u boshqa mashinalarga, ba'zan esa butun tarmoqlarga tarqaladi. Kiberjinoyatning asosiy ta'siri moliyaviydir. Kiberjinoyatlar foyda keltiruvchi jinoiy faoliyatning ko‘plab turlarini, jumladan, to'lovga qarshi hujumlar, elektron pochta va internetdagi firibgarlik, shaxsiy ma’lumotlarga oid firibgarliklarni, shuningdek, moliyaviy hisob, kredit karta yoki boshqa to‘lov kartasi ma’lumotlarini o‘g‘irlashga urinishlarni o‘z ichiga olishi mumkin. Kiberjinoyatchilar shaxsning shaxsiy ma'lumotlarini yoki korporativ ma'lumotlarini o'g'irlash va qayta sotish uchun nishonga olishlari mumkin. Pandemiya tufayli ko‘plab ishchilar masofaviy ish tartibiga o‘tayotganligi sababli, 2021-yilda kiberjinoyatlar tez-tez o‘sishi kuzatildi, bu esa zahiraviy ma’lumotlarni himoya qilishni ahamiyatini oshirdi. Internetga ulanish zarurati kiberjinoyatchilik faoliyatining hajmi va sur'atini oshirishga imkon berdi, chunki jinoyat sodir etganda jinoyatchi jismonan hozir bo'lishi shart emas. Internet tezligi, qulayligi, anonimligi va chegaralarning yo'qligi kompyuterga asoslangan

moliyaviy jinoyatlarni - to'lov dasturi, firibgarlik va pul yuvish, shuningdek, ta'qib qilish va bezorilik kabi jinoyatlarni amalga oshirishni osonlashtiradi. Kiberjinoyatchilik faoliyati nisbatan kam texnik malakaga ega bo‘lgan shaxslar yoki guruhlar yoki yuqori darajada uyushgan global jinoiy guruhlar tomonidan amalga oshirilishi mumkin, ular orasida malakali ishlab chiquvchilar va tegishli tajribaga ega bo‘lgan boshqalar ham bo‘lishi mumkin. Aniqlash va jinoiy javobgarlikka tortish imkoniyatlarini yanada kamaytirish uchun kiberjinoyatchilar ko'pincha kiberjinoyat qonunlari zaif yoki mavjud bo'lmagan mamlakatlarda faoliyat yuritishni afzal ko'radilar. Internetdan tashqarida sodir etilgan ko'plab jinoyatlarda bo'lgani kabi, pul ko'plab kiber jinoyatchilar uchun asosiy turtki hisoblanadi. Ayniqsa, siz tarmoq orqasida yashiringanингizda jinoyatchilik xavfi unchalik sezilmaganligi sababli past xavf va juda yuqori moliyaviy mukofotni idrok etish ko'plab kiber jinoyatchilarni zararli dasturlar, fishing, shaxsiy ma'lumotlarni o'g'irlash va firibgar pul so'rovi hujumlarida qatnashishga undaydi. Jinoyatchilarni rag'batlantiradigan sabablardan tashqari, kiberjinoyat sodir bo'ladigan muhit ham bu hodisaning keng tarqalganligini tushuntirishga xizmat qiladi. Bitta muvaffaqiyatli kiberhujumning oqibatlari moliyaviy yo'qotishlar, intellektual mulkni o'g'irlash va iste'molchilarning ishonchi va ishonchini yo'qotish kabi keng qamrovli oqibatlarga olib kelishi mumkin. Kiberjinoyatning jamiyat va hukumatga umumiy pul ta'siri yiliga milliardlab dollarni tashkil qiladi.

Shu o’rinda kiberjinoyatlar sodir bo’lishining asosiy omillarini sanab o’tamiz:

Oson kirish tizimi

Tizimni murakkab texnologiyalarni o'z ichiga olgan ma'lumotlar buzilishidan himoya qilish ko'pincha qiyin yoki imkonsizdir. Xavfsizlik faqat xakerlar uchun tizimga kirish oson bo'lgandagina buzilishi mumkin. Malakali xakerlar kirish kodlarini buzish orqali ruxsatsiz kirish huquqiga ega bo'lishlari mumkin. Ular biometrik tizimni osongina aldashlari va tizimning xavfsizlik devori orqali o'tishlari mumkin.\

Kichik maydonda ma'lumotlarni saqlash

Ma'lumki, kompyuter juda katta hajmdagi ma'lumotlarni ixcham joyda saqlaydi va bu kiberhujumlar ortidagi eng katta sabablardan biridir. Aynan kompyuterlar kashf etilgandan keyin kiberjinoyat paydo bo'ldi. Kichkina joyda ma'lumotlarni saqlash xakerlarga qisqa vaqt ichida ma'lumotlarni o'g'irlash va ulardan o'z foydalari uchun foydalanishni osonlashtiradi. Shuning uchun tizimda barcha kerakli ma'lumotlarni saqlamaslik va ularni turli joylarda ajratish tavsiya etilmoqda.

Murakkab kodlashlar

Operatsion tizimlar kompyuterlarni funksional qiladi va bu operatsion tizimlar millionlab kodlar bilan yaratilgan. Operatsion tizimlar insonlar bo'lgan ishlab chiquvchilar tomonidan dasturlashtirilgan va shu bilan kodlarni xatolarga qarshi himoyasiz qildi. Kodlardagi eng kichik halqa operatsion tizim funksiyalarida katta farq qilmasligi mumkin bo'lsa-da, bu bo'shliqlardan kiber-jinoyatchi osonlikcha foydalanishi mumkin. Ular ushbu bo'shliqlardan o'tib, operatsion tizimni

foydalanuvchilar uchun zararli qilishlari mumkin. Murakkab kodlash ko'pincha kiber jinoyatlarning umumiy sababiga aylanishi mumkin.

Beparvolik

Biz e'tiborsiz qoldiradigan va e'tiborsiz qoldirish oson deb hisoblagan har qanday narsa jiddiy tashvishga aylanishi mumkin. Kiberjinoyat xuddi shunday ishlaydi. Tizimingiz xavfsizligini ta'minlashda beparvolik sizga katta muammolarni keltirib chiqarishi mumkin. Sizning oxirida biroz beparvolik kiberjinoyatchilar uchun mehmondo'st yo'lak bo'lishi mumkin. Shuning uchun tizimingizdagi voqealarga hushyor bo'lishingiz kerak.

Dalillarni yo'qotish

Xakerlar odatda tizimingizga bo'limlarga bo'lingan holda hujum qilishadi va ularning birinchi buzilishi haqidagi dalillarni osongina yo'q qilish mumkin. Bu ularning jinoyatlarini yanada kuchliroq qiladi, bu esa kiberjinoyatlarni tergov qilish jarayonida aniqlanmaydi. Dalillarning yo'qolishi kiberjinoyatning muhim sababiga aylanishi mumkin, bu sizning tizimingizni falaj qilishi va uni kiberhujumlarga nisbatan zaifroq qilishi mumkin.

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 ularning ta'sirini kamaytirishi mumkin.

Kiberjinoyat xavfini quyidagi qadamlar bilan kamaytirish mumkin:

1) Biznes va xodimlar uchun aniq siyosat va tartiblarni ishlab chiqish;

2) Ushbu siyosat va tartiblarni qo'llab-quvvatlash uchun kiberxavfsizlik hodisalariga javob rejalarini yaratish;

3) Tizimlar va korporativ ma'lumotlarni himoya qilish bo'yicha amaldagi xavfsizlik choralarini belgilash;

4) Moliyaviy menejer bilan gaplashish orqali pul jo'natish bo'yicha so'rovlarning haqiqiyligini og'zaki tekshirish;

5) Kengaytmalari kompaniya elektron pochtalariga o'xshash elektron pochta xabarlarini belgilovchi tajovuzlarni aniqlash tizimi qoidalarini yaratish;

6) Pul mablag'larini o'tkazish bo'yicha barcha elektron pochta so'rovlarini diqqat bilan ko'rib chiqib, so'rovlar odatiy emasligini aniqlash;

7) Xodimlarni kiberxavfsizlik haqidagi ma’lumotlar va tartib-qoidalari hamda xavfsizlik buzilgan taqdirda nima qilish kerakligi bo‘yicha doimiy ravishda o‘qitish;

8) Qurilmalar va tizimlarni doimiy ravishda yangilab borish;

9) Ma'lumotlar buzilgan taqdirda zararni kamaytirish uchun ma'lumotlar va ma'lumotlarni muntazam ravishda zaxiralash.

Axborot xavfsizligi va kiberjinoyat hujumlariga qarshilik mahalliy qattiq disklar va elektron pochta platformalarini shifrlash, virtual xususiy tarmoq (VPN) va shaxsiy,

xavfsiz domen nomlari tizimi (DNS) serveridan foydalanish orqali ham yaratilishi mumkin.

Xulosa o’rnida shuni aytish joizki, birovning telefoni orqali shaxsning shaxsiy ma’lumotlarini o‘g‘irlashi yoki moliyaviy jinoyat sodir etishi kibermakonda muloqotga o‘tayotgan jamiyat uchun xavf tug‘diradi. Aytish mumkinki, kelajakda kiberhujumlar kattaroq ijtimoiy ta'sir ko'rsatishi mumkin, chunki odamlar Internetga, texnologiyalarga va onlayn xizmatlarga qaramlikni oshirishda davom etmoqda. Jamiyat o'z niyatlariga ega bo'lgan kiberjinoyatchilarning maqsadi bo'lishi mumkin va bu mamlakatlar va shaharlarning rivojlanishiga qanday ta'sir qilishini hech kim bilmaydi. Shunga qaramay, har bir kishi yaqinlashib kelayotgan tahdiddan xabardor bo'lishi kerak.

FOYDALANILGAN ADABIYOTLAR RO’YXATI:

1. Ўзбекистон Республикасининг ЗРУ547сонли “Шахсий маълумотлар тўғри сида»ги Қонуни, 02.07.2019 й.

2. Ўзбекистон Республикасининг 439IIсонли “Ахборот эркинлиги принцип лари ва кафолатлари тўғрисида»ги Қонуни, 12.12.2002 й.;

3. Ўзбекистон Республикаси Президентининг ПҚ-4024сонли “Ахборот технологиялари ва коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштириш чоратадбирлари тўғри сида»ги Қарори, 21.11.2018 й

4. Recommendation № R (89) 9 of the Committee of Ministers of the Council of Europe to member States for the ComputerRelated Crime and Final Report of the European Commitee on Crime Problems. — Strasbourg, 1990

5. БМТ НЖҚКБ. Кибержиноятлар бўйича очиқ ҳукуматлараро экспертлар гуруҳи учун ҳисобот лойиҳаси. “Кибержиноятчилик муаммосини ҳар томонлама тадқиқ қилиш”, — 2013 й., 218бет

6. Лумбунова В.В. Доведение до самоубийства несовершеннолетних с использованием социальных сетей и сети “Интернет”: пути решения проблемы //URL:http://izron.ru/articles/aktualnyeproblemyyurisprudentsii