AXBOROT VA KIBERXAVFSIZLIK TUSHUNCHASI

Mamatqobilov Mirolim Zafar o‘g‘li
“Yosh chegarachilar” harbiy-akademik litseyi informatika va axborot texnologiyalari fani o‘qituvchisi

Annotatsiya: *Ushbu maqolada ta’lim jarayonida o‘quvchilarga axborot va kiberxafsizlik tushunchalari, muommolari va himoyalash haqida tushuncha beriladi. Kiberxavfsizlik axborot xafsizligining asosi hisoblanadi. Hozirgi davr shiddat bilan o‘sayotgan zaminda har bir ta’lim olayotgan yosh, zamon bilan hamnafas bo‘lishi kerakdir. O‘quvchilar axborotni kiber olamda ham himoyalash uchun qnday choralar amalga oshirilishi, nimalarga e’tibor qaratilishi haqida fikrlarimiz ushbu maqolada o‘rin olgandir.*

Kalit so‘zlar: *Axborot xavfsizligi, Kiberxavfsizlik, identifikatsiya, autentifikatsiya, avtorizatsiya,information security*

Axborotni ishlash, uzatish va to‘plashning zamonaviy usullarining rivojlanishi foydalanuvchilar axborotini yo‘qolishi, buzilishi va oshkor etilishi bilan bog‘liq tahdidlarning ortishiga olib kelmoqda. Shu sababli, kompyuter tizimlari va tarmoqlarida axborot xavfsizligini ta’minlash axborot texnologiyalari rivojining yetakchi yo‘nalishlaridan biri hisoblanadi.

Bugungi kunda axborot va kiberxavfsizlik dunyo miqyosida muhim va dolzarb masalalardan biriga aylangan. Texnologiyalar rivojlanishi va internetning keng tarqalishi bilan axborotlarni himoya qilish va kiberxavfsizlikni ta’minlash yanada murakkablashgan. Axborot xavfsizligi insoniyatning kelajagi, iqtisodiyoti va siyosiy barqarorligi uchun o‘ta zarur bo‘lgan tushuncha sifatida har jihatdan dolzarb.

Axborot texnologiyalari va raqamli tizimlar jamiyatning barcha jabhalariga chuqur kirib borishiga qaramay, kiberxavfsizlik va axborot xavfsizligi sohalariga nisbatan talab va ehtiyojlar hamon o‘sishda davom etmoqda. Bugungi kunda davlatlar, kompaniyalar va jismoniy shaxslar axborot xavfsizligini ta’minlash uchun yangi texnologiyalarni joriy etmoqda, tarmoqlar va tizimlarni xavfsiz qilishga harakat qilmoqda. Kiberxavfsizlik va axborot xavfsizligi — bu texnologik infratuzilma va resurslarni himoya qilish, ma’lumotlarning uzatish jarayonida xavfsizligini ta’minlash, hamda foydalanuvchilarning maxfiyligini himoya qilish kabi masalalarni o‘z ichiga oladi.

Axborot xavfsizligi

Axborot xavfsizligi (information security) — bu axborot tizimlarining ma’lumotlarni himoya qilish uchun amalga oshiriladigan barcha usullarni, jarayonlar va vositalarni o‘z ichiga oladi. Axborot xavfsizligining asosiy maqsadi ma’lumotlarning maxfiyligini, butunligini va mavjudligini ta’minlashdir. Buning uchun axborot xavfsizligi mutaxassislari turli xavf-xatarlarni oldini olish, tizimlarni himoya qilish, zarur xavfsizlik protokollarini joriy qilish va foydalanuvchi axborotlarini tasdiqlash ishlari bilan shug‘ullanadi.

Axborot xavfsizligining uchta asosiy prinsipi:

1. Maxfiylik (Confidentiality) — Axborotning faqat ruxsat etilgan shaxslar tomonidan mavjud bo‘lishi va foydalanilishi kerakligini ta’minlash. Misol uchun, shifrlash texnologiyalari yordamida axborot faqat to‘g‘ri va ruxsat etilgan foydalanuvchilarga ochiladi.
2. Butunlik (Integrity) — Axborotning o‘zgarishi, buzilishi yoki noto‘g‘ri yo‘naltirilishi oldini olish. Axborot tizimlarida joriy etilgan xatoliklar yoki zararli o‘zgarishlar tizimning to‘g‘ri ishlashiga ta’sir qilmasligi kerak.
3. Mavjudlik (Availability) — Axborot va tizimlarning doimiy ravishda, kerakli vaqtda mavjud bo‘lishi ta’minlanishi kerak. Har qanday shaxs yoki tizim axborotni zarur paytda olish imkoniyatiga ega bo‘lishi zarur.

Axborot xavfsizligi xatarlari:

- Tashqi tahdidlar — Hujumchilar yoki zararli dasturlar (malware) orqali tizimlarni buzish yoki ma’lumotlarni o‘g‘irlash.
- Ichki tahdidlar — Xodimlar yoki tashkilot ichidagi shaxslarning noto‘g‘ri yoki zararli harakatlari.
- Texnologik kamchiliklar — Tizimdagi zaifliklar yoki zaif parollarni o‘g‘irlash orqali ma’lumotlarga kirish imkoniyatlari.

Kiberxavfsizlik

“ *Kiber* ” atamasi odatda kompyuterlar, axborot texnologiyalari yoki internet bilan bog‘liq narsalarni anglatadi. Buni yaxshiroq tushunish uchun uni *kompyuterlar* va *internetga* tegishli maxsus so‘z sifatida tasavvur qiling .

Xavfsizlik – bu xavf yoki tahdiddan xoli bo’lish va xavfsiz bo’lish holatini anglatadi.

Kiberxavfsizlik – hisoblashlarga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni to‘g‘ri bajarilishini kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonlarni mujassamlashtiradi. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlillash va testlashni o‘z ichiga oladi. Kiberxavfsizlik ta’limning mujassamlashgan bilim sohasi bo‘lib, qonuniy jihatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni o‘z ichiga oladi.

Tarmoq sohasida faoliyat yuritayotgan Cisco tashkiloti esa kiberxavfsizlikka quyidagicha ta’rif bergan: Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberhujumlar odatda maxfiy axborotni boshqarishni, almashtirishni yoki yo‘q qilishni; foydalanuvchilardan pul undirishni; normal ish faoliyatini buzishni maqsad qiladi. Hozirda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar va ularning turlari sonining kattaligi va buzg‘unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda. Kiberxavfsizlik bilim sohasining zaruriyati birinchi meynfreym kompyuterlar ishlab chiqarilganidan boshlab paydo bo‘la boshlagan. Bunda mazkur qurilmalarning va ularning vazifalarining himoyasi uchun ko‘p sathli xavfsizlik choralari amalga oshirilgan. Milliy xavfsizlikni ta’minlash zaruriyatini oshib borishi kompleks va texnologik murakkab ishonchli xavfsizlik choralarini paydo bo‘lishiga sabab bo‘ladi.

Kiberxavfsizlik (cybersecurity) — bu raqamli tizimlar, tarmoqlar, dasturiy ta’minot va ma’lumotlarni kiberhujumlardan himoya qilishga qaratilgan harakatlar majmuasidir. Bu tushuncha nafaqat ma’lumotlarning himoyasi, balki tizimlarning ish faoliyatini saqlash, zararli xatti-harakatlarni oldini olish va kiberhujumlar natijasida tizimlar va ma’lumotlarning buzilishini oldini olishni o‘z ichiga oladi.

Kiberxavfsizlikning asosiy jihatlari:

1. Tarmoq xavfsizligi — Tarmoq va internet orqali uzatiladigan ma’lumotlarning xavfsizligini ta’minlash, xususan, tarmoqni himoya qilish uchun xavfsizlik devorlari (firewall) va boshqa texnologiyalarni ishlatish.
2. Dasturiy ta’minot xavfsizligi — Dasturlar va ilovalar foydalanuvchilarni kiberxavf-xatarlar, masalan, viruslar va xakerlik hujumlaridan himoya qilish uchun ishlab chiqilgan.
3. Ma’lumotlarni himoya qilish — Ma’lumotlarning saqlanishi va uzatilishi davomida shifrlash va boshqa xavfsizlik protokollarini ishlatish.
4. Foydalanuvchi xavfsizligi — Foydalanuvchi hisoblarini himoya qilish, parolni murakkab qilish va shaxsni tasdiqlashda qo‘shimcha usullarni (masalan, biometrik autentifikatsiya) joriy etish.

Kiberxavfsizlik tahdidlarining turlari:

1. Phishing — Foydalanuvchilarni aldaydigan yolg‘on elektron pochta yoki veb-saytlar orqali ma’lumotlarni o‘g‘irlash.
2. Malware (zararli dasturlar) — Viruslar, troyanlar, rootkitlar va boshqa zararli dasturlar orqali tizimlarni ishga solish va ma’lumotlarni o‘g‘irlash.

3. Ransomware — Tizimlarni shifrlash va undan foydalanish uchun to‘lov talab qilish.

4. DDoS (Distributed Denial of Service) hujumlari — Tarmoqni haddan tashqari yuklash orqali tizimlarni ishlashini to‘xtatish.

5. Zero-Day Exploit — Tizimdagi noma’lum zaifliklardan foydalanib, xavfsizlikni buzish.

Kiberxavfsizlikni ta’minlash usullari

1. Shifrlash (Encryption) — Ma’lumotlarni maxfiy saqlash va uzatish uchun shifrlash texnologiyalari qo‘llaniladi. Bu orqali faqat ruxsat etilgan shaxslar axborotni o‘qish imkoniga ega bo‘ladi.

2. Multifaktorli autentifikatsiya (MFA) — Foydalanuvchining kimligini tasdiqlash uchun bir nechta usullardan foydalanish (masalan, parol va mobil telefon orqali yuborilgan kod).

3. Xavfsizlik devorlaridan foydalanish — Xavfsizlik devorlari (firewalls) orqali tarmoqlarga kirishni nazorat qilish va noxush faoliyatni bloklash.

4. Antivirus dasturlari va zararkunandalarga qarshi himoya — Zararli dasturlarni aniqlash va tizimlarni himoya qilish uchun antivirus dasturlari va zararkunanda skanerlari.

5. Tezkor javob tizimlari (Incident Response) — Kiberhujum yuzaga kelganida, uni aniqlash va bartaraf etish uchun tezkor javob tizimlarini joriy qilish.

6. Zaifliklarni tahlil qilish (Vulnerability Assessment) — Tizim va dasturlardagi zaifliklarni aniqlash va tuzatish.

Kiberxavfsizlikni boshqarish va yondashuvlar

Kiberxavfsizlikni ta’minlash uchun har bir tashkilot o‘z xavfsizlik siyosatini ishlab chiqishi kerak. Bunga quyidagilar kiradi:

- Xavfsizlik siyosatini ishlab chiqish — tashkilotning barcha axborot tizimlarida xavfsizlikni ta’minlash uchun asosiy qoidalar va standartlarni belgilash.
- Xavfni boshqarish — xavf-xatarlarni tahlil qilish, ularni baholash va zaruriy choralar ko‘rish.
- Tizimlarni monitoring qilish — tizimlar va tarmoqlarni doimiy ravishda monitoring qilib, noma’lum faoliyatlarni aniqlash.
- O‘quv mashg‘ulotlari — xodimlarni kiberxavfsizlik bo‘yicha o‘qitish va xavfsizlikning asosiy tamoyillarini tushuntirish.

Axborot xavfsizligi sohasi, axborotning ifodalanishidan qat’iy nazar (qog‘oz ko‘rinishidagi, elektron va insonlar fikrlashida, og‘zaki va vizual) intelektual huquqlarni himoyalash bilan shug‘ullanadi.

Kiberxavfsizlik esa elektron shakldagi axborotni (barcha holatdagi, tarmoqdan to qurilmagacha bo‘lgan, o‘zaro birga ishlovchi tizimlarda saqlanayotgan, uzatilayotgan va ishlanayotgan axborotni) himoyalash bilan shug‘ullanadi.

XULOSA

Axborot xavfsizligi va kiberxavfsizlik bugungi raqamli dunyoda jamiyat va tashkilotlarning muhim ehtiyojiga aylangan. Bu sohalar bizning kundalik hayotimizga kirib, shaxsiy va professional faoliyatimizga bevosita ta’sir ko‘rsatmoqda. Kiberxavfsizlikni ta’minlash va axborotlarni himoya qilish masalalari texnologik rivojlanish bilan yanada muhimroq bo‘lib boradi. Tashkilotlar va jismoniy shaxslar uchun axborot xavfsizligi siyosatini ishlab chiqish va undan qat'iy rioya qilish, kiberxavfsizlikni ta’minlashdagi muvaffaqiyatni ta’minlaydi.

FOYDALANILGAN ADABIYOTLAR:

1. G'aniyev S. K., Karimov M. M., Tashev K. A. AXBOROT XAVFSIZLIGI Toshkent 07

2. S.S. Qosimov Axborot texnologiyalari xaqida o'quv qo'llanma Toshkent 07

3. G‘aniyev S.K.Karimov M.M. Hisoblash tizimlari va tarmoqlarida axborot xavfsizligi TDTU 03 4. http://www.kaspersky.ru/

4. Axborot xavfsizligi asoslari: Ma’ruzalar kursi / fizika-matematika fanlari nomzodi, katta ilmiy xodim I.M.Karimovning umumiy tahriri ostida. – T.: O‘zbekiston Respublikasi IIV Akademiyasi, 2013. – 123 b.

5. «Axborot texnologiyasi. Axborotlami kriptografik muhofazasi. Ma’lumotlami shifrlash algoritmi» 0‘zbekiston Davlat standard. 0‘zDSt 1105:2006 2. https://mininnovation.uz/ru/news/post-808

6. https://chat.openai.com/