XI-BOB. KIBERXAVFSIZLIK ASOSLARI.

Reja:

1. Kiberxavfsizlik tushunchasi va uning mazmuni
2. Kiberxavf turlari
3. Asosiy kiberxavfsizlik tamoyillari
4. Kiberxavfsizlik vositalari va texnologiyalari
5. Kiberhujumlardan himoya choralari
6. Shaxsiy ma’lumotlarni himoya qilish
7. Kiberxavfsizlik siyosati va qonunchilik asoslari
8. Kiberxavfsizlikdagi dolzarb muammolar va tahdidlar
9. Kiberxavfsizlikda foydalanuvchi madaniyati

11.1. Kiberxavfsizlik tushunchasi va uning mazmuni

“Kiberxavfsizlik” atamasining ta’rifi

Kiberxavfsizlik (Cybersecurity) — bu raqamli muhitda mavjud bo‘lgan axborot tizimlari, kompyuter tarmoqlari, qurilmalar, dasturiy ta’minotlar va foydalanuvchi ma’lumotlarini ruxsatsiz kirish, o‘g‘irlash, buzish, yo‘q qilish yoki o‘zgartirishdan himoya qilishga qaratilgan chora-tadbirlar tizimidir. Bu atama so‘nggi yillarda axborot texnologiyalarining tez sur’atlarda rivojlanishi va internet vositasida sodir bo‘layotgan hujumlar sonining oshishi sababli keng qo‘llanila boshlandi.

Kiberxavfsizlik nafaqat texnik himoya tizimlarini o‘z ichiga oladi, balki inson omiliga, ya’ni foydalanuvchi madaniyati, parol xavfsizligi, ijtimoiy muhandislikka qarshi choralar va xabardorlikni oshirishga ham katta e’tibor qaratadi.

Kiberxavfsizlikning maqsadi va zarurati

Kiberxavfsizlikning asosiy maqsadi — axborotning uchta asosiy tamoyilini ta’minlash:

1. Maxfiylik (Confidentiality) – ma’lumotlarga faqat ruxsat etilgan foydalanuvchilarning kirishini ta’minlash.
2. Butunlik (Integrity) – ma’lumotlar buzilmasdan, o‘zgarmasdan saqlanishini kafolatlash.
3. Mavjudlik (Availability) – axborot resurslariga doimo, kerakli vaqtda erkin kirish imkoniyatini ta’minlash.

Bugungi kunda shaxsiy ma’lumotlar, moliyaviy axborotlar, davlat sirlarini raqamli formatda saqlash keng tarqalgan. Shu sababli, har qanday raqamli tizimni kiberhujumlardan

himoya qilish dolzarb ehtiyojga aylangan. Masalan, bank tizimlariga bo‘lgan hujumlar moliyaviy yo‘qotishlarga olib kelsa, sog‘liqni saqlash tizimiga qilingan zararli hujumlar inson hayotiga tahdid solishi mumkin.

Axborot xavfsizligi va kiberxavfsizlik o‘rtasidagi farq

Ko‘pincha axborot xavfsizligi va kiberxavfsizlik tushunchalari o‘zaro almashlab ishlatiladi, biroq ular orasida farq mavjud:

Ko‘rsatkichlar	Axborot xavfsizligi	Kiberxavfsizlik
Mazmuni	Har qanday shakldagi (qog‘ozli, og‘zaki, raqamli) axborotni himoya qilish	Faqat raqamli axborot tizimlari va internetdagi tahdidlarga qarshi himoya
Soha ko‘lami	Keng: hujjatlar, faxlar, suhbatlar, tizimlar	Torroq: kompyuterlar, tarmoqlar, onlayn platformalar
Vositalari	Fizik xavfsizlik, siyosiy choralar, texnik va tashkiliy nazorat	Dasturiy himoya, shifrlash, tarmoq nazorati, xakerlikka qarshi kurash

Kiberxavfsizlik — bu axborot xavfsizligining bir bo‘lagi bo‘lib, asosan raqamli tahdidlar va internetga bog‘liq xatarlarga qarshi kurashishga qaratilgan. U kundan-kunga rivojlanib borayotgan texnologik xavflarga javob berish uchun muhim strategik yo‘nalish hisoblanadi.

Kiberxavfsizlik tarixining shakllanish bosqichlari

Kiberxavfsizlik bugungi kunda eng dolzarb sohalardan biri bo‘lsa-da, uning shakllanishi va rivojlanishi ko‘p bosqichli tarixiy jarayon natijasidir. Kiberxavfsizlikning shakllanish tarixi texnologik taraqqiyot bilan chambarchas bog‘liq.

1. Ilk bosqich: Axborot xavfsizligining boshlanishi (1950–1970 yillar)

Dastlabki yillarda kompyuterlar yakkaxon (lokal) tarzda ishlagan va tarmoqqa ulanmagan. Bu davrda axborot xavfsizligi tushunchasi fizik xavfsizlik (kompyuter xonasini qulflash, hujjatlarni saqlash) bilan bog‘liq edi.

AQSHdagi Department of Defense (Mudofaa vazirligi) ilk marta 1967-yilda axborot xavfsizligi siyosatini ishlab chiqqan.

1970-yillarda MULTICS (Multiplexed Information and Computing Service) tizimida ilk marta foydalanuvchilarni autentifikatsiyalash (parol bilan himoyalash) mexanizmi joriy etildi.

2. Tarmoqlar davri: Internet va yangi tahdidlar (1980–1990 yillar)

1980-yillarda ARPANET (Internetning ilk ko‘rinishi) kengayishi bilan kompyuterlar o‘rtasidagi tarmoq paydo bo‘ldi.

Bu davrda kompyuter viruslari, masalan, "Brain" (1986) va "Morris Worm" (1988) kabi dastlabki zararli dasturlar (malware) paydo bo‘ldi.

1986 yilda AQSHda "Computer Fraud and Abuse Act" (Kompyuter firibgarligi va suiiste'molligi to‘g‘risida qonun) qabul qilinib, raqamli jinoyatlar huquqiy asosda tan olindi.

1988 yilda ilk kiberxavfsizlik insidenti sifatida tan olingan “Morris Worm” internetdagi minglab kompyuterlarni ishdan chiqardi va ogohlantirish choralarini boshlashga sabab bo‘ldi.

3. Professional soha sifatida shakllanishi (1990–2000 yillar)

1990-yillarda internet ommalashdi va kiberhujumlar ko‘paydi. Bu esa axborot xavfsizligi bo‘yicha mutaxassislar ehtiyojini oshirdi.

Antivirus dasturlar (Symantec, McAfee, AVG) keng tarqala boshladi.

Firewalls (xavfsizlik devorlari) va IDS/IPS (tarmoq hujumlarini aniqlovchi tizimlar) joriy etildi.

1993-yilda RSA Data Security ilk raqamli shifrlash algoritmlarini taklif qildi.

Kiberxavfsizlik so‘zining o‘zi 1990-yillar oxirida akademik va amaliy muhitda faol ishlatila boshlandi.

4. Global muammo darajasiga chiqishi (2000–2010 yillar)

Bu davrda internet xizmatlari, elektron tijorat, onlayn bank xizmatlari kengaydi va kiberjinoyatchilik xalqaro darajaga chiqdi.

DDoS (Distributed Denial of Service) hujumlari, fishing, ransomware kabi kiber tahdidlar avj oldi.

2007-yil Estoniya tarixida yirik kiberhujumlar bo‘lib o‘tdi – bu kiberhujum bir davlatga qilingan ilk global tajovuz deb hisoblanadi.

2009-yilda “Stuxnet” nomli virus Eronning yadro inshootlarini nishonga olgan va u kiberqurol sifatida foydalanilgan birinchi virus bo‘ldi.

5. Zamonaviy davr: Sun’iy intellekt va ilg‘or texnologiyalar davri (2010–hozirgi vaqt)

Kiberxavfsizlik endilikda faqat texnik himoya emas, balki siyosiy, iqtisodiy, ijtimoiy muammolarga aylangan.

Ransomware hujumlari (WannaCry, Petya, LockBit) korxonalar, sog‘liqni saqlash muassasalari, hatto davlat tashkilotlariga tahdid solmoqda.

Sun’iy intellekt (SI) va Big Data kiberxavfsizlikda ishlatilmoqda – tahdidlarni oldindan bashorat qilish va avtomatik himoya qilish imkoniyati yaratilmoqda.

Kiberxavfsizlik milliy xavfsizlik darajasiga ko‘tarildi: har bir rivojlangan davlat o‘zining milliy kiberxavfsizlik strategiyasini ishlab chiqmoqda (masalan, AQSH, Xitoy, Isroil, Rossiya va O‘zbekiston).

Kiberxavfsizlik bugungi kunda texnologik taraqqiyotga hamnafas rivojlanib, oddiy foydalanuvchidan tortib, global davlatlar darajasigacha muhim masalaga aylangan. Uning tarixi — texnologiya va tahdidlar o‘rtasidagi uzluksiz kurash tarixidir. Har bir bosqichda yangi xavf-xatarlar, shuningdek, ularni bartaraf etish vositalari yuzaga kelgan. Bugungi kunda kiberxavfsizlik — ta’lim, sog‘liqni saqlash, sanoat, moliya, va davlat boshqaruvida hal qiluvchi rol o‘ynamoqda.

11.2. Kiberxavf turlari

Kiberxavfsizlik – bu nafaqat texnik himoya, balki raqamli muhitdagi real xavf-xatarlarni aniqlash, oldini olish va ularga qarshi kurashish tizimi hamdir. Bugungi kunda internet foydalanuvchilari duch keladigan kiberxavf-xatarlar xilma-xil bo‘lib, ularni quyidagi asosiy toifalarga ajratish mumkin:

Kompyuter viruslari, troyanlar va zararli dasturlar (Malware)

Zararli dastur (Malware) – bu foydalanuvchining roziligisiz kompyuter tizimiga kirib, ma’lumotlarni o‘g‘irlash, o‘chirish, buzish yoki foydalanuvchining faoliyatiga zarar yetkazish uchun yaratilgan dasturiy ta’minot turidir.

Viruslar o‘zini boshqa fayllarga yoki tizimlarga ko‘paytiradi va odatda ishlayotgan fayllarga zarar yetkazadi.

Troyanlar (Trojan Horse) o‘zini foydali yoki zararsiz dastur sifatida ko‘rsatib, foydalanuvchining kompyuteriga kirib oladi va orqa fonda zarar yetkazadi.

Spyware – foydalanuvchining faoliyatini yashirin tarzda kuzatadi.

Ransomware – tizim yoki fayllarni shifrlab, ularga kirishni cheklaydi va to‘lov talab qiladi.

Himoya chorasi: Antivirus dasturlari, doimiy yangilanishlar va ehtiyotkorlik bilan fayllarni yuklab olish.

Phishing (Qarmoqqa ilish) va ijtimoiy muhandislik

Phishing – bu foydalanuvchini aldash orqali maxfiy ma’lumotlarini (parol, karta raqami, login) olishga qaratilgan firibgarlik turi.

Odatda elektron pochta orqali bank, ijtimoiy tarmoq yoki davlat nomidan yuborilgan soxta xabarlar orqali amalga oshiriladi.

Ijtimoiy muhandislik – bu texnik vositalarsiz, balki psixologik usullar bilan foydalanuvchini o‘zining maxfiy ma’lumotlarini oshkor qilishga undashdir.

Himoya chorasi: Havolalarga ehtiyotkorlik bilan qarash, real manbalardan tekshirish, ikki bosqichli autentifikatsiya.

DDoS hujumlar (Distributed Denial of Service)

DDoS – bu server, sayt yoki tarmoq xizmatini haddan tashqari ko‘p so‘rovlar orqali band qilib, ularni ishdan chiqarish hujumidir.

Bu hujumda minglab “zombi” kompyuterlar bir vaqtning o‘zida bitta manzilga murojaat qilib, serverni o‘z ishini bajara olmaydigan holatga olib keladi.

Ko‘pincha raqobatchilarga zarar yetkazish, siyosiy yoki iqtisodiy bosim o‘tkazish uchun qo‘llaniladi.

Himoya chorasi: Tarmoq trafik monitoringi, xavfsizlik devorlari, DDoS-ga qarshi himoya xizmatlari (CDN, Cloudflare).

Xakerlik va noqonuniy tizimga kirish (Unauthorized Access)

Xakerlik – bu foydalanuvchi ruxsatisiz kompyuter tizimi, server, tarmoq yoki platformalarga noqonuniy tarzda kirish harakatidir.

White-hat hackers – tizimlardagi zaifliklarni aniqlab, ularga tuzatish kiritishga yordam beruvchi mutaxassislar.

Black-hat hackers – yovuz niyatli, foydalanuvchining ma’lumotini buzish, o‘g‘irlash, o‘chirish maqsadida tizimlarga kiruvchi kiberjinoyatchilar.

Grey-hat hackers – qoidalarni buzib, ammo zarar yetkazmasdan tizimdagi zaifliklarni ko‘rsatib beruvchilar.

Himoya chorasi: Kuchli parollar, xavfsiz autentifikatsiya tizimlari, VPN, xavfsizlik devorlari, log-fayllarni monitoring qilish.

Kiberxavf turlari tobora ko‘payib, murakkablashib bormoqda. Har bir foydalanuvchi kiberxavfsizlikka jiddiy yondashmog‘i va o‘zini, tizimini himoyalash uchun zarur vosita va bilimlarga ega bo‘lishi kerak. Eng oddiy ehtiyotsizlik ham katta tahdidga sabab bo‘lishi mumkin. Shuning uchun, zamonaviy kiber tahdidlarga qarshi kurashish – har bir foydalanuvchining raqamli madaniyatining ajralmas qismiga aylanishi lozim.

11.3. Asosiy kiberxavfsizlik tamoyillari

Kiberxavfsizlik sohasining asosiy vazifasi – raqamli resurslar, ma’lumotlar va tizimlarning ishonchli ishlashini ta’minlashdir. Bu maqsadga erishish uchun bir nechta asosiy tamoyillar mavjud bo‘lib, ular har qanday kiberxavfsizlik siyosatining negizini tashkil etadi. Quyidagi tamoyillar axborot xavfsizligining “CIA triadasi” (Confidentiality, Integrity, Availability) va unga qo‘shimcha tamoyillar asosida yoritiladi:

1. Maxfiylik (Confidentiality)

Maxfiylik – axborot faqat ruxsat etilgan shaxslar tomonidan ko‘rilishini yoki foydalanilishini ta’minlovchi tamoyildir.

- Bu tamoyil foydalanuvchilarning shaxsiy ma’lumotlari, moliyaviy axborotlari yoki tashkilotga tegishli maxfiy hujjatlarning begona shaxslar qo‘liga tushmasligini kafolatlaydi.
- Maxfiylikni ta’minlash vositalariga shifrlash (encryption), parollar, kirishni nazorat qilish tizimlari va ro‘yxatdan o‘tish mexanizmlari kiradi.

Masalan: Bankda mijozning hisob raqami faqat u yoki vakolatli xodimlar tomonidan ko‘rilishi kerak.

2. Butunlik (Integrity)

Butunlik – ma’lumotlarning aniqligi, to‘g‘riligi va o‘zgarmasligiga ishonch hosil qiluvchi tamoyildir.

- Axborot tizimida saqlanayotgan yoki uzatilayotgan ma’lumotlar ruxsatsiz o‘zgartirishdan himoyalangan bo‘lishi kerak.

- Ma’lumotni buzish, o‘zgartirish yoki almashtirish tizimni ishdan chiqarishi, yolg‘on tahlillarga olib kelishi mumkin.

Texnik jihatdan bu tamoyil hashing algoritmlari, versiyalash, raqamli imzolar, zaxira nusxalar yordamida amalga oshiriladi.

3. Foydalanish imkoniyati (availability)

Foydalanish imkoniyati – axborot resurslari va tizimlar doimiy ravishda ruxsat etilgan foydalanuvchilar uchun ochiq va ishlaydigan bo‘lishini anglatadi.

- Foydalanuvchi o‘z vaqtida kerakli resursdan foydalanish imkoniyatiga ega bo‘lmasligi tizimning ishdan chiqishiga yoki foydasiz bo‘lishiga olib keladi.
- DDoS hujumlari aynan ushbu tamoyilga qarshi qaratilgan bo‘ladi.

Uskunalar ishonchliligi, avariyalardan tiklanish (disaster recovery), zaxira serverlar va uzluksiz xizmat ko‘rsatish rejasi muhim rol o‘ynaydi.

4. Autentifikatsiya va avtorizatsiya

Bu ikki tamoyil, ko‘pincha birgalikda ishlaydi:

- Autentifikatsiya – foydalanuvchi yoki tizimning kimligini aniqlash (masalan, parol, biometrik, ikki bosqichli tasdiqlash).
- Avtorizatsiya – autentifikatsiyadan o‘tgan foydalanuvchiga qanday resurslarga, qanday darajada ruxsat berilishini belgilash (masalan, “faqat o‘qish” yoki “tahrirlash” huquqi).

Masalan: Talaba universitet portaliga kirganda, autentifikatsiyadan keyin faqat o‘z kurslariga avtorizatsiya qilinadi.

Kiberxavfsizlikning asosiy tamoyillari – maxfiylik, butunlik, foydalanish imkoniyati, hamda autentifikatsiya va avtorizatsiya — har qanday tashkilot, ta’lim muassasasi yoki shaxsiy foydalanuvchi uchun raqamli xavfsizlik asoslarini tashkil etadi. Bu tamoyillarni hayotga tatbiq qilish orqali raqamli dunyodagi xavflar sezilarli darajada kamayadi, axborotga bo‘lgan ishonch esa oshadi.

11.4. Kiberxavfsizlik vositalari va texnologiyalari

Bugungi kunda kiberxavfsizlik tahdidlari tobora murakkablashib borayotgan bir davrda, raqamli tizimlarni himoya qilish uchun bir qator zamonaviy vositalar va texnologiyalar ishlab chiqilgan. Ular foydalanuvchi ma’lumotlarini, tarmoqlarni va

kompyuter tizimlarini turli xurujlar, zararli dasturlar hamda nolegitim kirishlardan himoya qilishga qaratilgan. Quyida ularning eng asosiy turlarini ko‘rib chiqamiz:

1. Antiviral dasturlar va xavfsizlik devorlari (Firewall)

Antiviral dasturlar:

- Bu dasturlar kompyuter tizimiga tushgan zararli kodlar – viruslar, trojanlar, spyware kabi elementlarni aniqlash, izolyatsiya qilish va yo‘q qilish uchun ishlatiladi.
- Ular real vaqt rejimida skanerlash, fayl faoliyatini nazorat qilish, va avtomatik yangilanish kabi funksiyalarga ega.

Firewall (xavfsizlik devori):

- Bu tizim lokal tarmoq bilan tashqi internet o‘rtasida filtr vazifasini bajaradi.
- Foydalanuvchi qurilmasiga kiruvchi va chiquvchi trafikni nazorat qilib, ruxsatsiz harakatlarni bloklaydi.
- U apparat (hardware) va dasturiy (software) shakllarda bo‘lishi mumkin.

Masalan: Windows Defender Firewall yoki Cisco Firewall.

2. VPN (Virtual Private Network)

VPN — Virtual xususiy tarmoq bo‘lib, foydalanuvchi internetdan foydalanayotganida uning ma’lumotlarini shifrlangan kanalda uzatadi.

- VPN orqali foydalanuvchining IP-manzili yashiriladi va u boshqa mamlakatda joylashgandek ko‘rinadi.
- Bu texnologiya ochiq Wi-Fi tarmoqlarida xavfsiz ulanish, geo-bloklangan kontentga kirish hamda shaxsiy ma’lumotlarni himoya qilish uchun qo‘llaniladi.

Mashhur VPN xizmatlari: NordVPN, ExpressVPN, ProtonVPN.

3. Shifrlash (Encryption) texnologiyalari

Shifrlash — ma’lumotlarni ruxsatsiz shaxslar tushunmaydigan formatga aylantirish texnologiyasidir.

- Bu vosita orqali yuborilayotgan yoki saqlanayotgan axborot, faqat maxsus kalit (key) yordamida o‘qilishi mumkin bo‘lgan holga keltiriladi.
- Shifrlashning mashhur algoritmlari: AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), SHA (Secure Hash Algorithm).

Misollar:

- Bank tizimlarida kartadan foydalanish vaqtida ma’lumotlar shifrlanadi.
- WhatsApp yoki Telegram kabi messenjerlar "end-to-end" shifrlashdan foydalanadi.

4. Biometrik autentifikatsiya

Biometrik autentifikatsiya – foydalanuvchining biologik yoki xulqiy xususiyatlari asosida tizimga kirishini nazorat qiluvchi xavfsizlik texnologiyasidir.

Mashhur usullari:

- Barmoq izi (fingerprint)
- Yuzni aniqlash (facial recognition)
- Ko‘z qorachig‘i (iris scan)
- Ovozni tanish (voice recognition)

Bu texnologiya ikki bosqichli autentifikatsiya (2FA) tizimlarining muhim komponentidir. U an’anaviy parollarga nisbatan yuqori darajadagi xavfsizlikni ta’minlaydi.

Kiberxavfsizlik vositalari va texnologiyalari — zamonaviy axborot infratuzilmasining ajralmas qismidir. Antiviral dasturlar, xavfsizlik devorlari, VPN texnologiyasi, shifrlash usullari va biometrik autentifikatsiya vositalari kiberxavf-xatarlarni kamaytirish, axborotlar ustidan nazoratni kuchaytirish va foydalanuvchilarning shaxsiy hayotini himoya qilishda muhim rol o‘ynaydi. Har qanday tashkilot va shaxs ushbu vositalardan samarali foydalangan holda o‘z raqamli xavfsizligini mustahkamlashi mumkin.

11.5. Kiberhujumlardan himoya choralari

Kiberhujumlar – bu kompyuter tizimlari, tarmoqlar, foydalanuvchilar ma’lumotlariga ruxsatsiz kirish yoki ularni buzish maqsadida amalga oshiriladigan zararli harakatlardir. Bugungi kunda bunday tahdidlar soni va murakkabligi ortib

borayotgani sababli, har bir foydalanuvchi va tashkilot o‘zini kiberhujumlardan himoya qilish uchun muhim choralarni ko‘rishi zarur. Quyida asosiy va samarali himoya choralari yoritib berilgan:

1. Kuchli parollar yaratish va ularni boshqarish

Kuchli parol – bu birinchi himoya qatlamidir. Parollar quyidagi talablarga javob berishi lozim:

- Kamida 10–12 belgidan iborat bo‘lishi;
- Katta va kichik harflar, raqamlar hamda maxsus belgilarni o‘z ichiga olishi;
- Foydalanuvchining shaxsiy ma’lumotlariga (ism, tug‘ilgan sana va h.k.) asoslanmagan bo‘lishi kerak.

Parol boshqaruv tizimlari (masalan, LastPass, Bitwarden) orqali parollarni xavfsiz saqlash va avtomatik yangilash mumkin.

2. Qurilmalarni va dasturlarni muntazam yangilab borish

Dasturiy ta’minot va operatsion tizimlar vaqt o‘tishi bilan zaifliklarga ega bo‘lishi mumkin. Shuning uchun:

- Operatsion tizim (Windows, macOS, Linux) va mobil tizimlarni muntazam yangilash kerak;
- Antivirus va xavfsizlik devorlarini yangilab turish shart;
- Ilovalarni faqat ishonchli manbalardan o‘rnatish va ularning so‘nggi versiyasidan foydalanish zarur

Bu chora kiberjinoyatchilarning “exploit”lar (zaifliklardan foydalanish) orqali tizimga kirishining oldini oladi.

3. Elektron pochta xavfsizligi va shubhali havolalardan ehtiyot bo‘lish

Ko‘pgina kiberhujumlar (xususan, phishing) elektron pochta orqali amalga oshiriladi. Quyidagilarga e’tibor berish kerak:

- Noma’lum manbalardan kelgan xabarlarga javob bermaslik;
- Havolalarga bosishdan oldin ularning manzilini tekshirish;
- Ilovalarni ochishdan avval ularni antivirus bilan tekshirish;
- Elektron pochta platformasida 2 bosqichli autentifikatsiyani yoqish.

Misol: phishing xabarlari ko‘pincha bank, pochta yoki kompaniya nomidan yuborilgandek ko‘rinadi, lekin havola soxta bo‘ladi.

4. Tarmoq xavfsizligini ta’minlash

Tarmoq – bu kiberhujumlar uchun eng keng yo‘nalishlardan biridir. Shuning uchun quyidagilarga e’tibor qaratish lozim:

- Uy va ofis Wi-Fi tarmoqlarini kuchli parol bilan himoyalash;
- Routerning standart parolini darhol o‘zgartirish;
- VPN (Virtual Private Network) orqali ochiq tarmoqlarda ishlash;
- Tarmoq faoliyatini muntazam kuzatish va noma’lum qurilmalarga ruxsat bermaslik.

Wi-Fi tarmog‘i orqali o‘g‘irlangan ma’lumotlar katta xavf tug‘dirishi mumkin, ayniqsa moliyaviy yoki shaxsiy axborotlar bo‘lsa.

Kiberhujumlardan himoya qilish nafaqat IT mutaxassislarning, balki har bir foydalanuvchining majburiyatidir. Kuchli parollar, muntazam yangilanishlar, hushyorlik bilan ishlash, xususan e-pochta va internet tarmog‘ida ehtiyotkorlik — kiberxavfsizlikning asosiy ustunlaridir. Ushbu oddiy, ammo samarali choralarni ko‘rish orqali yirik xavflarning oldini olish mumkin.

11.6. Shaxsiy ma’lumotlarni himoya qilish

Bugungi raqamli davrda har bir foydalanuvchi o‘zining shaxsiy ma’lumotlariga ega: ism-familiyasi, manzili, telefon raqami, moliyaviy hisoblari, sog‘ligi yoki ish faoliyatiga doir axborotlar. Ushbu ma’lumotlar kiberjinoyatchilar uchun qimmatli resurs hisoblanadi. Shu bois shaxsiy ma’lumotlarni himoya qilish zamonaviy kiberxavfsizlik siyosatining muhim yo‘nalishlaridan biridir. Quyida eng asosiy choralarga to‘xtalamiz:

1. Ma’lumotlarni zaxiralash (backup qilish)

Zaxiralash (backup) – bu ma’lumotlarning nusxasini boshqa xavfsiz joyda saqlash orqali ularni yo‘qolishdan, buzilishdan yoki kiberhujumlardan himoya qilish usulidir. Zaxiralashning asosiy turlari:

- Mahalliy zaxira (kompyuterga yoki tashqi diskka);
- Bulutli zaxira (Google Drive, Dropbox, OneDrive kabi xizmatlar orqali).

Muhim hujjatlar, fotosuratlar, loyihalar muntazam ravishda avtomatik zaxiralanib turilishi lozim.

2. Onlayn faoliyatda maxfiylikni saqlash

Internetda faoliyat yuritayotgan har bir foydalanuvchi quyidagilarga rioya qilishi zarur:

- Faqat kerakli hollardagina shaxsiy ma’lumotlarni onlayn kiritish;
- Saytlarga kirishda HTTPS xavfsiz protokolini tanlash;
- Xavfsiz parollar yaratish va ularni tez-tez almashtirib turish;
- Internetda anonimlikni ta’minlash uchun VPN xizmatlaridan foydalanish.

Maxfiylikni saqlash — ma’lumotlarning noqonuniy foydalanilishining oldini olishga xizmat qiladi.

3. Ijtimoiy tarmoqlarda xavfsiz xatti-harakatlar

Ijtimoiy tarmoqlar (Facebook, Instagram, Telegram, TikTok va boshqalar) foydalanuvchilardan ko‘p miqdorda shaxsiy ma’lumotlarni yig‘adi. Shu bois quyidagi choralarni ko‘rish muhim:

- ✓ Profil sozlamalarida maxfiylik darajasini sozlash (masalan, faqat do‘stlar ko‘rsin);
- ✓ Telefon raqami, yashash manzili, GPS joylashuv kabi ma’lumotlarni ochiq joylashtirmaslik;
- ✓ Shubhali akkauntlar, havolalar va do‘stlik so‘rovlaridan ehtiyot bo‘lish;
- ✓ Har qanday shaxsiy yoki moliyaviy ma’lumotni DM orqali begonalarga yubormaslik.

Ijtimoiy tarmoqlarda ehtiyotsizlik – shaxsiy hayotga tajovuz, xakerlik yoki firibgarlik holatlariga sabab bo‘lishi mumkin.

Shaxsiy ma’lumotlar – insonning raqamli identiteti. Ularni himoya qilish esa har bir foydalanuvchining mas’uliyatli harakati va bilimiga bog‘liq. Ma’lumotlarni zaxiralash, onlayn maxfiylikni ta’minlash va ijtimoiy tarmoqlarda ehtiyotkorlik — bu nafaqat texnik chora, balki raqamli madaniyatning asosiy qismlaridandir.

11.7. Kiberxavfsizlik siyosati va qonunchilik asoslari

Kiberxavfsizlik nafaqat texnologik choralarni o‘z ichiga oladi, balki qonuniy, siyosiy va huquqiy tartibga solish asoslari bilan ham chambarchas bog‘liq. Har bir davlat o‘z raqamli infratuzilmasining barqarorligi va fuqarolarining ma’lumot xavfsizligini ta’minlash maqsadida kiberxavfsizlik siyosatini ishlab chiqadi. Shu jumladan, xalqaro hamjamiyatda ham universal standart va qonunlar shakllangan.

O‘zbekiston Respublikasida axborot xavfsizligi qonunlari

O‘zbekistonda so‘nggi yillarda raqamli transformatsiya tez sur’atlar bilan kechmoqda. Shu bilan birga, axborot xavfsizligini ta’minlash bo‘yicha huquqiy bazalar yaratilmoqda. Quyidagi qonun va hujjatlar muhim rol o‘ynaydi:

1. “Axborotlashtirish to‘g‘risida”gi Qonun – axborot resurslari va texnologiyalaridan foydalanish tartiblarini belgilaydi;
2. “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun (2019-yil) – fuqarolarning shaxsiy ma’lumotlarini yig‘ish, saqlash va himoya qilish me’yorlarini belgilaydi;
3. “Elektron hukumat to‘g‘risida”gi Qonun – davlat xizmatlarini raqamlashtirishda axborot xavfsizligini ta’minlash tamoyillarini o‘z ichiga oladi;
4. O‘zbekiston Respublikasi Prezidentining qarorlariga binoan, Kiberxavfsizlik markazi va tegishli texnik idoralar tashkil etilgan.

Xalqaro kiberxavfsizlik standartlari (ISO/IEC 27001 va boshqalar)

ISO/IEC 27001 – bu axborot xavfsizligini boshqarish tizimiga (ISMS) oid xalqaro standart bo‘lib, tashkilotlarga axborotni qanday muhofaza qilishni ko‘rsatadi. Ushbu standart:

- Tashkilotlarda xavfsizlik siyosatini shakllantirish;
- Risklarni baholash va boshqarish;
- Axborot aktivlarini to‘g‘ri boshqarish;
- Uzoq muddatli himoya strategiyalarini ishlab chiqish imkonini beradi.
- Bundan tashqari:
- ISO/IEC 27002 – xavfsizlik choralarining qo‘llanma shaklidagi tavsiyalarini o‘z ichiga oladi;

- NIST Cybersecurity Framework – AQShda ishlab chiqilgan kiberxavfsizlik amaliyoti asosidagi qo‘llanma.

Global qonunchilik: GDPR, CCPA va boshqa me’yorlar

Dunyo miqyosida fuqarolarning shaxsiy ma’lumotlarini himoya qilish borasida quyidagi qonunchiliklar asosiy o‘rinni egallaydi:

- ✓ GDPR (General Data Protection Regulation) – Yevropa Ittifoqining 2018-yildan kuchga kirgan qonuni. U:
  - Fuqarolarning ma’lumot ustidan nazoratini oshiradi;
  - Kompaniyalarga ma’lumotlarni qayta ishlash bo‘yicha aniq ruxsat olishni majbur qiladi;
  - Ma’lumotlar buzilganida 72 soat ichida xabardor qilish talabini belgilaydi.
- ✓ CCPA (California Consumer Privacy Act) – AQShning Kaliforniya shtatida qabul qilingan qonun bo‘lib, iste’molchilarning shaxsiy ma’lumotlariga egalik huquqini kafolatlaydi.

Bu qonunlar kiberxavfsizlik sohasidagi shaffoflik, ishonchlilik va hisobdorlik tamoyillarini mustahkamlashga xizmat qiladi.

Kiberxavfsizlik siyosati va qonunchilik asoslari – davlatlar va tashkilotlar darajasida axborot muhofazasining kafolati hisoblanadi. Har bir raqamli foydalanuvchi, muassasa yoki tadbirkor bu qonunchilik asosida o‘z faoliyatini yo‘lga qo‘yishi kerak. O‘zbekiston xalqaro standartlarga uyg‘un holda o‘zining kiberxavfsizlik siyosatini yanada takomillashtirib bormoqda.

11.8. Kiberxavfsizlikdagi dolzarb muammolar va tahdidlar

Kiberxavfsizlik sohasi bugungi kunda jadal rivojlanayotgan texnologiyalar bilan birga doimiy tahdidlar va muammolarga duch kelmoqda. Kiberjinoyatchilar tobora murakkabroq va aqlli usullarni qo‘llab, tashkilotlar, hukumat idoralari va oddiy foydalanuvchilarga qarshi yangi shakldagi hujumlar uyushtirmoqda. Quyida ayni paytda eng dolzarb sanalayotgan tahdidlar va muammolar tahlil qilinadi:

1. Ransomware (garov dasturlar) hujumlari

Ransomware – foydalanuvchining kompyuteriga kirib, undagi muhim fayllarni shifrlab, ularni tiklash evaziga to‘lov talab qiladigan zararli dasturiy vositalardir. Bu hujumlar:

- Tibbiyot muassasalari, universitetlar, korporatsiyalar kabi yirik tashkilotlarni nishonga oladi;
- Ko‘pincha elektron pochta orqali yuboriladigan zararli fayllar orqali tarqatiladi;
- To‘lovlar asosan kriptovalyuta orqali amalga oshiriladi, bu jinoyatchilarni aniqlashni qiyinlashtiradi.

Misol: 2017-yildagi WannaCry hujumi dunyo bo‘ylab yuz minglab kompyuterlarga zarar yetkazgan va katta iqtisodiy yo‘qotishlarga sabab bo‘lgan.

2. Sun’iy intellekt yordamida amalga oshirilayotgan kiberhujumlar

Bugungi texnologik taraqqiyot natijasida sun’iy intellekt (SI) faqat himoya tizimlari emas, balki hujum vositasi sifatida ham qo‘llanilmoqda. Kiberjinoyatchilar SI algoritmlaridan:

- Tarmoqdagi zaif nuqtalarni avtomatik aniqlash;
- Foydalanuvchi xatti-harakatlarini analiz qilib, ijtimoiy muhandislik hujumlarini rejalashtirish;
- Soxta ovozlar (deepfake), chatbotlar va avtomatik xabarlar orqali ishonchli tarzda aldash kabi maqsadlarda foydalanmoqda.

Bu holat kiberhujumlarning tezligini, aniqligini va ko‘lamini sezilarli darajada oshiradi.

3. IoT (Internet of Things) qurilmalari xavfsizligi

Internetga ulangan “aqlli qurilmalar” (IoT) soni millionlab ortmoqda: aqlli televizorlar, kameralar, termostatlar, tibbiy qurilmalar va boshqalar. Ularning asosiy xavfli jihati:

- Ko‘pchiligi standart xavfsizlik protokollarisiz ishlab chiqiladi;
- Foydalanuvchilar parollarni o‘zgartirmasdan standart sozlamalarda ishlatishda davom etadi;

- Kiberjinoyatchilar bunday qurilmalarni botnetga aylantirib, katta DDoS hujumlar uyushtirishi mumkin.

Masalan: 2016-yildagi Mirai botnet hujumi minglab IoT qurilmalari orqali butun bir internet xizmatlarini ishdan chiqargan edi.

Zamonaviy kiberxavfsizlik tahdidlari – endilikda nafaqat texnik muammo, balki ijtimoiy, siyosiy va iqtisodiy tahdidga ham aylangan. Ransomware, sun’iy intellekt vositasidagi hujumlar va IoT qurilmalarning zaifligi global darajadagi xavfsizlik muammosi bo‘lib bormoqda. Bunday vaziyatda xavfsizlikni ta’minlash uchun keng ko‘lamli siyosat, doimiy monitoring va zamonaviy texnologik yechimlar zarur.

11.9. Kiberxavfsizlikda foydalanuvchi madaniyati

Kiberxavfsizlik sohasida texnologik himoya vositalari qanchalik rivojlangan bo‘lmasin, foydalanuvchi xatti-harakatlari bu tizimning eng muhim va zaif bo‘g‘inidir. Bugungi raqamli jamiyatda har bir foydalanuvchi kiberxavfsizlik madaniyatiga ega bo‘lishi zarur. Bu madaniyat — insonning texnologiyalardan foydalanishdagi mas’uliyati, axloqiyati va savodxonligini o‘z ichiga oladi.

1. Kiberxavfsizlik bo‘yicha xabardorlikni oshirish

Aksariyat kiberhujumlar foydalanuvchining oddiy xatolari natijasida sodir bo‘ladi: noaniq havolaga bosish, zaif parol yaratish, noma’lum ilovalarni o‘rnatish. Shuning uchun kiberxavfsizlik bo‘yicha doimiy xabardorlik talab etiladi:

- Xavfli elektron pochta xabarlari va fishing hujumlarini aniqlash;
- Shaxsiy ma’lumotlarni begonalarga bermaslik;
- Qurilmalarni xavfsiz tarzda ishlatish qoidalarini bilish;
- Doimiy ravishda o‘z bilimlarini yangilab borish.

Yevropa Ittifoqi, AQSH va boshqa davlatlar har yili “Kiberxavfsizlik haftaligi” tadbirlarini o‘tkazib, jamoatchilikni ogohlikka chaqiradi.

2. Ta’lim tizimida kiberxavfsizlikni o‘rgatish zarurati

Raqamli texnologiyalar ta’lim tizimining ajralmas qismiga aylangan bir davrda, maktabgacha ta’limdan to oliy o‘quv yurtlarigacha kiberxavfsizlik bo‘yicha dasturlarni joriy etish zarur. Bu orqali:

- Yosh avlodni xavfsiz raqamli muhitda yashashga tayyorlash;
- Internetdagi tahdidlarni tushunish va ulardan himoyalanish ko‘nikmalarini shakllantirish;
- O‘qituvchilarni ham onlayn muhitdagi xavfsizlik qoidalariga o‘rgatish mumkin.

Ta’lim orqali shakllantirilgan madaniyat himoya tizimlaridan ham kuchliroq bo‘lishi mumkin.

3. Kiberetika va onlayn mas’uliyat

Kiberxavfsizlik faqat texnik bilim emas, balki axloqiy va huquqiy mas’uliyat hamdir. Kiberetika — bu raqamli muhitda insonlar o‘rtasidagi madaniyatli muloqot, axloqiy me’yorlar, muomala tamoyillari va samarali hamkorlik tushunchalarini o‘z ichiga oladi. Har bir foydalanuvchi:

- Boshqalarning shaxsiy hayotiga hurmat bilan qarashi;
- Onlayn muhitda tahdid, tuhmat yoki diskriminatsiya qilmasligi;
- Boshqalarning axborot va mulk huquqini buzmasligi;
- Mualliflik huquqini hurmat qilishi lozim.

Kiberetika madaniyati — bu zamonaviy jamiyatda insoniylik, adolat va mas’uliyat tamoyillarini saqlab qolish vositasidir.

Kiberxavfsizlik madaniyati har bir fuqaroning raqamli hayotda o‘zini tutish qoidalarini belgilaydi. Texnologiyalar taraqqiy etar ekan, inson omili har doim markazda qolaveradi. Demak, nafaqat dasturlar, balki insonlarni ham doimiy ravishda axborot xavfsizligiga oid bilimlar bilan qurollantirish lozim. Faqat ana shundagina raqamli xavfsizlikning barqaror poydevori yaratiladi.

Bugungi kunda raqamli texnologiyalar taraqqiyoti bilan insoniyat hayotining deyarli barcha sohalari internet va axborot tizimlariga bog‘lanib bormoqda. Shu bilan birga, bu jarayon o‘zida jiddiy xavf va tahdidlarni ham olib kelmoqda. Ayniqsa, axborot tizimlarining buzilishi, shaxsiy va moliyaviy ma’lumotlarning o‘g‘irlanishi, zararli dasturiy hujumlar, sun’iy intellekt orqali amalga oshirilayotgan manipulyativ harakatlar — bularning barchasi kiberxavfsizlikni jamiyatning eng dolzarb masalalaridan biriga aylantirmoqda. Endilikda kiberxavfsizlik masalasi nafaqat

axborot texnologiyalari sohasiga tegishli muammo, balki har bir fuqaro, ta’lim muassasasi, korxona, davlat tashkiloti va butun jamiyat oldidagi strategik vazifadir.

Kiberxavfsizlikning ustuvorligi shundan iboratki, u nafaqat mavjud ma’lumotlarni himoya qiladi, balki fuqarolarning ishonchini saqlab qoladi, raqamli iqtisodiyot rivojiga xizmat qiladi, davlat boshqaruvi va milliy xavfsizlikni kafolatlaydi. Shu bois, kiberxavfsizlik siyosati global miqyosda strategik darajaga ko‘tarilgan. Zamonaviy kiberxavfsizlik yondashuvi faqat texnik choralar bilan emas, balki foydalanuvchi madaniyatini shakllantirish, huquqiy me’yorlarni belgilash, xalqaro hamkorlikni mustahkamlash orqali amalga oshiriladi.

Ta’lim tizimida kiberxavfsizlikni rivojlantirish esa kelajak avlodni raqamli muhitda ongli va mas’uliyatli ishtirokchiga aylantirish uchun zaruriy shartdir. Maktab va oliy ta’lim dasturlariga raqamli xavfsizlik, shaxsiy ma’lumotlar bilan ishlash madaniyati, internet etikasi kabi mavzularni majburiy tarzda kiritish, o‘quvchilar va talabalar uchun amaliy mashg‘ulotlar va simulyatsiyalarni tashkil qilish — kiberhujumlarning oldini olishdagi samarali vositalardandir.

Shu bilan birga, foydalanuvchilarning o‘zlari ham kuchli parollar ishlatish, antivirus dasturlaridan foydalanish, shubhali havolalarga bosmaslik, axborotlarni zaxiralash kabi oddiy, ammo samarali choralarni bilishi va ularga amal qilishi zarur. Tashkilotlar esa maxsus IT xavfsizlik mutaxassislarini tayyorlash, xalqaro standartlarga mos audit va xavf tahlillarini o‘tkazish orqali tizimli yondashuvni kuchaytirishlari kerak.

Shunday qilib, kiberxavfsizlik – bu faqat texnologiya emas, bu raqamli hayot tarzining ajralmas tamoyilidir. Kiberhujumlar doimiy yangilanib borayotgan bir paytda, bizning himoyamiz ham yangilanib borishi shart. Ustuvor yo‘nalish sifatida kiberxavfsizlikni ta’lim, ishlab chiqarish va boshqaruv tizimlariga chuqur integratsiyalash, keng jamoatchilik ongida raqamli mas’uliyatni shakllantirish va global tahdidlarga qarshi birgalikda harakat qilish — zamonaviy davrning muqarrar talabi bo‘lib qolmoqda.

Uyga vazifa savollari

1. “Kiberxavfsizlik” atamasi qanday shakllangan va uning mohiyati nimadan iborat?

2. Axborot xavfsizligi va kiberxavfsizlik o‘rtasidagi asosiy farqlarni misollar bilan tushuntiring.

3. O‘z hayotingizda duch kelgan (yoki eshitgan) kiberhujum holatini tahlil qiling.

4. Kiberxavfsizlikda “Confidentiality, Integrity, Availability” tamoyillarini real misollar bilan izohlang.

5. Sizningcha, eng xavfli kiberxavf turi qaysi va nima uchun?

6. Kuchli parol yaratish qoidalarini amaliy misollar bilan yozib bering.

7. Internetda shaxsiy ma’lumotlaringizni qanday himoya qilasiz? Strategiyalaringizni yozing.

8. O‘zbekistonda kiberxavfsizlik bo‘yicha qanday qonun va hujjatlar mavjud? Qisqacha tahlil bering.

9. Sun’iy intellekt orqali kiberxavflarni aniqlash va oldini olish usullari haqida tadqiqot qiling.

10. Kiberetika va onlayn madaniyatning foydalanuvchi xavfsizligiga ta’siri haqida fikringizni yozing.

Nazorat savollari

1. Kiberxavfsizlik tushunchasini izohlang. U axborot xavfsizligidan nimasi bilan farq qiladi?

2. Kiberxavfsizlik nima uchun zamonaviy jamiyatda muhim ahamiyat kasb etadi? Hayotiy misollar bilan tushuntiring.

3. Kompyuter viruslari va zararli dasturlar qanday ishlaydi va ulardan qanday himoyalanish mumkin?

4. Phishing hujumlari qanday amalga oshiriladi? Ularning oldini olish uchun qanday choralar ko‘riladi?

5. DDoS hujumi deganda nimani tushunasiz? U qanday tahdid tug‘diradi va unga qarshi qanday texnologiyalar mavjud?

6. Kiberxavfsizlikning uch asosiy tamoyilini (maxfiylik, butunlik, foydalanish imkoniyati) izohlang. Har biriga hayotiy misollar keltiring.

7. VPN texnologiyasi qanday ishlaydi va foydalanuvchilar uchun qanday afzalliklar beradi?

8. Shaxsiy ma’lumotlarni himoya qilish uchun har bir foydalanuvchi qanday kundalik odatlarga amal qilishi kerak?

9. Global darajadagi kiberxavfsizlik qonunlari va standartlari haqida ma’lumot bering (masalan: ISO/IEC 27001, GDPR).

10. Kiberetika nima? Onlayn faoliyatda etik xatti-harakatlar qanday bo‘lishi kerak deb o‘ylaysiz?