# INTERNETDA AXBOROT XAVFSIZLIGI

**Turayev A.K**
Shahrisabz "Temurbeklar maktabi" harbiy-akademik
litseyi informatika va axborot texnologiyalari fani o'qituvchisi
E-mail: AzamTurayev1982@gmail.com

## ANNOTATSIYA

Internetdagi axborotlarga xavf va tahdidlar nimalardan iboratligi, ushbu xavflarni oldini olish uchun texnik yechim va tashkiliy ishlarni amalga oshirish, xavfsizlikni ta'minlash borasida internet foydalanuvchilari orasida o'rnatilmagan tartib qoidalar, resurslaridan foydalanishdan avval foydalanuvchi kompyuter tizimining identifikatsiya va autentifikatsiya o'tish jarayoni.

**Kalit so'zlar:** Axborotni muhofazalash,axborot xavfsizligi, identifikatsiya, autentifikatsiya, ma'murlash, parol, dinamik parol.

Hozirgi kunda internet xalqaro tarmog'i kun sayin rivojlangani sari, undagi axborotlarni muhofazalash va axborotlarni xavfsizligi masalalari dolzarblashib bormoqda.

**Axborotni muhofazalash**–bu ma'lumotlarni o'g'irlash, yo'qotish, soxtalashtirish, qalbakilashtirish, ruxsatsiz foydalanish va ko'paytirishning oldini olishga yo'naltirilgan tadbirlar majmuasidir.

**Axborot xavfsizligi –** foydalanish talablari asosida ma'lumotlarning yashirinligi, yaxlitligi va foydalanuvchanligini ta'minlashdir.

Internet tizimi orqali tarmoqlararo ma'lumot almashinuvini ta'minlash, butun dunyodagi bilimlar manbalariga kirish, qisqa vaqt ichida ko'plab ma'lumotlar yig'ish, ishlab chiqarishning va uning texnik vositalarini masofadan turib boshqarish mumkin. Shu bilan bir qatorda internetning ushbu imkoniyatlaridan foydalanib tarmoqdagi

begona kompyuterlarni boshqarish ularning ma'lumotlar bazasiga kirish, nusxa ko'chirish g'arazli maqsadda turli xil viruslar tarqatish kabi noqonuniy ishlarni amalga oshirsh mumkin. Internetda mavjud bo'lgan ushbu xavf, axborot xavfsizlik muammolari bevosita tarmoqlarning xususiyatlaridan kelib chiqadi. Ixtiyoriy tarmoq xizmatini o'zaro kelishilgan qoida (protokol) asosida ishlovchi juftlik «Server» va «Mijoz» dastur ta'minoti bajaradi. Ushbu protokollar miqyosida ham «Server», ham «Mijoz» dasturlari ruxsat etilgan amallarini (operatsiya) bajarish vositalariga ega. Ruxsat etilgan operatsiyalar, faol ob'ektlardan foydalanib internetda ba'zi bir noqonuniy harakatlarni amalga oshirish tarmoqdagi kompyuterlarga va ma'lumotlar ba'zasiga kirish hamda ularga tahdid solish mumkin bo'ladi. Bu xavf va tahdid nimalardan iborat:

- Tarmoqdagi kompyuterlarga ruxsatsiz kirish va uni masofadan turib boshqarish. Ularga sizning manfaatingizga zid bo'lgan dasturlarni joylashtirish mumkin.
- Web sahifalarida joylashtirilgan «faol ob'ektlar» agressiv dastur kodlari bo'lib, siz uchun xavfli virus yoki josus dastur vazifasini o'tashi mumkin.
- Internetda uzatilayotgan ma'lumotlar yo'l yo'lakay aloqa kanallari yoki tarmoq tugunlarida tutib olinishi ulardan nusxa ko'chirilishi, almashtirilishi mumkin.
- Davlat muassasasi, korxona faoliyati, moliyaviy ahvoli va uning xodimlari haqidagi ma'lumotlarni razvedka qilinishi o'g'irlashi va shu orqali sizning shaxsiy hayotingizga, korxona rivojiga tahdid solishi mumkin.
- Internetda e'lon qilinayotgan har qanday ma'lumot ham jamiyat uchun foydali bo'lmasligi mumkin, ya'ni internet orqali bizning ma'naviyatimizga, madaniyatimizga va e'tiqodimizga zid bo'lgan informatsiyalarni kirib kelishi ehtimoli ham mavjud.

Internet foydalanuvchisi ushbu xavflarni oldini olish uchun quyidagi texnik yechim va tashkiliy ishlarni amalga oshirishi zarur:

- Shaxsiy kompyuterga va mahalliy kompyuter tarmog'iga hamda unda mavjud bo'lgan axborot resurslarga tashqaridan internet orqali kirishni cheklovchi va ushbu jarayonni nazorat qilish imkonini beruvchi texnik va dasturviy usullardan foydalanish.

• Tarmoqdagi axborot muloqot ishtirokchilari va ular kuzatayotgan ma'lumotlarni asl nusxasiga mosligini tekshirish.

• Ma'lumotlarni uzatish va qabul qilishda kriptografiya usullaridan foydalanish

• Viruslarga qarshi nazoratchi va davolovchi dasturlardan foydalanish.

• Shaxsiy kompyuter va mahalliy kompyuter tarmog'iga begona shaxslarni qo'ymaslik va ularda mavjud bo'lgan ma'lumotlardan nusxa olish imkoniyatlarini cheklovchi tashkiliy ishlarni amalga oshirish.

Bundan tashqari axborot xavfsizlikni ta'minlash borasida internet foydalanuvchilari orasida o'rnatilmagan tartib qoidalar mavjud. Ulardan ba'zi birlarini keltiramiz:

Hech qachon hech kimga internetdagi o'z nomingiz va parolingizni aytmang.

Hech qachon hech kimga o'zingiz va oila a'zolaringiz haqidagi shaxsiy hamda ishxonangizga oid ma'lumotlarni internet orqali yubormang.

Elektron manzilingiz (*E-mail*)dan maqsadli foydalaning. Internet orqali dasturlar almashmang.

▪ Internetda tarqatilayotgan duch kelgan dasturlardan foydalanmang. Dasturlarni faqat ishonchli egasi ma'lum bo'lgan serverlardan ko'chiring.

▪ Elektron pochta orqali yuborilgan «aktiv ob'ektlar» va dasturlarni ishlatmang, yoki qo'shimchali o'z-o'zidan ochiluvchi sizga noma'lum arxiv holidagi ma'lumotlarni ochmang.

▪ Elektron pochta xizmatidan foydalanayotganingizda ma'lumotlarni shifrlash zarur, ya'ni kriptografiya usullaridan foydalaning.

▪ Egasi siz uchun noma'lum bo'lgan xatlarni ochmang.

▪ Egasi ma'lum bo'lgan va uning sifatiga kafolat beruvchi antivirus dasturlardan foydalaning va ularni muntazam yangilab boring.

▪ Internetda mavjud bo'lgan axborot resurslar va dasturlardan ularning mualliflari ruxsatisiz foydalanmang.

▪ Tarmoqdagi begona kompyuter va serverlarning IP manzillarini aniqlash va shu orqali ruxsat etilmagan serverlar va axborot resurslarga kirish nusxa ko'chirish,

viruslar tarqatish kabi noqonuniy dasturlashtirish ishlari bilan shug‘ullanmang, bu jinoyatdir.

Internet bilan ishlaganda tizimning ixtiyoriy qismidan unga kirish imkoniyati mavjud bo‘ladi. Shu sababli, axborot xavfsizligini ta’minlash uchun foydalanuvchilarni identifikatsiyalash, autentifikatsiyalash va autorizatsiyalash zarur bo‘ladi.

Kompyuter tizimida ro‘yxatga olingan har bir sub’ekt (foydalanuvchi yoki foydalanuvchi nomidan harakatlanuvchi jarayon) bilan uni bir ma’noda indentifikatsiyalovchi axborot bog‘liq.

Bu ushbu sub’ektga nom beruvchi son yoki simvollar satri bo‘lishi mumkin. Bu axborot sub’ekt indentifikatori deb yuritiladi. Agar foydalanuvchi tarmoqda ro‘yxatga olingan indentifikatorga ega bo‘lsa u legal (qonuniy), aks holda legal bo‘lmagan (noqonuniy) foydalanuvchi hisoblanadi. Kompyuter resurslaridan foydalanishdan avval foydalanuvchi kompyuter tizimining identifikatsiya va autentifikatsiya jarayonidan o‘tishi lozim.

**Identifikatsiya (Identification)** - foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni. Bu foydalanuvchi tarmoqdan foydalanishga uringanida birinchi galda bajariladigan funktsiyadir. Foydalanuvchi tizimga uning so‘rovi bo‘yicha o‘zining identifikatorini bildiradi, tizim esa o‘zining ma’lumotlar bazasida uning borligini tekshiradi.

**Autentifikatsiya (Authentication)** — ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi. Bu tekshirish foydalanuvchi (jarayon yoki qurilma) haqiqatan aynan o‘zi ekanligiga ishonch xosil qilishiga imkon beradi. Autentifikatsiya o‘tqazishda tekshiruvchi taraf tekshiriluvchi tarafning xaqiqiy ekanligiga ishonch hosil qilishi bilan bir qatorda tekshiriluvchi taraf ham axborot almashinuv jarayonida faol qatnashadi. Odatda foydalanuvchi tizimga o‘z xususidagi noyob, boshqalarga ma’lum bo‘lmagan axborotni (masalan, parol yoki sertifikat) kiritishi orqali identifikatsiyani tasdiqlaydi.

Identifikatsiya va autentifikatsiya sub’ektlarning (foydalanuvchilarning) haqiqiy

ekanligini aniqlash va tekshirishning o‘zaro bog‘langan jarayonidir. Muayyan foydalanuvchi yoki jarayonning tizim resurslaridan foydalanishiga tizimning ruxsati aynan shularga bog‘liq. Sub’ektni identifikatsiyalash va autentifikatsiyalashdan so‘ng uni avtorizatsiyalash boshlanadi.

**Avtorizatsiya (Authorization)** — subektga tizimda ma’lum vakolat va resurslarni berish muolajasi, ya’ni avtorizatsiya sub’ekt harakati doirasini va u foydalanadigan resurslarni belgilaydi. Agar tizim avtorizatsiyalangan shaxsni avtorizatsiyalanmagan shaxsdan ishonchli ajrata olmasa bu tizimda axborotning konfidentsialligi va yaxlitligi buzilishi mumkin. Autentifikatsiya va avtorizatsiya muolajalari bilan foydalanuvchi harakatini ma’murlash muolajasi uzviy bog‘langan.

**Ma’murlash (Accounting)** — foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish. Ushbu hisobot axboroti xavfsizlik nuqtai nazaridan tarmoqdagi xavfsizlik xodisalarini oshkor qilish, tahlillash va ularga mos reaktsiya ko‘rsatish uchun juda muhimdir.

Ma’lumotlarni uzatish kanallarini himoyalashda sub’ektlarning o‘zaro autentifikatsiyasi, ya’ni aloqa kanallari orqali bog‘lanadigan sub’ektlar xaqiqiyligining o‘zaro tasdig‘i bajarilishi shart. Xaqiqiylikning tasdig‘i odatda seans boshida, abonentlarning bir-biriga ulanish jarayonida amalga oshiriladi. “Ulash” atamasi orqali tarmoqning ikkita sub’ekti o‘rtasida mantiqiy bog‘lanish tushuniladi. Ushbu muolajaning maqsadi — ulash qonuniy sub’ekt bilan amalga oshirilganligiga va barcha axborot mo‘ljallangan manzilga borishligiga ishonchni ta’minlashdir.

O‘zining xaqiqiyligining tasdiqlash uchun sub’ekt tizimga turli asoslarni ko‘rsatishi mumkin. Sub’ekt ko‘rsatadigan asoslarga bog‘liq holda autentifikatsiya jarayonlari quyidagi kategoriyalarga bo‘linishi mumkin:

**biror narsani bilish asosida**. Misol sifatida parol, shaxsiy identifikatsiya kodi PIN (Personal Identification Number) hamda “so‘rov javob” xilidagi protokollarda namoyish etiluvchi maxfiy va ochiq kalitlarni ko‘rsatish mumkin;

**biror narsaga egaligi asosida**. Odatda bular magnit kartalar, smart-kartalar, sertifikatlar va touch memory qurilmalari;

**qandaydir daxlsiz xarakteristikalar asosida.** Ushbu kategoriya o‘z tarkibiga foydalanuvchining biometrik xarakteristikalariga (ovozlar, ko‘zining rangdor pardasi va to‘r pardasi, barmoq izlari, kaft geometriyasi va x.) asoslangan usullarni oladi. Bu kategoriyada kriptografik usullar va vositalar ishlatilmaydi. Beometrik xarakteristikalar binodan yoki qandaydir texnikadan foydalanishni nazoratlashda ishlatiladi.

**Parol** — foydalanuvchi hamda uning axborot almashinuvidagi sherigi biladigan narsa. O‘zaro autentifikatsiya uchun foydalanuvchi va uning sherigi o‘rtasida parol almashinishi mumkin. Plastik karta va smart-karta egasini autentifikatsiyasida shaxsiy identifikatsiya nomeri PIN sinalgan usul hisoblanadi. PIN — kodning mahfiy qiymati faqat karta egasiga ma’lum bo‘lishi shart.

**Dinamik — (bir martalik) parol** - bir marta ishlatilganidan so‘ng boshqa umuman ishlatilmaydigan parol. Amalda odatda doimiy parolga yoki tayanch iboraga asoslanuvchi muntazam o‘zgarib turuvchi qiymat ishlatiladi.

Ikkala tarafga bitta sir ma’lum bo‘lgani sababli, birinchi taraf ikkinchi taraf javobini to‘g‘riligini tekshirishi mumkin.

**FOYDALANILGAN ADABIYOTLAR RO‘YXATI: (REFERENCES)**

1. Tayloqov Norbek Isaqulovich, Axmedov Akrom Burxonovich Informatika va axborot texnologiylari O‘rta ta’lim muassasalarining 11-sinflari va o‘rta maxsus, kasb-hunar ta’limi muassasalari o‘quvchilari uchun darslik.

2. G‘aniyev Salim Karimovich, Karimov Majid Malikovich, Tashev Komil Axmatovich “Axborot xavfsizligi”.

3. www.tami.uz , www.uzbekdevs.uz