# 57-dars. TARMOQ XAVFSIZLIGI VA AXBOROTNI XAVFSIZLANTIRISH DASTURLARI

**1. Tarmoq xavfsizligi deganda nimani tushunasiz?**

**2. Tarmoq foydalanuvchilari uchun qanday xavflar mavjud deb hisoblaysiz?**

Hozirda ko'plab qurilmalar uchun simli, simsiz yoki mobil tarmoqlar orqali aloqa o'rnatish imkoniyatlari yo'lga qo'yilgan. Foydalanuvchi o'z shaxsiy kompyuteri vositasida lokal va mintaqaviy tarmoqlar hamda Internet yordamida butunjahon hamjamiyati bilan aloqa qilish, ma'lumotlar uzatish, qabul qilish, saqlash, tovar sotish va sotib olish, to'lovlarni amalga oshirish, pul o'tkazish, boshqa shaxslar bilan muloqot qilish kabi imkoniyatlardan foydalana oladi.

**TAYANCH TUSHUNCHALAR**

**Tarmoq xavfsizligi** – tarmoq va unga ulangan qurilmalarga ruxsatsiz kirish, odatiy faoliyatga tasodifan yoki qasddan aralashish yoki o'zgartirish, uning tarkibiy qismlarini yo'q qilishga urinishdan himoya qilish usul va vositalari.

**Tarmoqqa ruxsatsiz kirish** – boshqa foydalanuvchi ma'lumotlari yordamida yoki turli noqonuniy usullardan foydalangan holda tarmoqqa kirish huquqini qo'lga kiritish.

Afsuski, so'nggi vaqtlarda tarmoqlar orqali ko'plab kompyuter jinoyatlari sodir etilmoqda. Jumladan, tajovuzkor virtual tengdoshlar yoki begona shaxslar tomonidan akkauntlarni buzib kirish, shaxsiy ma'lumotlarni o'g'irlash va ulardan g'arazli maqsadlarda foydalanishga urinishlar ko'plab kuzatilmoqda. Bunday hujumlarning oldini olish uchun ham tarmoqlarda axborot xavfsizligini ta'minlash lozim.

Tarmoq xavfsizligi axborot tarmog'idan ruxsatsiz foydalanishdan, faoliyatga tasodifan yoki atayin aralashishdan yoki tarmoq komponentlarini buzishga urinishdan ehtiyot qiluvchi choralar hisoblanadi va u o'z ichiga asbob-uskuna, dasturiy ta'minot hamda ma'lumotlarni himoyalashni oladi.

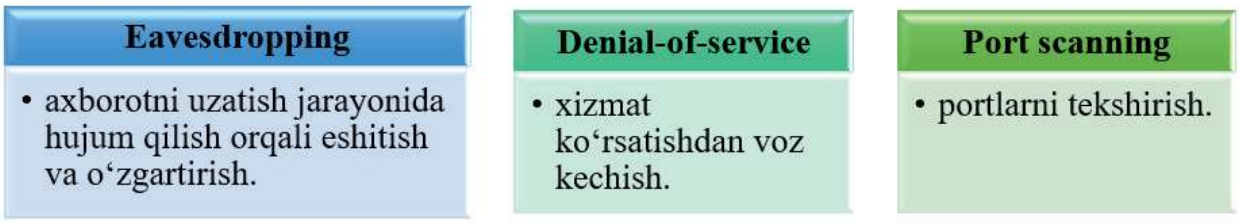
Tarmoq xavfsizligi ko'plab texnologiya, qurilma va jarayonlarni qamrab oladigan keng qamrovli tushunchadir. Oddiy qilib aytganda, tarmoq xavfsizligi dasturiy va apparat texnologiyalaridan foydalangan holda kompyuter tarmoqlari va ma'lumotlar yaxlitligini, maxfiyligi va mavjudligini himoya qilish uchun mo'ljallangan qoida va konfiguratsiyalar to'plamidir.

Tarmoqlardan foydalanish natijasida axborot almashinuv tezligi ortadi, axborotlarni yig'ish, saqlash, qayta ishlash va ulardan foydalanish bo'yicha tezkor natijaga erishiladi. Bunday faoliyat vaqtida tarmoqqa noqonuniy kirish, axborotlardan ruxsatsiz foydalanish, ularni o'zgartirish va yo'qotish kabi tahdidlar oldini olish uchun tarmoq xavfsizligiga e'tibor

qaratish lozim.

Tarmoq xavsizligini ta'minlash maqsadida qo'llaniladigan usul va vositalar xavf-xatarni tez aniqlashi va unga nisbatan qarshi chora ko'rishi zarur.

Tarmoq xavfsizligiga tahdidning turlari ko'p bo'lib, ular bir necha toifalarga bo'linadi:




*Axborotni uzatish jarayonida eshitish va o'zgartirish hujumi* orqali telefon aloqa liniyalari, Internet orqali tezkor xabar almashish, videokonferensiya va faks jo'natmalari orqali amalga oshiriladigan axborot almashinuvida foydalanuvchilarga sezdirmagan holda axborotni tinglash, o'zgartirish va to'sib qo'yish mumkin.

*Xizmat ko'rsatishdan voz kechish hujumini* amalga oshirishdan avval obyektning tarmoq hujumlariga qarshi qo'llanilgan himoya vositalari to'liq o'rganilib chiqiladi va tekshiruv natijalariga asoslanib, maxsus dastur yoziladi. Yaratilgan dastur serverlarga, serverlar esa o'z bazasidagi ro'yxatdan o'tgan minglab, hatto millionlab foydalanuvchilarga yuboradi va ular dasturni o'rnatadi. Dastur belgilangan vaqtda barcha kompyuterlarda faollashadi va to'xtovsiz ravishda hujum qilinishi mo'ljallangan obyektning serveriga so'rovlar yuboradi. Server tinimsiz kelayotgan so'rovlarga javob berish bilan ovora bo'lib, asosiy ish faoliyatini yurita olmaydi. Natijada, server xizmat qilishdan voz kechishga majbur bo'ladi.

*Portlarni tekshirish hujumi*, odatda, tarmoq xizmatini ko'rsatuvchi kompyuterlarga nisbatan ko'p qo'llanadi. Tarmoq xavfsizligini ta'minlash uchun ko'proq virtual portlarga e'tibor qaratish lozim. Chunki portlar ma'lumotlarni kanal orqali tashuvchi vosita hisoblanadi.

Tarmoq xavfsizligi mijozlarning ma'lumot va axborotlarini himoya qilish, ular umumiy xavfsizligini ta'minlash, tarmoqqa ishonchli kirish hamda ishlashni ta'minlash, shuningdek, kiber tahdidlardan himoya qilish uchun muhim ahamiyatga ega. Tarmoq orqali ma'lumot almashish davomida yuborilayotgan axborotni eshitish va o'zgartirishga qarshi samarali natija beruvchi bir nechta texnologiyalar mavjud: IPSec (ingl. *Internet protocol security*) protokoli; VPN (ingl. *Virtual Private Network*) – virtual xususiy tarmoq; IDS (ingl. *Intrusion Detection System*) –ruxsatsiz kirishlarni aniqlash tizimi.

Demak, tarmoq xavfsizligini ta'minlashda foydalanish mumkin bo'lgan texnologiyalar bilan tanishib chiqamiz.

**Xavfsizlik devori** (ingl. *Brandmauer yoki Firewall*) – tarmoq trafigini bloklash va filtrlash uchun mo'ljallangan tarmoqqa kirishni boshqaruvchi qurilma yoki dasturiy ta'minot. Xavfsizlik

devori kompyuter va unga kiradigan ma'lumotlar o'rtasida to'siq yaratadi. Bu turdagi dasturlar orqali qaysi dastur yoki funksiyalar Internet bilan bog'lana olishini, shaxsiy ma'lumotlarni ruxsatsiz uzatmasligini ta'minlash mumkin. Xavfsizlik devoridan foydalanishning asosiy maqsadi axborotni tajovuzkorlardan himoya qilish va trafikni filtrlashdan iborat.

**Virtual xususiy tarmoq** (ingl. *Virtual Private Network*) – qurilma va Internet o'rtasidagi xavfsiz tunnel. VPN onlayn kuzatuv, aralashuv va turli taqiqlardan himoya qiladi. VPN ommaviy tarmoq doirasida ma'lumotlarni uzatish va olish uchun xususiy tarmoqni aniqlash va ulardan foydalanish imkonini beradi. VPNda ishlaydigan ilovalar xavfsiz tarzda himoyalangan. VPN ichki tarmoqqa masofadan ulanish imkonini beradi. VPN kanali orqali o'tayotgan barcha ma'lumotlar shifrlangan holatda bo'ladi. Demak, bunda kimdir ushbu tarmoqqa ulanib olsa ham, oqib o'tayotgan ma'lumotlardan foydalana olmaydi.

**Antivirus dasturlari** Internetga ulangan qurilmaga o'rnatiladi va tarmoqdagi barcha ma'lumotlarni Internetda skanerlaydi. Ular zararli dasturlarni tanib olish va zararsizlantirish uchun mo'ljallangan. Kompyuter ishlayotgan vaqtda skanerlash uzluksiz amalga oshiriladi va uni foydalanuvchi xohishiga ko'ra ishga tushirish mumkin. Antivirus dasturlari nafaqat zararli dasturlarni aniqlay oladi va uning ma'lumotlarga kirishini bloklaydi, balki virus kompyuterga kirib olgan bo'lsa ham, zararlangan fayllarni tiklaydi.

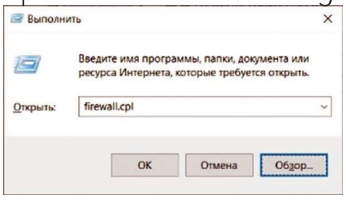
**Autentifikatsiya** shaxsiy ma'lumotlarni ruxsatsiz kirishdan himoya qiladi. Kompyuter, smartfon yoki planshet uchun autentifikatsiyani o'rnatish, ya'ni qurilma qayta ishga tushirilganda har gal login va parol kiritilishini talab qilish orqali ularni himoya qilish mumkin.

Tarmoq xavfsizligini ta'minlash va unga amal qilish bugun hammamiz uchun har qachongidan ko'ra dolzarb masaladir. Odatda, ruxsat etilmagan tarmoq, veb-sayt, foydalanuvchi hisob-qaydlari yoki xizmatlarga kirish nogonuniy hisoblanadi.

| TOPSHIRIQLAR |
|---|
| **1-topshiriq.** ESET Internet Security dasturining xavfsizlik imkoniyatlarini o'rganish. |

| | Imkoniyatlar |
|---|---|
| Internet himoyasi | |
| Tarmoq himoyasi | |
| Xavfsizlik vositalari | |

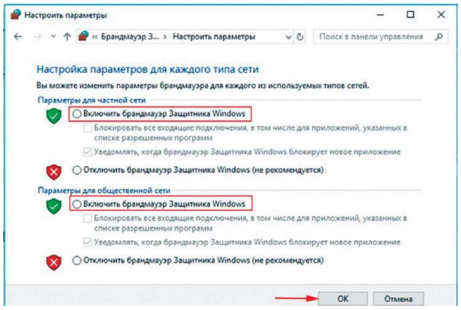
1. ESET Internet Security dasturini ishga tushiring;
2. "Настройка" bandini tanlang va quyidagi jadvalni to'ldiring:




3. Kompyuterni spam va fishingdan himoyalash funksiyalarini faollashtiring.

**2-topshiriq.** Windows 10 OTda xavfsizlik devorini sozlash.

1. Klaviaturadan "Пуск" + R" tugmachalar majmuasini bosing, ochilgan oynaga *firewall.cpl* buyrug'ini yozing va OK tugmachasini bosing.
2. "Брандмауэр Защитника Windows" oynasidagi "Включение и отключение брандмауэр Защитника Windows" havolasini tanlang.
3. Xususiy va umumiy tarmoqlar uchun himoyalovchi xavfsizlik devorini yoqish uchun "Включить брандмауэр Защитника Windows" parametrini faollashtiring va OK tugmachasini bosing.




## SAVOL VA TOPSHIRIQLAR

1. Tarmoqqa ruxsatsiz kirish nima?
2. Tarmoq xavfsizligiga tahdidlarning qanday turlari mavjud?
3. FireWall va VPN nima uchun qo'llaniladi?
4. Axborotlar xavfsizligini ta'minlash uchun qanday dasturlardan foydalanish mumkin?

## UYGA VAZIFA

1. Shaxsiy kompyuteringizda VPN profilini yarating.
2. Tarmoqlarda axborot xavfsizligini ta'minlashga qaratilgan texnologiyalarning afzallik va kamchiliklarini tahlil qiling va jadvalni to'ldiring:

| | Afzalliklari | Kamchiliklari |
|---|---|---|
| **Xavfsizlik devori** | | |
| **Antivirus dasturlari** | | |
| **Arxivlash dasturlari** | | |
| **VPN** | | |