INTERNETDAGI KIBERXAVFSIZLIK TAHDIDLARI VA ULARNING YECHIMLARI

Mo’minov Hayotbek Zavqiy o’g’li
Ichki Ishlar vazirligi Akademiyasi kursanti

Аннотация: *В данной статье рассматриваются типы угроз в кибербезопасности, приведены короткие анализы часто выявляемых киберугроз в киберпространстве. Представлены статистические данные о кибератаках в Республике Узбекистан за прошедший год и сопоставительные данные между Узбекистаном и ведущими государствами мира по киберугрозам.*

Ключевые слова: *Угрозы, кибербезопасность, киберугроза, интернет, цифровая жизнь, киберпреступность, киберпространство, мошенничество.*

Annotation: *This article discusses the current types of cybersecurity threats, provides short analyses of frequently identified cyber threats in cyberspace. Statistical data on cyber attacks in the Republic of Uzbekistan over the past year and comparative data between Uzbekistan and the world's leading states on cyber threats are presented.*

Key words: *Threats, cybersecurity, cyber threat, Internet, digital life, cybercrime, cyberspace, fraud.*

Annotatsiya: *Maqolada kiberxavfsizlik nima ekanligi, hozirda kiberxavfsizlikka bo’layotgan tahdidlar va tahdidlarning turlari haqida so’z yuritilgan. Ushbu maqolada internetdagi turli kibertahdidlar tahlil qilingan va aniqlangan, shuningdek, internet foydalanuvchilariga ehtiyot bo'lishlari uchun mumkin bo'lgan yechimlar taklif qilingan. Kibermakonda O’zbekiston Respublikasiga bir yil davomida bo’lgan kiberhujumlar haqida statistik ma’lumotlar, O’zbekistonning milliy kiberxavfsizlik darajasi va kiberxavfsizlik bo’yicha O’zbekiston va dunyoning yetakchi davlati o’rtasidagi farq berilgan.*

Kalit so‘zlar: *Tahdidlar, kiberxavfsizlik, internet, raqamli hayot, kiberjinoyat, kibermakon, kiberjosuslar, kibertahdidlar, kiberxavfsizlik darajasi.*

Kompyuter texnologiyalarining paydo bo'lishi insoniyatga katta ta'sir ko'rsatdi. Kompyuter texnologiyalarining ajralmas qismi bo'lgan axborot texnologiyalari katta ma'lumotlar bilan ishlashda ishlarni oson bajarishga katta hissa qo'shdi. Hisoblash texnologiyasining samaradorligiga qaramay, kompyuterlar, mobil telefonlar va internetdagi eng ishonchli saqlanadigan fayllar xakerlar hujumlariga va kibermakonga ruxsatsiz kirishning barcha shakllariga moyil bo'lib, bu samarali kiberxavfsizlik tizimlariga ehtiyoj tug'diradi. Aloqa texnologiyalarini qo'llashning eng keng tarqalgan namunasi bu Internetdir. Internet paydo bo'lganidan beri undan foydalanadiganlarning eng katta umidlari va qo'rquvlarini aks ettiradigan darajada kuchli kuchga aylandi. Internet bizning yashash, ishlash, o'qish va biznes yuritish uslubimizni o'zgartirdi. Bu dunyoni global aloqaning inklyuziv qishlog'iga aylantirdi. Biz tez va arzon narxlarda norasmiy suhbatlar, xabarlar almashishimiz yoki sayyoramizning narigi tomonidagi odamlar bilan haqiqiy biznes yuritishimiz mumkin. Shaxsiy kompyuterlarning keng tarqalishi, mobil texnologiyalar, internetga oson kirish va tegishli yangi aloqa qurilmalari bozorining gullab-yashnashi bizning bo'sh vaqtimizni o'tkazish va biznes

yuritish uslubimizni o'zgartirdi. Ushbu texnologik taraqqiyot jinoyatchilarning jinoyat sodir etish usullarini ham o'zgartirdi. Umumjahon raqamli hayot endi jinoyatchilar uchun yangi imkoniyatlar ochadi. Kompyuterlar, tegishli texnologiyalar va tarmoqlar endi kiberjinoyatchilarni ta'qib qilish va ularning fuqarolarga nisbatan turli kibertahdidlarini oldini olish uchun foydalanilmoqda.

Kiberxavfsizlik kibermakonni kibertahdidlardan himoya qilish bilan bog'liq. “Kibertahdidlar” tushunchasi juda noaniq bo‘lib, g’arazli niyatli shaxslarning keng doirasi tomonidan axborot-kommunikatsiya texnologiyalaridan (AKT) jinoiy maqsadlarda noqonuniy foydalanishini nazarda tutadi. Odatda ishlatiladigan "kiberxavfsizlik" atamasi uchta narsani anglatadi:

1.Kompyuterlarni, kompyuter tarmoqlarini, tegishli apparat va dasturiy ta'minotni, shu jumladan ma'lumotlar va ma'lumotlar bazalarini, shuningdek kibermakonning boshqa elementlarini barcha tahdidlardan, shu jumladan milliy xavfsizlikka tahdidlardan himoya qilishga qaratilgan texnik va texnik bo'lmagan tadbirlar va boshqa chora-tadbirlar majmui ;

2.Ushbu faoliyat va choralarni qo'llash natijasida yuzaga keladigan himoya darajasi;

3.Ushbu faoliyatni amalga oshirish va ularning sifatini oshirishga qaratilgan tadqiqot va tahlillarni o'z ichiga olgan kasbiy faoliyatning tegishli sohasi [1].

Kiberxavfsizlik, shuningdek, turli xil kiberhujumlar bilan bog'liq muammolarni tushunish va har qanday raqamli ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini saqlaydigan mudofaa strategiyalari(ya'ni, qarshi choralar)ni ishlab chiqish bilan bog'liq [2]. Ko'pgina kiberxavfsizlik bo'yicha mutaxassislar zararli dasturlar kibermakondagi kiberxavfsizlikni buzish bo'yicha zararli niyatlarni amalga oshirishning asosiy quroli ekanligiga ishonishadi. Zararli dastur deganda, odatda qonuniy egasining xabarisiz, dushman foydasiga tizimni buzish uchun tizimga yuklangan dastur tushuniladi. Zararli dasturlarning quyidagi turlari mavjud: viruslar, qurtlar(Worms), troyan otlari(Trojan), josuslik dasturlari va botlarning bajariladigan dasturlari kiradi.

Xavfsizlikka tahdidi, hujumlar va zaiflik. Internetdagi xavfsizlikka tahdidlarini bartaraf etish uchun avvalo internetni tashkil etuvchi tizim komponentlarini aniqlash kerak. Tizim komponentlarini, shu jumladan barcha komponentlar, qurilmalar va xizmatlarni tushunish muhimdir. Har qanday tizimning asosiy aktivlari - tizim apparati, dasturiy ta'minoti, xizmatlar va xizmatlar tomonidan taqdim etilgan ma'lumotlardir [3].

Zaiflik - bu tizimning o'zida mavjud bo'lgan nuqson yoki zaiflikni bildiruvchi kiberxavfsizlik atamasi bo'lib, axborotning kibertahdid yoki kiberhujumlarga duchor bo'lishiga imkon beradi. Zaiflikning ikki turi mavjud: apparat zaifligi va dasturiy ta'minot zaifligi. Apparat zaifliklarini aniqlash va tuzatish juda qiyin, hattoki zaiflik apparat mosligi va o'zaro muvofiqligi tufayli aniqlangan bo'lsa ham, dasturiy ta'minotdagi zaifliklarni esa operatsion tizimlar, amaliy dasturlar, aloqa protokollari va qurilmalar drayverlari kabi boshqaruv dasturlarida topish mumkin.

Tahdid - bu ma'lumotlarni buzish yoki o'g'irlash yoki tashkilot tizimini yoki butun tashkilotni buzishga qaratilgan zararli harakat. Tahdidlar ikkita asosiy manbadan kelib chiqishi mumkin: inson va tabiat.

Inson tahdidlari - bu tizimga zarar etkazish va buzishni maqsad qilgan ichki yoki tashqi tahdidlardan tashkil topgan zararli tahdidlar kabi odamlar tomonidan yuzaga keladigan tahdidlar.

Tabiiy tahdidlar - zilzilalar, bo'ronlar, suv toshqini va yong'in kabi tabiiy ofatlar kompyuter tizimlariga jiddiy zarar yetkazishi mumkin va hech kim ularni oldini olomaydi. [4] Kiberxavfsizlik tahdidi tushunchasini ma’lumotlarga zarar yetkazishga yoki o‘g‘irlashga va umuman raqamli hayotni buzishga qaratilgan zararli harakat sifatida tushunish mumkin[5]. Kiberga asoslangan texnologiyalar hozir butun dunyoda keng tarqalgan. Jinoyatchilar, terrorchilar va josuslar ham o'z maqsadlarini amalga oshirish uchun axborot xavfsizligini buzishga qaratilgan maxsus tayyorlangan texnologiyalarga tayanadi. Ushbu jinoyatchilar xizmatni rad etish(DOS), ma'lumotlarni o'g'irlash yoki manipulyatsiya qilish yoki o'ziga yoki boshqa uskunaga hujum qilish uchun axborot xavfsizligini buzishga qaratilgan maxsus tayyorlangan texnologiyalarga tayanishi mumkin. Dunyoda keng tarqalgan kiberjinoyatlarga quyidagilar kiradi: kiberterrorchilar, kiberjosuslar, kibero'g'rilar, kiberjangchilar va kiberhaktivistlar.

Kiberjosuslar: Kiberjosuslar xususiy yoki davlat korporatsiyalari tomonidan raqobatbardosh strategik, xavfsizlik, moliyaviy yoki siyosiy ustunlikka erishish uchun foydalaniladigan maxfiy yoki mulkiy ma’lumotlarni o‘g‘irlaydigan shaxslardir.

Kiberterrorchilar: Kiberterrorchilar - bu kompyuter texnologiyalari va internetdan, ayniqsa qo'rquv va buzilishlarni keltirib chiqarish uchun foydalanadigan jinoyatchilar. Isyonchilar, jihodchilar va transmilliy terroristik tashkilotlar internetdan hujumlarni rejalashtirish, radikallashtirish va yollash, tashviqot tarqatish usuli va aloqa vositasi sifatida foydalanganlar.

Kibero'g'rilar: Kibero'g'rilar - pul daromadlari olish uchun kompyuterdan foydalangan holda boshqalardan kredit karta raqamlarini o'g'irlash, ishlatish yoki sotish uchun texnologik tizimga noqonuniy ravishda kirgan tashkilot yoki jismoniy shaxs va jabrlanuvchini moliyaviy hisob qaydnomasiga kirish uchun aldagan shaxs.

Kiberjangchilar: Kiberjangchilar - strategik yoki harbiy maqsadlarda, axborot tizimlariga kirish va sabotaj qilish yoki axborot tizimlarini tashqi hujumlardan himoya qilish bilan shug'ullanadigan kompyuter mutaxassislari.

Kiberxaktivistlar: Kiberhaktivistlar siyosiy xabarlarni, shu jumladan tashqi siyosat yoki tashviqot bilan bog'liq xabarlarni yetkazish uchun veb-saytlar yoki xavfsiz aloqa tizimlarini buzadigan shaxslardir. Masalan, texnologik tizimga shaxsiy muammo sifatida hujum qiladigan kishi (uni “klassik” xaker deb atash mumkin) va siyosiy sabablarga ko‘ra hujum qilgan anonim kiber-guruh a’zosi kabilar kiradi.

Kiberxavfsizlikka top 7 ta tahdid va ularning yechimlarini ko’rib chiqsak. "Kiberxavfsizlik tahdidlari" atamasi ko'p odamlar uchun juda ko'p turli xil narsalarni anglatishi mumkin. Ba'zilar uchun kiberxavfsizlikka tahdidlar zararli dasturlar kabi virtual hujum vektorlari orqali kelganlar bilan chegaralanadi, ammo kibertahdidlar doimiy ravishda o'zgarib turadi. Quyida kiberxavfsizlikka tahdid soluvchi internetda ko’p uchraydigan 7 ta tahdid keltirib o’tilgan:

1. Inson omili. Insayderlar (kompaniyangizda ishlaydigan odamlar) kiberxavfsizlik uchun eng katta tahdid ekanligi tasdiqlangan. Ushbu zaifliklar xodimlar, sotuvchilar yoki sizning tarmog'ingizga yoki IT bilan bog'liq tizimlarga kirish huquqiga ega bo'lgan boshqa har

qanday kishidan kelib chiqadi. Bundan tashqari, kiberhujum yoki ma'lumotlarning buzilishi shunchaki inson xatosi yoki kiberxavfsizlikdan yetarli darajada xabardor bo’lmaslik, masalan, ko’p ishlatilatiladigan taxmin qilish oson bo’lgan parollardan foydalanish yoki fishing xabarlar elektron pochtangizga tushib qolishi tufayli sodir bo'lishi mumkin. Misol uchun, xakerlar tez-tez o'z qurbonlarini kerakli ma'lumotlarni taqdim etishlari yoki zararli kontent bilan shug'ullanishlariga majbur qilish uchun "kodsiz buzish" kabi ijtimoiy muhandislik taktikalaridan foydalanadilar. Shunday qilib, ular zararli dasturlarni o'rnatishlari, ma'lumotlarni yuklab olishlari yoki potentsial xavf tug'diradigan boshqa zararli harakatlarni bajarishlari mumkin.

Tavsiya etilgan yechim(lar): Kuchli xavfsizlik devorlari va antivirusdan foydalanishning o’zigina yechim bo’lib xizmat qilolmaydi. O’z faoliyatida onlayn xizmatlardan foydalanishni taklif qilgan kompaniyalar o'zlarining umumiy kiberxavfsizliklari uchun ichki yoki uchinchi tomon kiberxavfsizlik operatsiyalari markazi (CSOC) xizmatlaridan foydalanishlari kerak.

2. Zararli dasturlarning turli shakllari. Zararli dastur - bu kompyuter, server va kompyuter tarmog'iga zarar yetkazish uchun ataylab ishlab chiqilgan har qanday dasturiy ta'minot. 2019-yil sentabridagi zararli dasturlar:Zeus, Kovter, Dridex, Nanocore, Cryptowall, Ghost, Coinminer, Trickbot, Ursnif va Bifrose.

Tavsiya etilgan yechim(lar): Zararli dasturlarga asoslangan kiberhujumlardan kompyuteringizni himoya qilish uchun siz quyidagi amallarni bajarishingiz mumkin:

–Cheklangan foydalanuvchi ruxsati va dastur imtiyozlaridan foydalanish huquqi.

–Kuchli antivirus va zararli dasturlarga qarshi dasturlardan, elektron pochta spam-filtrlaridan foydalanish.

–Shubhali elektron pochta xabarlari va veb-saytlardan ma’lumotlaringizni himoya qilish uchun xodimlaringizni muntazam ravishda kiberxavfsizlik bo'yicha ogohlantirib, ularni kiberxavfsizlik bo’yicha bilimini oshirishga qaratilgan treninglarga ishtirok etishini taminllash.

3. Fishing hujumlarining har xil turlari va ijtimoiy muhandislik. Fishing - bu noqonuniy harakatlarni amalga oshirish (tarmoq yoki akkauntlarga kirish, ma'lumotlarga kirish, jabrlanuvchini pul o'tkazmalari kabi amallarni bajarish va hokazo) qilish orqali jabrlanuvchidan maxfiy ma'lumotlarni olishga qaratilgan firibgarlik urinishi.

Tavsiya etilgan yechim(lar): Kiberxavfsizlik tahdidlarini oldini olish uchun bir nechta ishlarni bajarishingiz mumkin:

–Har bir xodimni kiberxavfsizlikdan xabardor qilish bo'yicha ogohlantirish ishlarini amalga oshirish.

–Ishonchli elektron pochta va spam filtrlaridan foydalanish.

–Elektron pochtani shifrlash va elektron pochtani imzolash sertifikatlaridan foydalanish.

–Xavfsiz, shifrlangan ulanishlarni yaratish uchun veb-saytingizda HTTPS-dan foydalanish.

–Ikki bosqichli autentifikatsiyani ta'minlash.

4. Formjacking. Formjacking kiberxavfsizlikka tahdidning bir turi bo‘lib, kiberjinoyatchi veb-saytlarning kamchiliklaridan foydalangan holda saytni egallab oladi.

Tavsiya etilgan yechim(lar):Formjackingni oldini olishning ba'zi usullari mavjud. Bularga quyidagilar kiradi:

–Zaiflikni skanerlash va kirish testini o'tkazish kiberxavfsizlik himoyasidagi har qanday zaif tomonlarni aniqlashga yordam beradi.

–Bir veb-saytdan boshqasiga chiquvchi trafikni kuzatish.

–Veb-ilovalar va hujjatlar tomonidan foydalaniladigan fayllarda xeshlash yordamida kutilmagan, boshqariladigan tarkib bo'lmasligini ta'minlash uchun sub-resurs yaxlitligi (SRI) teglaridan foydalanish.

5. Kiberjinoyatchilikning yana bir turi — bu ma'lumotlarning bloklanishi va kompyuter va kompyuter tarmog‘ining buzilishiga olib keladigan ruxsatsiz kirishning turlaridan biri bo‘lgan DoS jinoyat yoki “xizmat ko‘rsatishni rad etish” tipidagi jinoyatlar. DoS jinoyatini xakerlar jinoyati va zararli dasturlardan foydalanishning sintezi sifatida ham ko‘rib chiqish mumkin, bunda farqning muhim o‘lchami ma'lumotlarni blokirovka qilishdan iborat bo‘lgan DoS jinoyatining maqsadi hisoblanadi. DoS jinoyatlari paytida ma'lumotni blokirovka qilish serverga va vositachilik qurilmalariga ortiqcha yuklashga asoslangan tizimlarga xalaqit beradi, bu esa saytga kirishni va kompyuter tizimidan foydalanishni oldini oladi.

Tavsiya etilgan yechim(lar): Ushbu kiberhujumni oldinin olish uchun siz serveringizni kuchaytirishingiz kerak bo’ladi. Shuningdek, Linux operatsion sistemasi serverilaridan foydalanish tavsiya etiladi. Bir vaqtda bitta kompyuterdan ko’p so’rov keladigan bo’lsa, o’sha kompyuterning IP manzilini blokka oladigan dasturiy vositadan foydalanishingiz kerak.

Shuni ta'kidlash kerakki, kiberhujum qurboni bo’lib qo’lish ko’p jihatdan eskirgan apparat va dasturiy ta’minotga bog’liq bo’lib qolishi mumkin. Shu sababli, apparat va dasturiy ta'minot aktivlarini (komponentlarini) yangilab turish tashkilotingiz tarmog'i, serverlari, qurilmalari, ma'lumotlari va mijozlari xavfsizligi uchun juda muhimdir. Agar siz eskirgan texnologiyalardan foydalanayotgan bo'lsangiz, sizning xavfsizlik himoyangiz dushmanlarni to'xtata olmaydi.

Tavsiya etilgan yechim(lar):Eskirgan apparat va dasturiy ta'minot natijaida kelib chiqadigan tahdidlarni oldini olishning ba'zi usullari quyidagilardan iborat:

–Tashkilotingiz uchun qurilmalarni boshqarish siyosatlarini ishlab chiqing va sanoatning eng yaxshi texnologiyalaridan foydalaning.

–Tizimlaringiz va dasturiy ta'minotingizni yangilab turish xakerlar tomonidan ma'lumotlaringizga xavf solishini oldini oladi.

–Ishlab chiqaruvchi yangilanishni chiqarganida, xavfsiz bo’lishi va kiberjinoyatchilar yangilangan dasturlarni zararlab ulgurmasdan uni darhol o’z tizimingizda qo'llashingiz kerak.

Buyumlar internetiga ishonchsizlik. Bugungi kunda rivojlanayotgan navbatdagi texnologiya bu buyumlar internet (IoT) bo‘lib, bu nafaqat Internet orqali moddiy dunyo obyektlarini ular o‘rtasida ma’lumot almashish uchun birlashtirish, balki shahar miqyosida, uyda va ishda odamlarning xulq-atvori to‘g‘risida ma’lumot to‘plash imkonini beradi. Ta’kidlash kerakki, ushbu texnologiya O‘zbekiston Respublikasida faol rivojlanmoqda. Dunyo obyektlarini birlashtiradigan buyumlar internetini keng miqyosda namoyish etish uchun quyidagi ma’lumotlarni berish kerak: Xalqaro simsiz tadqiqotlar forumining prognozlariga ko‘ra, 2020 yil oxiriga qadar bitta tarmoqqa birlashtiriladigan buyumlar soni 7 trln. donani tashkil qiladi. Umuman olganda, bitta tarmoqqa ulanishi mumkin bo‘lgan buyumlar sonining chegaraviy qiymati bir kishi uchun 5000 birlikka baholanmoqda, bu bizga 50 trlngacha narsalarni yagona ma’lumot almashish tarmog‘iga birlashtirish istiqbollari

to‘g‘risida gapirishga imkon beradi Ochiq veb-ilovalar xavfsizligi loyihasi yoki OWASP buyumlar interneti zaifliklari ro‘yxatining eng so‘nggi 10 tasini e’lon qilgani haqida xabar berdi. Bular: zaif, taxmin qilinadigan yoki qattiq kodlangan parollar, xavfsiz bo‘lmagan tarmoq xizmatlari, xavfsiz ekotizim interfeyslari, xavfsiz bo‘lmagan standart sozlamalar, xavfsiz ma’lumotlarni uzatish va saqlash, maxfiylikni himoya qilishning yetarli emasligi, xavfli yoki eskirgan komponentlardan foydalanish, xavfsiz yangilash mexanizmlarining yo‘qligi, qurilmaning boshqarishning yetishmasligi va texnik mustahkamlikning yetishmasligi.[7]

Tavsiya etilgan yechim(lar): Buyumlar interneti xavfsizligi tahdidlaridan himoya qilishning ba'zi usullari. Bularga quyidagilar kiradi:

Qurilmalaringizni himoya qilish, ma'lumotlar va maxfiylikni himoya qilish IoT-ni himoya qilishdir.

–Har qanday zaifliklar va potentsial majburiyatlarni aniqlash

–ikki faktorli autentifikatsiyadan foydalanish

–Foydalanuvchiga kirish va ilova imtiyozlarini cheklashga harakat qiling. Masalan, siz:

–binolar va kompyuterlar tarmog'iga jismoniy kirishni nazorat qilish.

–ruxsatsiz foydalanuvchilarga kirishni cheklash.

–ilova boshqaruvlari orqali ma’lumotlar yoki xizmatlarga kirishni cheklash.

–Xavfsizlik dasturidan foydalanish.

–Tizimlaringiz va dasturlaringiz muntazam yangilanib turishiga ishonch hosil qiling

–Har bir inson uchun kiberxavfsizlikdan xabardorlik bo'yicha treningni o'tkazing.

–Tizim va noodatiy tarmoq faoliyatini kuzatish uchun hujum detektorlaridan foydalanish.

–Nufuzli antivirus va zararli dasturlarga qarshi yechimlardan, elektron pochta spam-filtrlaridan va oxirgi nuqta xavfsizligi choralaridan foydalanish. [6].

Kiberxavfsizlik reytingida o'zbekistonning mavqei. Global reytinglarda O'zbekistonning mavqeini oshirish davlat siyosati darajasida ko'tarilgan. Kiberxavfsizlik darajasini aniqlash bo'yicha xalqaro va milliy reytinglarni o'rganish, ularda belgilangan baholash mezonlari bo'yicha davlat organlari va tashkilotlarida, muhim axborot infratuzilmasi obyektlarida axborot xavfsizligi siyosatini samarali yo'lga qo'yish dolzarb masalalardan biri hisoblanadi.

Kiberxavfsizlik sohasida buyumlar interneti bilan bog'liq bo'lgan tahlikalarning yuzaga kelayotgani jiddiy xavotirlarga sabab bo'lmoqda. Baholashlarga ko'ra, bugungi kunda 20 milliardga yaqin qurilma internetga ulangan holda ishlaydi. Kelgusi besh yil ichida bu ko'rsatkich ikki barobar oshishi taxmin qilinmoqda.

Davlat organlari va tashkilotlarida belgilangan xavfsizlik talablariga javob bermaydigan qurilmalardan foydalanish oqibatida kibertahdidlar soni va ko'lami ortib bormoqda. Bu holatni O'zbekistonning kibertahdidlarga duchor bo'lish indeksida

(CEI – Cybersecurity Exposure Index) 165 ta davlat orasida 90-o'rinda, ya‘ni kiberhimoyaning o’rtachadan past darajasi 36.36 indeks bilan baholanganligida ko'rish mumkin. Kiberxavfsizlki darajasi eng yuqori davlat esa Gretsiya hisoblanadi.Quyidagi rasmda O’zbekiston va Gretsiya davlatining kiberxavfsizlik darajasi bo’yicha o’rni, millliy kiberxavfsizlik indeksi

“Kiberxavfsizlik markazi” davlat unitar korxonasi O'zbekiston kibermuhitining xavfsizligi va sog'lomligini ta‘minlash, axborotlashtirish obyektlarining doimiy va uzluksiz

ishlashini qo'llab-quvvatlash, turli ko'lamdagi kiberhujumlardan himoya qilish bo'yicha ishlar olib bormoqda. Belgilangan maqsad va vazifalarni to'laqonli bajarish maqsadida markaz tomonidan Internet milliy segmentida axborot va kiberxavfsizlik hodisalari doimiy monitoring qilib boriladi.

Monitoring natijalariga ko'ra, o'tgan 2022 yilda internetning o'zbek segmentida axborot va kiberxavfsizlikka tahdid soluvchi 65 milliondan ortiq tarmoq hodisasi kuzatilgan.

“.UZ” domen zonasidagi veb-saytlarning uzluksiz monitoringi davomida 236 ta kiberxavfsizlik insidenti aniqlanib, ularning asosiy qismi ruxsatsiz kontent yuklash (191 ta) hamda asosiy oynani ruxsatsiz o’zgartirish (19 ta) bilan bog’liq bo’lgan insidentlardir. Aniqlangan insidentlarning tahlili shuni ko’rsatmoqdaki, davlat idoralarining veb-saytlari (50 ta) xususiy sektor vakillarining veb-saytlaridan (186 ta) ko’ra, 3 barobar kamroq hujumlarga uchragan.

Xulosa qilib shuni aytish joizki kiberxavfsizlikka tahdidlar siz kutmagan vaziyatlarda, sharoitlarda bo’lishi mumkin. IT sohasi rivojlangan sari kiberjinoyatlar ham ko’payaveradi va ularning yangi turlari kelib chiqadi. Buning natijasida davlat organlari, korparativ tashkilotlar va har bir internet foydalanuvchilarining shaxsiy ma’lumotlari xavf ostida qolishi mumkin. Ushbu kibertahdidlarning oldini olish uchun har bir internet foydalanuvchi shaxslar, tashkilotlar ehtiyot bo’lishlari lozim, hamda kiberxavfsizlikni ta’minlash va kiberjinoyat qurboni bo’lib qolishni oldini olish uchun ushbu maqoladagi ma’lumotlarga amal qilishlari tavsiya etiladi.

FOYDALANILGAN ADABIYOTLAR:

[1]. M. Duun, A Comparative Analysis of Cyber Security Initiatives Worldwide: WSIS Thematic Meeting on Cyber Security. Geneva, 28 Jun 1 July 2005.

[2]. J. Jang, and S. Nepal, “A Survey of Emerging Threats in Cyber security”. Journal of Computer and System Sciences, 80 (2014), 973-993. 2014.

[3]. M. Abomhara, and G. Koien, “Security and privacy in the internet of things: Current status and open issues,”. The 2nd International Conference on Privacy and Security in Mobile Systems (PRISMS 2014), Aalborg, Denmark, May 2014.

[4]. T. T. Abi, What is a Cyber Threat?, 2020. [Online]. Available: Http://www.upguard.com/blog/cyber threat

[5]. A. F. Eric, C. L. Edward, W.R John, and A.T. Catherine, The 2013 Cyber security Executive Order: Overview and Consideration of Congressional Research Service Report. 2013.

[6]. Common Cyber Security Measures. [Online]. Available:https://Nibusinessinfo.co.uk.html

[7] Интернет вещей (IoT): возможности и угрозы для современных организаций Интернет-ресурс // URL: https://cyberleninka.ru/article/n/internet-veschey-iot-vozmozhnosti-i-ugrozydlya-sovremennyh-organizatsiy

[8] Internet ma’lumotlari (Wikipedia sahifasi): https://uz.wikipedia. org/wiki/MarshGolden#/media/Fayl: Marshgolden.jpg

[9] Internet ma’lumotlari: https://ncsi.ega.ee/ncsi-index/?order=rank&type=c

[10] “Kiberxavfsizlik markazi” davlat unitar korxonasi veb sayti https://csec.uz/upload/iblock/33e/2022%20yil%20uchun%20yakuniy%20hisobot%20UZB.pdf
[11] Internet ma’lumotlari: https://ncsi.ega.ee/comp