KIBERMAKONDA AXBOROT XAVFSIZLIGIGA BO‘LADIGAN TAHDIDLAR

Akbarova Muattar Raxmatulayevna
Davlat statistika qo‘mitasi huzuridagi Kadrlar malakasini oshirish va statistik tadqiqotlar instituti, 3-kusr doktoranti

ANNOTATSIYA

Ushbu maqola axborot xavfsizligiga bo‘ladigan tahdidlarga bag‘ishlangan bo‘lib, unda tahdid haqida umumiy tushuncha, axborotni muhofaza qilishning maqsadi, tahdidlarning kelib chiqishi, ularning sababi, axborot tizimidagi zaifliklar ko‘rib chiqilgan. Shuningdek, axborot xavfsizligiga bo‘ladigan tahdidlarning turlari atroflicha o‘rganilgan va O‘zbekistonda 2020 yilda yuz bergan taxdidlar taxlil qilingan.

Kalit so‘zlar: tahdid, axborot tizimi, axborotni muhofaza qilish, axborot havfsizligi, konfedenstial ma’lumotlar.

ABSTRACT

This article focuses on threats to information security, provides an overview of the threat, the purpose of protecting information, the origin of threats, their causes and vulnerabilities in the information system. It also examines the types of information security threats and analyzes the threats that occurred in Uzbekistan in 2020.

Keywords: Threats, information systems, information security, information security, confidential information.

«Axborot erkinligi printsiplari va kafolatlari to‘g‘risida»gi Qonunning qabul qilinishi har kimning axborotni erkin va moneliksiz olish hamda foydalanish huquqlarini amalga oshirishda, shuningdek, axborotning muhofaza qilinishi, shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta’minlashda muhim ahamiyat kasb etdi. Darhaqiqat, 2002 yil 12 dekabrda qabul qilingan bu qonunda axborot xavfsizligini ta’minlash sohasidagi davlat siyosati axborot sohasidagi ijtimoiy munosabatlarni tartibga solishga qaratilgan bo‘ladi hamda shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta’minlash sohasida davlat hokimiyati va boshqaruv organlarining asosiy vazifalari hamda faoliyat yo‘nalishlarini belgilaydi deb belgilangan.

Tahdid deganda kimlarningdir manfaatlariga ziyon yetkazuvchi ro‘y berishi mumkin bo‘lgan voqea, ta’sir, jarayon tushuniladi. Axborotga yoki axborot tizimiga

salbiy ta’sir etuvchi potentsial ro‘y berishi mumkin bo‘lgan voqea yoki jarayon axborot munosabatlari sub’ektlari manfaatlariga qaratilgan tahdid deb yuritiladi.[1]

Shuni aytib o‘tish kerakki, ba’zida tahdidlar tizimdagi xatolik yoki noto‘g‘ri tashkil etilgan faoliyat oqibatida emas, balki tabiiy, ob’ektiv tarzda kelib chiqadilar. Masalan, elektr ta’minoti uzilishi yoki kuchlanishning pasayishi yoki chegaradan oshib ketishi bilan bog‘liq tahdidlar axborot tizimining bevosita apparat qurilmalari ishiga bog‘liqligidan kelib chiqadilar.

Umuman olganda axborotni muhofaza qilishning maqsadini quyidagicha ifodalash mumkin:

– axborotni tarqab ketishi, o‘g‘irlanishi, buzilishi, qalbakilashtirilishini oldini olish;

– shaxs, jamiyat, davlatning xavfsizligiga tahdidni oldini olish;

– axborotni yo‘q qilish, modifikatsiyalash, buzish, nusxa olish, blokirovka qilish kabi noqonuniy harakatlarning oldini olish;

– axborot resurslari va axborot tizimlariga noqonuniy ta’sir qilishning boshqa shakllarini oldini olish, hujjatlashtirilgan axborotga shaxsiy mulk ob’ekti sifatida huquqiy rejimni ta’minlash;

– axborot tizimida mavjud bo‘lgan shaxsiy ma’lumotlarning maxfiyligini va konfidentsialligini saqlash orqali fuqarolarning konstitutsiyaviy huquqlarini himoyalash;

– davlat sirlarini saqlash, qonunchilikka asosan hujjatlashtirilgan axborotlar konfidentsialligini ta’minlash;

– axborot jarayonlarida hamda axborot tizimlari, texnologiyalari va ularni ta’minlash vositalarini loyihalash, ishlab chiqish va qo‘llashda sub’ektlarning huquqlarini ta’minlash.

O‘zbekistonda kiberxavfsizlik sohasidagi munosabatlarni tartibga solish maqsadida 2022 yilda “Kiberxavfsizlik to‘g‘risida”gi qonun qabul qilindi. Qonunning 3- moddasida kiberjinoyatchilik, kibermakon, kibertahdid, kiberxavfsizlik kabi tushunchalarga ta’rib berib o‘tilgan.

Qonunning 4-moddasida esa Kiberxavfsizlikni ta’minlashning asosiy prinsiplari sanab o‘tilgan:

– qonuniylik;

– kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi;

– kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv;

– kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi;

– O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi.[2]

Axborotni muhofaza qilishning samaradorligi uning o‘z vaqtidaligi, faolligi, uzluksizligi va kompleksligi bilan belgilanadi. Himoya tadbirlarini kompleks tarzda o‘tkazish axborotni tarqab ketishi mumkin bo‘lgan xavfli kanallarni yo‘q qilishni ta’minlaydi. Ma’lumki, birgina ochiq qolgan axborotni tarqab ketish kanali butun himoya tizimining samaradorligini keskin kamaytirib yuboradi.

Axborotni muhofaza qilish sohasidagi ishlar holatining tahlili shuni ko‘rsatadiki, muhofaza qilishning to‘liq shakllangan kontseptsiyasi va tuzilishi hosil qilingan, uning asosini quyidagilar tashkil etadi:

– sanoat asosida ishlab chiqilgan, axborotni muhofaza qilishning o‘ta takomillashgan texnik vositalari;

– axborotni muhofaza qilish masalalarini hal etishga ixtisoslashtirilgan tashkilotlarning mavjudligi;

– ushbu muammoga oid yetarlicha aniq ifodalangan qarashlar tizimi;

– etarlicha amaliy tajriba va boshqalar.

Biroq, horijiy matbuot xabarlariga ko‘ra ma’lumotlarga nisbatan amalga oshirilayotogan jinoiy harakatlar kamayib borayotgani yo‘q, aksincha barqaror o‘sish tendentsiyasiga egadir.

Tahdidlarning kelib chiqishi, ularning sababi, axborot tizimidagi zaifliklar haqida tasavvurga ega bo‘lish kam chiqimli axborot xavfsizligini ta’minlovchi vositalar bilan qurollanish imkonini beradi. Axborot texnologiyalari sohasida tahdidlar, xujumlarga oid noxush ma’lumotlar ko‘plab mavjud. Ularning kelib chiqish sabablari va xususiyatlarini bilmaslik tahdidlardan ximoyalanish choralarini ishlab chiqishda ortiqcha xarajatlar sarflanishiga olib kelishi mumkin.

Umuman «tahdid» tushunchasi turli holatlarda turlicha talqin etilishi mumkin. Masalan, ochiq ko‘rinishda faoliyat ko‘rsatuvchi korxona uchun axborotning maxfiyligini oshkor qilishga qaratilgan tahdid muammosi umuman bo‘lmasligi mumkin. Chunki bunday korxonada axborotlarga barcha foydalanuvchilar murojaat qilishlari mumkin. Lekin ba’zi vakolati bo‘lmagan shaxslarning korxona axborotlaridan foydalanishlari jiddiy xavf keltirib chikarishi mumkin. Boshqacha qilib aytganda, tahdid axborot munosabatlari sub’ektlarining manfaatlaridan kelib chiqqan holda vujudga keladi va ular bilan bog‘liq bo‘ladi.

Tahdidlarni quyidagi mezonlar asosida sinflarga ajratish mumkin:

– axborot xavfsizligining asosiy tashkil etuvchilariga nisbatan bo‘ladigan tahdidlar (axborotga murojaat qilish imkoniyatiga qarshi, axborotning yaxlitligini buzishga qaratilgan, axborotning maxfiyligini oshkor qilishga qaratilgan tahdidlar);

– axborot tizimining tashkil etuvchilariga nisbatan bo‘ladigan tahdidlar (berilgan ma’lumotlar, dasturlar, apparat qurilmalari va tizimni qo‘llab-quvvatlovchi infrastruktura);

– tahdidni amalga oshirish usuli bo‘yicha (tabiiy, texnogen, tasodifiy, g‘arazli maqsadda);

– tahdid manbaining axborot tizimiga nisbatan joylashgan o‘rni bo‘yicha (ichki yoki tashqi).[3]

Umumiy yo‘nalishga ko‘ra axborot xavfsizligiga tahdidlar quyidagilarga bo‘linadi:

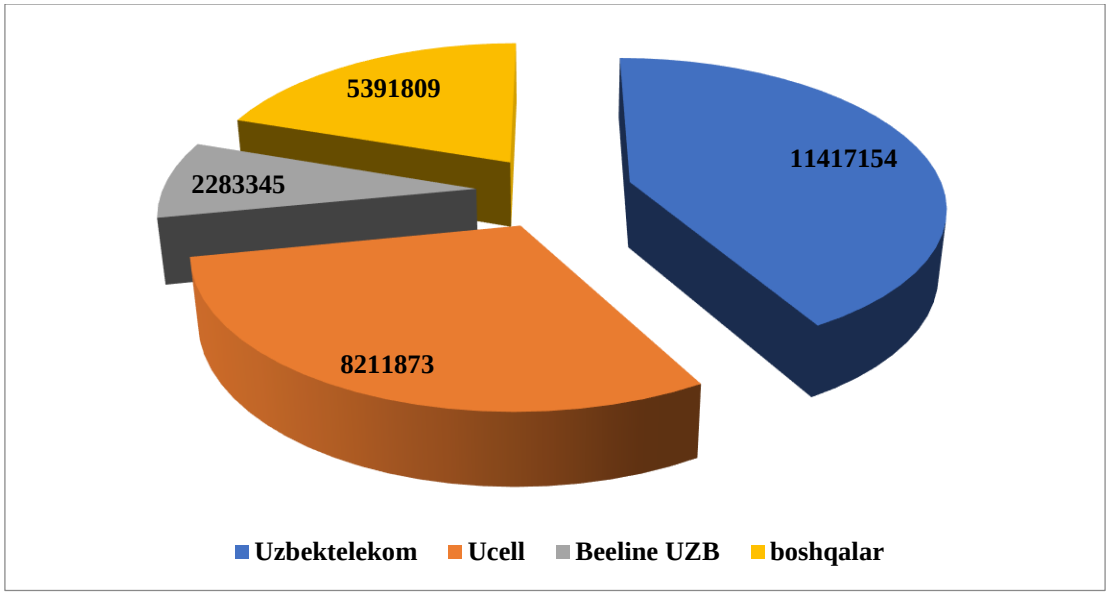
– O‘zbekistonning ma’naviy ravnaqi sohalarida, ma’naviy hayot va axborot faoliyatida fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga tahdidlar;

– mamlakatning axborotlashtirish, telekommunikatsiya va aloqa vositalari industriyasini rivojlanishiga, ichki bozor talablarini qondirishga, uning mahsulotlarini jahon bozoriga chiqishiga, shuningdek mahalliy axborot resurslarini yig‘ish, saqlash va samarali foydalanishni ta’minlashga nisbatan tahdidlar;

– Respublika hududida joriy etilgan hamda yaratilayotgan axborot va telekommunikatsiya tizimlarining me’yorida ishlashiga, axborot resurslari xavfsizligiga tahdidlar.

Ilmiy va amaliy tekshirishlar natijalarini umumlashtirish natijasida axborotlarga nisbatan xavf xatarlarni quyidagicha tasniflash mumkin.

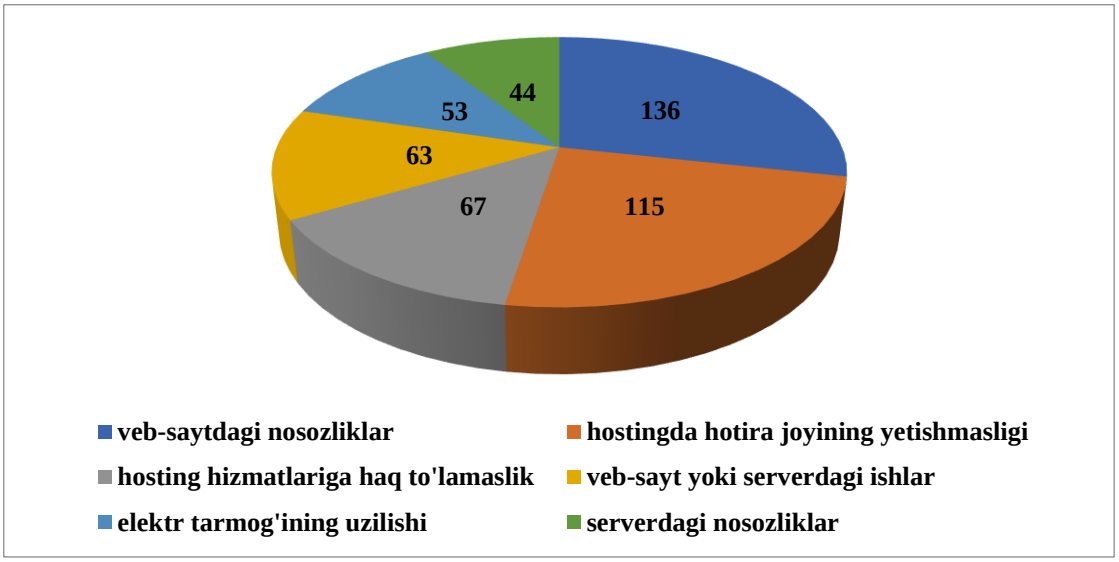
2020 yil monitoring natijalariga ko‘ra, milliy internet segmentida 27 000 000 dan ortiq zararli va shubhali tarmoq hodisalari kuzatilgan. Bu tahdidlarning asosiy qismi Uzbektelecom, Beeline va Ucell kompaniyalari tarmoqlariga to‘gri keladi(1-rasm).[4]



1-rasm. Taxdidlarning soni aloqa operatorlari kesimida

Manba: csec.uz

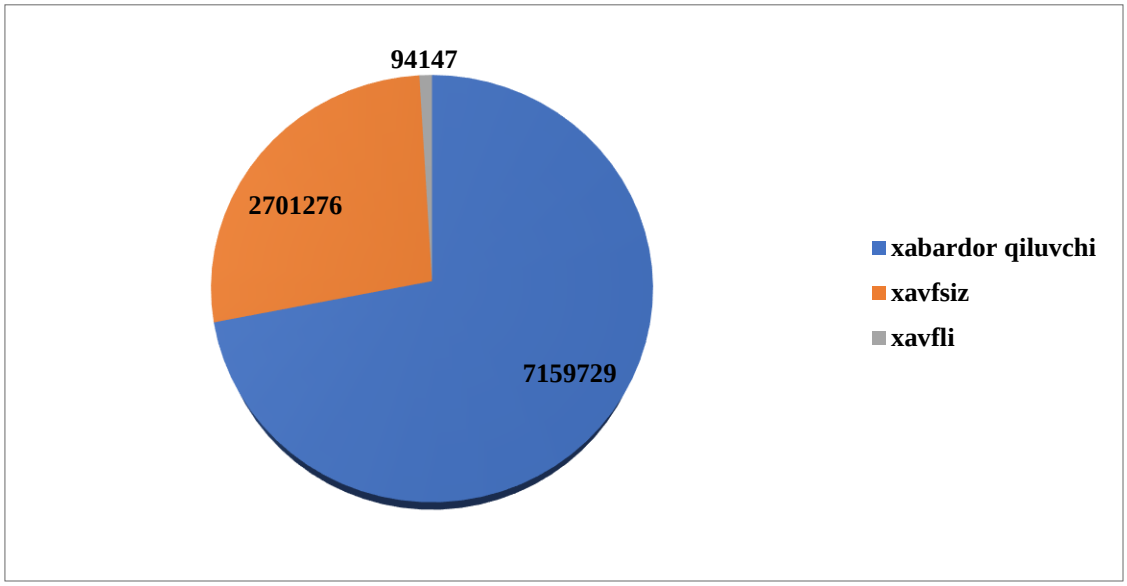
O‘tgan 2020 yil davomida axborot tizimlari va veb-saytlarning xafvsizligini ta’minlash doirasida 680 ta hodisa ro‘y bergan. Oqibatda 1 000 000 daqiqa mobaynida veb saytlarning ishdan chiqish holati kuzatilgan(2-rasm).



2-rasm. Axborot tizimlari va veb-saytlar

Manba: csec.uz

Shu bilan birgalikda idoralararo ma’lumotlar uzatish tarmog‘iga ulangan axborot tizimlarida 9 955 152 ta hodisa qayd qilingan bo‘lib, shundan 94 147 tasi maxfiy ma’lumotlar bazasining buzilishi va konfedenstial ma’lumotlarning tarqalishiga olib keluvchi xavfli xodisa ekanligi aniqlandi(3-rasm).



3-rasm. Idoralararo ma’lumotlar uzatish tarmog‘iga ulangan tizimlarda aniqlangan hodisalar

Manba: csec.uz

2020 yilda milliy .UZ domenida 342 ta hodisa ro‘y bergan bo‘lib, ularning 306 tasi veb-saytlarga ruxsatsiz kirish va 36 tasi veb-saytning asosiy sahifasini noqonuniy o‘zgartirib(deface) qo‘yilishi bilan izoxlanadi.[4]

Shuni alohida ta’kidlash joizki, davlat sektori(81 ta hodisa) hususiy sektorga (261 ta hodisa) nisbatan 3 barobar kamroq hujumga duch kelgan.

Nufuzli xalqaro kompaniyalarning geosiyosiy xatarlar sohasidagi so‘nggi tadqiqotlariga ko‘ra, 2021 yilda dunyoda axborot-kommunikatsiya texnologiyalaridan foydalangan holda amalga oshiriladigan jinoyatlarning o‘sish dinamikasi kuzatilmoqda.

Xalqaro ekspertlarning xulosalari Kovid-19 pandemiyasi oqibatlari bilan bog‘liq karantin cheklovlari davrida dunyodagi vaziyatni chuqur tahlil qilish asosida qilingan. Shu bilan birga, mutaxassislarning fikriga ko‘ra, 2020 yilda kibermakonda jinoyatlar sodir etilishining asosiy omillari quyidagilardir:

– kompaniyalar (tashkilotlar) xodimlarining masofadan ishlashiga o‘tish;
– onlayn ta’lim;
– Internet-do‘konlarda xavfsiz bo‘lmagan xaridlarni amalga oshirish;
– IOT qurilmalaridan (kameralar, qurilmalar, sensorlar va boshqalar) keng foydalanish;
– tovlamachi-viruslarining tarqalishi.[5]

Shuni ta’kidlash kerakki, o‘tgan 2020 yilda bo‘lgani kabi, 2021 yilda ham Internetga qo‘shilgan yangi so‘nggi qurilmalar sonining tez sur’atlarda o‘sishi kuzatiladi.

Bundan tashqari, onlayn-do‘konlarda va onlayn savdo maydonchalarida xaridlarga bo‘lgan talabning ortishi Internetdagi firibgarlar uchun qo‘shimcha "tramplin" ni yaratadi, natijada fuqarolarning bank kartalaridagi mablag‘larni o‘g‘irlash ko‘payadi. Davlat va xususiy kompaniyalar duch kelishi mumkin bo‘lgan yana bir katta tahdid - bu tovlamachi-viruslar (ransomware) deb ataladigan viruslar bo‘lib, ularning tarqalishi asosan fishing pochta xabarlarini yuborish yoki tizimdagi zaifliklardan foydalanish orqali amalga oshiriladi.

Yuqorida aytib o‘tilganlarni hisobga olgan holda bizning mamlakatimizda duch kelishi mumkin bo‘lgan asosiy taxdidlar sifatida quyidagilarni ko‘rsatish mumkin: kiberhujumlarga qarshi IOT qurilmalari, tashkilotlarning axborot tizimlariga va ta’lim tizimiga buzg‘unchilik maqsadlarida ruxsatsiz kirish va Internetdagi firibgarlik.

Davlat va xususiy kompaniyalar (tashkilotlar) rahbarlari korporativ tarmoqning ichki va tashqi perimetrini axborot tizimlariga noqonuniy kirib borish va zararli dasturlarning tarqalishidan himoya qilishni kuchaytirish bo‘yicha samarali tashkiliy va dasturiy-texnik choralarni ko‘rishlari kerak. Yiliga kamida bir marta ushbu sohadagi

ekspert tashkilotlarini jalb qilgan holda axborot va kiberxavfsizlik auditi, shuningdek axborot tizimlari va resurslarini ekspertizadan o‘tkazish tavsiya qilinadi.

Fuqarolarga shubhali URL-manzillarga o‘tmaslik va ularda plastik kartalarni ro‘yxatdan o‘tkazmaslik, shuningdek begona shaxslarga plastik karta ma’lumotlarini (pin kod, karta raqami va amal qilish muddati, SMS orqali yuborilgan tasdiqlash kodini) bermaslik so‘rladi.

Axborot xavfsizligiga tahdidlarni bartaraf etish maqsadida veb-saytlarni himoya qilish uchun quyidagi tashkiliy va texnik choralarni ko‘rish tavsiya etiladi:

– Yangilanishlarni (update) muntazam ravishda o‘rnatib borish
– Zaxira nusxasi (backup)
– Foydalanilmayotgan plaginlarni o‘chirib tashlash
– Parol autentifikatsiyasini mustahkamlash
– Xavfsiz boshqaruvni olib borish
– Xavfsizlik plaginlaridan foydalanish
– Veb-saytni tekshiruvdan o‘tkazib turish

Korporativ tarmoqlarni himoyalash uchun quyidagi tavsiyalarga amal qilish maqsadga muvofiq:

– Axborot xavfsizligiga ichki tahdidlarning oldini olish uchun zarur dasturiy ta’minot va shuningdek, axborotni himoya qilish vositalarini o‘rnatish.

– Axborot-kommunikatsiya texnologiyalari va to‘g‘ridan-to‘g‘ri axborot tizimlari bilan ishlaydigan foydalanuvchilarning (xodimlarning) axborot xavfsizligini ta’minlash va ularning malakasini doimiy oshirib borish.

– Ma’lumotlarni idoralararo uzatish uchun global Internet orqali boshqa axborot tizimlari bilan o‘zaro aloqada bo‘ladigan axborot tizimlaridan foydalanmaslik.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI: (REFERENCES)

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonuni. Toshkent-2022y.
2. С.Гулямов, О.Кутлиев, М.Акбарова “Статистика органларида ахборот хавфсизлигини таъминлаш” Тошкент- 2017й.
3. М.Каримов ва бошқалар. Ахборот хавфсизлиги асослари. Маърузалар матни. Тошкент-2013й.
4. Ўзбекистон Республикаси киберхавфсизлиги. 2020 йил ҳисоботи. Тошкент - 2021 й.
Прогноз основных рисков кибербезопасности на 2021 год.
Манба:https://uzcert.uz/usefulinfo/prognoz-osnovnykh-riskov-kiberbezopasnosti-na-2021-god/