KIBERXAVFSIZLIK – AXBOROT XAVFSIZLIGINING ASOSIDIR

Tursunov Farxod Baxodir o`g`li
Termiz davlat universiteti "Kompyuter va dasturiy injiniring kafedrasi o`qituvchisi.
+99899 6731007. farxoddd1007@gmail.com

Annotatsiya: *Ushbu maqolada Axborot xavfsizligi sohasining bugungi kundagi ahamiyati, sohadagi muhim omillarning umumiy tahlili, Kiberxavfsizlik yo'nalishidagi zarur chora tadbirlar haqida so'z boradi.*

Kalit so`zlar: *Axborot xavfsizligi, Kiberxavfsizlik, Konfidensiallik, Risk, kiberfiribgarlik.*

Annotation. *This article talks about the importance of information security today, a general analysis of important factors in the field, and necessary measures in the area of cyber security.*

Key words. *Information Security, Cyber Security, Confidentiality, Risk, Cyber Fraud.*

KIRISH

Axborot xavfsizligi (inglizcha: Information Security, shuningdek, inglizcha: InfoSec) — axborotni ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o'zgartirish, tadqiq qilish, yozib olish yoki yo'q qilishning oldini olish amaliyotidir. Ushbu universal kontseptsiya ma'lumotlar qanday shaklda bo'lishidan qat'iy nazar (masalan, elektron yoki, jismoniy) amal qiladi. Axborot xavfsizligini ta'minlashning asosiy maqsadi ma'lumotlarning konfidensialligi, yaxlitligi va mavjudligini muvozanatli, qo'llashning maqsadga muvofiqligini hisobga olgan holda va tashkilot faoliyatiga hech qanday zarar yetkazmasdan himoya qilishdir. Bunga, birinchi navbatda, asosiy vositalar va nomoddiy aktivlar, tahdid manbalari, zaifliklar, potensial ta'sirlar va mavjud xavflarni boshqarish imkoniyatlarini aniqlaydigan ko'p bosqichli xavflarni boshqarish jarayoni orqali erishiladi. Bu jarayon xavflarni boshqarish rejasining samaradorligini baholash bilan birga olib boriladi.

Axborot xavfsizligi kiberxavfsizlikdan ko'lami va maqsadi jihatidan farq qiladi. Bu ikki atama ko'pincha bir-birining o'rnida ishlatiladi, ammo aniqrog'i, kiberxavfsizlik axborot xavfsizligining kichik ko'rinishidir. Axborot xavfsizligi – bu jismoniy xavfsizlik, endpoint (so'nggi nuqta) xavfsizligi, ma'lumotlarni shifrlash va tarmoq xavfsizligi kabi ko'plab sohalarni qamrab oluvchi keng soha sanaladi. Shuningdek, bu ma'lumotni tabiiy ofatlar va serverdagi nosozliklar kabi tahdidlardan himoya qiluvchi axborot kafolati bilan chambarchas bog'liq bo'ladi.

O'zbekiston Respublikasi hududida davlat va xo'jalik boshqaruvi organlarida, shuningdek, mahalliy davlat hokimiyati organlarida (bundan buyon matnda tashkilotlar deb yuritiladi) axborot xavfsizligi siyosatini ishlab chiqish va amalga oshirishning asosiy tamoyillari va tartibini belgilovchi «O'zbekiston Respublikasi hududida axborot xavfsizligi siyosatini ishlab chiqish bo'yicha uslubiy qo'llanmalar» ham 2013–2020 yilllarda O'zbekiston Respublikasi Milliy axborot-kommunikatsiya tizimini rivojlantirishni muvofiqlashtirish bo'yicha Respublika komissiyasining 2016-yil 23-fevraldagi 7-bayoni bilan tasdiqlangan.

Axborot xavfsizligida yana bir atama mavjud bo’lib, u sohaning asosini tashkil etadi deb aytishimiz mumkin. Bu kiberxavfsizlik atamasidir. Kiberxavfsizlik atamasiga alohida to’xtalib, uni asl ma’nosini tushunib yetishimiz kerak. Ushbu atama alohida so’zlardan tashkil topgan bo’lib, uni alohida so’z birligida ma’nosini aniqlashtiramiz. “ Kiber ” atamasi odatda kompyuterlar, axborot texnologiyalari yoki internet bilan bog’liq narsalarni anglatadi.

Xavfsizlik – bu xavf yoki tahdiddan xoli bo’lish va xavfsiz bo’lish holatini anglatadi. Shunday qilib, agar ikkita so’zni birlashtirsak, “kiberxavfsizlik” kompyuterlarni, tarmoqlarni va internetga ulangan har qanday qurilmani har qanday xavf yoki tahdiddan xavfsiz saqlashni anglatadi.

Axborot Xavfsizligining Siyosati Quyidagi Yo'nalishlarni O'z Ichiga Oladi:

1. Xavfsizlikni ta'minlashning asosiy tamoyillari: Axborot tizimlarida xavfsizlikni oshirish uchun asosiy tamoyillar va standartlar joriy etiladi. Bunda xavfsizlik protokollari, shifrlash algoritmlari, kirish tizimlari va boshqa xavfsizlikning muhim tushunchalari keng tarqalgan bo'ladi.

2. Xavfsizlik risklarini tahlil qilish: Axborot tizimlaridagi xavfsizlik risklarini aniqlash, shu jumladan, zararli programmalarning identifikatsiyasi, hujjatlarni himoya qilish, foydalanuvchilar ma'lumotlarining himoyasi, tarmoqlarni himoyalash va xavfsizlik ko'nikmalari bilan bog'liq xavfsizlik risklarini tahlil qilishni o'z ichiga oladi.

3. Xavfsizlikning texnik va tashkiliy tomonlari: Xavfsizlikning o'rganishini va o'zgarishlarni belgilash uchun, texnik va tashkiliy qo'llanmalarni joriy etish, xavfsizlikni ta'minlash uchun kerakli vositalarni, texniklar va infratuzilmani amalga oshirishni o'z ichiga oladi.

4. Huquqiy muhofaza va nazorat: Axborot xavfsizligining siyosati, foydalanuvchilar va axborot tizimlariga zararli faollanishlarni oldini olish kerak.

Mavzuga oid adabiyotlar tahlili. Mamlakatimizda ham raqamli jamiyatni rivojlantirish uchun davlat va jamiyat ahamiyatidagi ishlar amalga oshirilmoqda. Xususan, Raqamli iqtisodiyotni rivojlantirishdagi yana bir qadam bu davlatimiz rahbari tomonidan 2020 – yilni “Ilm, ma`rifat va raqamli iqtisodiyotni rivojlantirish yili” deb e`lon qilinishi ham katta voqeylik bo`ldi. Bu o`z navbatida nafaqat 2020 -yil uchun qo`llanma va dastur bo`ldi, balki keying yaqin kelajak uchun katta tarixiy rivojlanish uchun ilk qadam vazifasini bajardi.[3]

Kiberxavfsizlikda juda muhim omillar majjud bo’lib, ular shu yo’nalishda vazifa jihatida juda katta ko'lamga ega. quyida shu omillardan ba’zilarini ko’rib chiqamiz.

Konfidensiallik - axborot yoki uni eltuvchining shunday holati bo’lib, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo’ladi. Konfidensiallik axborotni ruxsatsiz “o’qish”dan himoyalash bilan shug’ullanadi. Ayniqsa, bank sistemasida bank uchun konfidensiallik juda muhim.

Risk - potensial foyda yoki zarar bo’lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo’shilganida risk paydo bo’ladi. ISO “risk – bu noaniqlikning maqsadlarga ta’siri” sifatida ta’rif bergan.

Kiberxavfsizlik 8 ta bilim sohasiga bo’lingan:

• Ma’lumotlar xavfsizligi;

• Dasturiy ta’minot xavfsizligi;

• Tashkil etuvchilar xavfsizligi;
• Aloqa xavfsizligi;
• Tizim xavfsizligi;
• Inson xavfsizligi;
• Tashkilot xavfsizligi;
• Ijtimoiy xavfsizlik.

Mamlakatimizda ham kiberxavfsizlik sohasini rivojlantirish uchun ko'plab islohotlar amalga oshirilmoqda. 2022-yil 25-fevralda O'zbekistonda kiberxavfsizlik sohasidagi munosabatlarni tartibga solish maqsadida "Kiberxavfsizlik to'g'risida"gi qonun qabul qilindi. Qonunda kiberxavfsizlikni ta'minlashning asosiy prinsiplari sifatida quyidagilar keltirilgan:

• 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. [1]

Tez rivojlanib borayotgan axborot-kommunikatsiya texnologiyalari bizning kundalik hayotimizning barcha jabhalariga sezilarli o'zgarishlarni olib kirmoqda. Hozirda — axborot tushunchasi‖ sotib olish, sotish, biror boshqa tovarga almashtirish mumkin bo'lgan maxsus tovar belgisi sifatida tez-tez ishlatilmoqda.Shu bilan birga axborotning bahosi ko'p hollarda uning o'zi joylashgan kompyuter tizimining bahosida bir necha yuz va ming barobarga oshib ketmoqda. Shuning uchun tamomila tabiiy holda axborotni unga ruxsat etilmagan holda kirishdan, qasddan o'zgartirishdan, uni o'g'irlashdan, yo'qotishdan va boshqa jinoiy harakatlardan himoya qilishga kuchli zarurat tug'iladi. Ammo, jamiyatning avtomatlashtirishni yuqori darajasiga intilishi uni foydalaniladigan axborot texnologiyalarning xavfsizligi saviyasiga bog'liq qilib qo'yadi.

Kiberfiribgarlik - Kiber makonda buzg`unchi shaxslar sun`iy intellekt vositalaridan yolg`on ma`lumot yaratish, fishing kampaniyalarini tashkil qilish va zararli kod yozish uchun foydalanishlari mumkin. Bu Internet foydalanuvchilari uchun qo`shimcha tahdidlarni keltirib chiqaradi.

Tadqiqot metodologiyasi. Axborot xavfsizligi va unda xavfsizlik siyosati ishlab chiqishning ahamiyati ilmiy - statistik tahlil qilindi. Axborot xavfsizligida muhim o'rin tutuvchi kiberxavfsizlik tushunchasiga to'xtalib uning mohiyati va ma'nosi tahlil qilindi. To`plangan ma`lumotlarga asoslangan holda tizimli yondashuv hamda mantiqiy yondashuv kabi usullardan samarali foydalanildi.

Tahlil va natijalar. "Kiberxavfsizlik markazi" DUK(Davlat unitar korxonasi) tahlillariga ko'ra, 2020 -yilda internetning milliy segmenti(.uz) veb-saytlarida 27 milliondan ortiq zararli va shubhali tarmoq hujumlari kuzatilgan.Bularning asosiy qismi botnet tizimlaridagi faollik ga tegishli bo'lib, u 19 491 783 ta.Keyin esa, himoyasiz httpprotokolida 4 631 375 ta va boshqa insidentlarda ham nisbatan kichikroq kiberxujumlar ro'yxatga olingan.

2020-yilda milliy ".UZ" domen hududining zamonaviy axborot tizimlari va resurslari xavfsizligini oshirish bo'yicha chora-tadbirlarni amalga oshirish davomida 297 ta tadqiqot va ekspertiza o'tkazildi.Amalga oshirilgan ishlar natijasida 695 ta zaifliklar aniqlanib zaifliklar haqida axborot tizim va resurs egalari darhol xabardor qilindi.Aniqlangan zaifliklarning asosiy qismi o'ta xavfli (466 ta), o'rta xavfli(205ta) va past xavfli(24 ta) hodisalarga tegishli tartibda choralar ko'rildi .

Xulosa va takliflar. Xulosa o'rnida shuni aytish mumkinki, axborot xavfsizligi bugungi kunda respublikamizning raqamli iqtisodiyotini rivojlantirishning eng muhim elementi darajasiga ko'tarilmoqda. Axborot xavfsizligi madaniyatini mamlakatning tijorat tashkilotlari va davlat tuzilmalari faoliyatining barcha sohalariga chuqur singdirmasdan bozor ishtirokchilarining elektron hamkorligini kengaytirish va yangi axborot texnologiyalaridan keng foydalanish mumkin emas. Tashkilotlarda axborot xavfsizligi madaniyatini oshirishning eng samarali vositasi bo'lgan axborot xavfsizligi siyosati zamonaviy sharoitda muhim omil bo'lib qolmoqda. Bundan tashqari, yurtimizda iqtisodiy faoliyat va davlat boshqaruvi jarayonlarining raqamlashtirilishi kuchayishi bilan axborot xavfsizligi siyosatining roli tobora oshib bormoqda.

FOYDALALANILGAN ADABIYOTLAR RO`YXATI:

1. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi qonuni. 2022-yil 25 – fevral.
2. O'zR Prezidentining «Sun'iy intellekt texnologiyalarini jadal joriy etish uchun shart - sharoitlar yaratish chora-tadbirlari to'g'risida»gi qarori. PQ-4996-son. 17.02.2021y
3. F.B.Tursunov, R.R.G`aniyeva " Raqamli iqtisodiyotni rivojlantirishda axborot kommunikatsion texnologiyalarining o`rni` // maqola. – " Yangi O`zbekistonda ilm fanning so`nggi yutuqlari" Respublika ilmiy amaliy anjuman. 2023 – yil. 572-575 -b
4. Baxodir o'g'li T. F. AHOLI TURMUSH DARAJASI BAHOLASHNING AHAMIYATI //IJODKOR O'QITUVCHI. – 2022. – T. 2. – №. 19. – C. 49-51.
5. Yaxshimuratova X. X. TURMUSH FAROVONLIGINI OSHISHIDA AHOLI DAROMADLARINING O 'RNI //INTERNATIONAL CONFERENCES. – 2022. – T. 1. – №. 19. – C. 209-213.
6. Baxodir o'g'li T. F. AHOLI TURMUSH DARAJASINI BAHOLASHDA HAL QILINADIGAN MASALALAR VA UNING AXBOROT TA'MINOTINI ISHLAB CHIQISH //SCIENTIFIC ASPECTS AND TRENDS IN THE FIELD OF SCIENTIFIC RESEARCH. – 2023. – T. 1. – №. 10. – C. 211-216.
7. David Poole Alan Mack worth Artificial Intelligence: Foundations of Computation al Agents, Cambridge University Press, 2010.
8. www.stat.uz – O'zbekiston Respublikasi Davlat statistika qo'mitasi ma`lumotlari.
9. www.imv.uz