“JOURNAL OF SCIENCE-INNOVATIVE RESEARCH IN UZBEKISTAN” JURNALI
VOLUME 2, ISSUE 5, 2024. MAY
ResearchBib Impact Factor: 8.654/2023 ISSN 2992-8869

AXBOROT XAVSIZLIGI – BUGUNGII KUNNING DOLZARB MASALASI SIFATIDA

Farg‘ona viloyati Quva tuman kasb-hunar maktabi informatika va axborot texnologiyalri fani katta o‘qituvchisi
Yunusova Gulnoraxon Odilovna

Annotatsiya: Bugungi kunda globallashuv davrida axoborot va uning xavfsizligi muhimbo‘rin tutadi. Axborot tizimlarning zaifligi mamlakat xavfsizlik tizimiga bevosita ta’sir qiladi.

Kalit so‘zlar: kibernetika, axborot xavfsizligi, axborot kompyuter, axborot tizimlar.

Bugun butun dunyoda axborot tahdidlari tinmasdan uchrab turgani ham bor gap. Bunda barcha tashkilolar, hatto bugun internet tarmoqlari orqali ma’lumotni tarqab ketishi natijasida har yili tashkilotlar banklar milliardlab dollar zarar ko‘rishadi. Shunday ekan bugun har bir shaxs axborot egasiga tahdid mavjud ekan.

Bugungi kunda axborot xavfsizligi tushunchasiga ko'plab ta'riflar berilgan. Mana, ularning ikkitasi. Axborot xavfsizligi (inglizcha "Information security") - axborot va tegishli infratuzilmani, shuningdek ma'lumot egalariga yoki foydalanuvchilariga zarar etkazish bilan bog’liq tasodifiy yoki qasddan ta'sirlardan himoya qilinganligi. Axborot xavfsizligi - ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlash.4 O’zbekistonda axborot xavfsizligini ta’minlash va ma’lumotlarni muxofaza qilish bo’yicha «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.5 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. 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.

Axborotning muhimlik darajasi qadim zamonlardan ma’lum. Shuning uchun ham qadimda axborotni himoyalash uchun turli xil usullar qo‘llanilgan. Ulardan biri – sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o‘qish imkoniga ega bo‘lmagan. Asrlar davomida bu san’at – sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixonarezidensiyalari va razvedkamissiyalaridan tashqariga chiqmagan. Faqat bir necha o‘n yil oldin hamma narsa tubdan o‘zgardi, ya’ni axborot o‘z qiymatiga ega bo‘ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlabchiqaradilar, saqlaydilar, uzatadilar, sotadilar va sotiboladilar. Bulardan tashqari uni o‘g‘irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shunday qilib, axborotni himoyalash zaruriyati tug‘iladi. Axborotning himoyasi deb, boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta’minlovchi va tashkilot axborot zahiralarining yaxlitliligi, ishonchliligi, foydalanish osonligi va maxfiyligini ta’minlovchi qat`iy reglamentlangan dinamik texnologik jarayonga aytiladi. Axborotni himoyalashning maqsadlari quyidagilardan iborat:

- axborotning kelishuvsiz chiqib ketishi, o‘g‘irlanishi, yo‘qotilishi, o‘zgartirilishi, soxtalashtirilishlarning oldini olish;
- shaxs, jamiyat, davlat xavfsizliligiga bo‘lgan xavf
– xatarning oldini olish;
- axborotni yo‘qqilish, o‘zgartirish, soxtalashtirish, nusxako‘chirish, to‘siqlash bo‘yicha ruxsatetilmagan harakatlarning oldini olish;

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. “Kiberxavfsizlik markazi” DUK mutaxasislari 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. Hulosa o’rnida shuni aytish mumkinki, axborot xavfsizligi bo’ladigan taxdidlarni oldini olish yoki vujudga kelgan taxdidlarni bartaraf etish uchun me’yoriy xuququy bazaning mavjudligi, axborot xafvsizligini ta’minlash soxasidagi mutaxasislarining bilim va malakalarining mavjudligi muxim ahamiyat kasb etadi.

Har qanday axborot hisoblash tizimlarini tashkil etishdan maqsad foydalanuvchilarning talablarini bir vaqtda ishonchli axborot bilan ta’minlash hamda ularning konfedensialligini saqlash hisoblanadi. Bunda axborot bilan ta’minlash vazifasi tashqi va ichki ruxsat etilmagan ta’sirlardan himoyalash asosida hal etilishi zarur.

Axborot tarqab ketishiga konfedensial ma’lumotning ushbu axborot ishonib topshirilgan tashkilotdan yoki shaxslar doirasidan nazoratsiz yoki noqonuniy tarzda tashqariga chiqib ketishi sifatida qaraladi.

Adabiyotlar ro‘yhati:

1. Ўзбекистон Республикасининг “Ахборот олиш кафолатлари ва эркинлиги тўғрисида”ги қонуни. Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 1997 й.

2. Галяутдинов Р.Р. Информационная безопасность. Виды угроз и защита информации // Сайт преподавателя экономики. [2014]. URL: http://galyautdinov.ru/post/informacionnaya-bezopasnost

3.https://tace.uz/upload/iblock/5fb/Кибербезопасность_Республики_Узбекис тан_%20Итоги_2020_года.pdf.pdf

4. https://uzcert.uz/usefulinfo/prognoz-osnovnykh-riskov-kiberbezopasnosti-na2021-god/

5. Рекомендации - ГУП "Центр кибербезопасности" (tace.uz)