O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

SAMARQAND DAVLAT VETERINARIYA MEDITSINASI, CHORVACHILIK VA BIOTEXNOLOGIYALAR UNIVERSITETI

Axborot texnologiyalari, tabiiy va aniq fanlar kafedrasi o‘qituvchisi

Ravshanov Sanjar Tolibjonovichning

Veterinariya profilaktikasi va davolash ishi fakulteti
Veterinariya meditsinasi yo‘nalishi
1-bosqich 101-guruh talabalari uchun
Sohada axborot kommunikatsiya texnologiyalari fanidan

Axborot xavfsizligi mavzusidagi

AMALIY MASHG‘ULOT ISHLANMASI

Samarqand 2025

Tuzuvchi:
S. Ravshanov - Samarqand davlat veterinariya meditsinasi, chorvachilik va biotexnologiyalar universiteti “Axborot texnologiyalari, tabiiy va aniq fanlar” kafedrasi o‘qituvchisi.

Taqrizchilar:
H.O.Akbarov – Samarqand agroinnovatsiyalar va tadqiqotlar instituti, Raqamli texnologiyalar, turizm va gumanitar fanlar kafedrasi dotsenti v.v.b PhD

X.Urdushev – Samarqand davlat veterinariya meditsinasi, chorvachilik va biotexnologiyalar universiteti. “Axborot texnologiyalari, tabiiy va aniq fanlar” kafedrasi dotsenti.

Axborot xavfsizligi mavzusidagi
Amaliy mashg`ulotining texnologik xaritasi

Talabalar soni 24	2 soat
Mashg‘ulot shakli	Amaliy mashg‘ulot.
Amaliy mashg‘ulot rejasi	Axborot xavfsizligi Kompyuter virusi va uning turlari Antivirus dasturlari Xavfsizlik devori (brandmauerlar) Kompyuter va tarmoq viruslarini xususiyatlari Antivirus va brandmauerni kompyuterga o‘rnatish Mavzu bo‘yicha vazifalar bajarish
O‘quv mashg‘ulotining maqsadi	Mavzu bo‘yicha ko‘nikmalarini hosil qilish.
Pedagogik vazifalar:	O‘quv faoliyati natijalari:
- Axborot xavfsizligi haqida tushuncha berish; - Axborotlarni himoyalash usullarini o‘rgatish;	- Axborot xavfsizligi haqida tushunchaga eaga bo‘lish; - Axborotlarni himoyalash usullarini o‘rganib olish;
O‘qitish usullari	namoyish, aqliy hujum, amaliy ish bajarish.
O‘qitish vositalari	Doska, videoproyektor, topshiriqlar, dasturiy ta’minotlar, kompyuterlar.
O‘qitish shakllari	Yakka tartibda va jamoaviy
O‘qitish sharoiti	Kompyuter bilan ta’minlangan auditoriya.
Monitoring va baholash	Kuzatish, og‘zaki baholash, savol- javob, kompyuterda amaliy ish bajarishiga qarab.

10-amaliy mashg‘ulot: Axborot xavfsizligi

Axborot xavfsizligi
Kompyuter virusi va uning turlari
Antivirus dasturlari
Xavfsizlik devori (brandmauerlar)
Kompyuter va tarmoq viruslarini xususiyatlari
Antivirus va brandmauerni kompyuterga o‘rnatish

Axborot xavfsizligi

Axborot xavfsizligi – bu axborotni tahdidlar, hujumlar, ruxsatiz kirish va sizdirish (utechka) yoki zararlanishdan himoya qilish uchun mo‘ljallangan chora-tadbirlar, usullar va texnologiyalar majmui.

Axborot xavfsizligining maqsadi ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash, shuningdek tashkilotning axborot resurslarini himoya qilishdir.

Axborot xavfsizligining asosiy tamoyillariga maxfiylik (ma’lumotlarning faqat vakolatli foydalanuvchilar uchun ochiq bo‘lishini ta’minlash), yaxlitlik (ma’lumotlarning to‘g‘riligi va izchilligini saqlash) va mavjudlik (ma’lumotlardan o‘z vaqtida foydalanishni ta’minlash) kiradi.

Axborot xavfsizligi kiberxavfsizlik, zararli dasturlardan himoya qilish, ma’lumotlarni shifrlash, kirishni boshqarish, xavfsizlik auditi, xodimlar uchun xavfsizlik bo‘yicha treninglar va ma’lumotlarning tahdidlardan himoyalanishini ta’minlashga qaratilgan boshqa choralar kabi turli jihatlarni o‘z ichiga oladi. Axborot xavfsizligining muhim elementi, shuningdek, xavfsizlik siyosatini yaratish va zaifliklar uchun tizimlarni muntazam monitoring qilish va sinovdan o‘tkazishdir.

Kiberhujum – bu xakerlar yoki kiberjinoyatchilarning zarar yetkazish yoki foyda olish maqsadida tizimlar, tarmoqlar, qurilmalar yoki ma’lumotlarning axborot xavfsizligini buzishga qaratilgan zararli harakati.

Kompyuter virusi – bu bir kompyuterdan ikkinchisiga tarqaladigan va kompyuterning ishlashiga xalaqit beradigan kichik dastur. Kompyuter virusi kompyuteringizdagi ma’lumotlarni buzishi yoki o‘chirishi, uni elektron pochta dasturi orqali boshqa kompyuterlarga tarqatishi yoki hatto qattiq diskingizdagi barcha ma’lumotlarni o‘chirib tashlashi mumkin. Kompyuter viruslari ko‘pincha elektron pochta yoki tezkor xabarlarda qo‘shimchalar sifatida tarqatiladi.

Kompyuter virusi va uning turlari

Kompyuter virusi – bu o‘zini nusxalashi va bir kompyuterdan ikkinchisiga tarqalishi, tizim va foydalanuvchi ma’lumotlariga zarar yetkazishi mumkin bo‘lgan zararli dastur. Viruslar shaxsiy ma’lumotlarni o‘g‘irlash, ma’lumotlarni yo‘q qilish, kompyuterni bloklash, josuslik va boshqa shu kabi ishlar uchun mo‘ljallangan bo‘lishi

mumkin. Viruslar zararlangan fayllar, operatsion tizim zaifliklari, zararli veb-saytlar, elektron pochta xabarlari va boshqa usullar orqali uzatilishi mumkin. Antivirus dasturlarini o‘rnatish va tizimni muntazam skanerlash kompyuteringizni viruslar va boshqa zararli dasturlardan himoya qilishga yordam beradi.

Kompyuter viruslarining turlari va ularning asosiy zararli funksiyalari:

• **Troyan oti** – maxfiy ma’lumotlarni, shu jumladan parollar va bank hisoblarini o‘g‘irlashi yoki tajovuzkorga kompyuterga masofadan kirish huquqini berishi mumkin.

• **Rutkit (Rootkit)** – o‘z faoliyatini antivirus dasturlaridan yashiradi, bu tajovuzkorga kompyuterni boshqarish va aniqlanmasdan noqonuniy faoliyat olib borish imkonini beradi.

• **Spayvar (Spyware)** – shaxsiy ma’lumotlar, ko‘rilgan veb-saytlar va Internet odatlari kabi foydalanuvchilar haqidagi ma’lumotlarni ularning roziligisiz to‘playdi.

• **Ransomvar (Ransomware)** – kompyuteringizdagi fayllarni shifrlaydi va ularning shifrini ochish uchun to‘lovni talab qiladi.

• **Botnet (Botnet)** – kompyuterlardan foydalanib ommaviy **DDoS**-hujumlari uyushtiradi yoki spam-xabarlarni uning egalarining xabarisiz va roziligisiz uzatishni amalga oshiradi.

• **Virus (ViruC)** – kompyuterda o‘z-o‘zini ko‘paytiradi va boshqa fayllarga oson yuqadi, turli nosozliklarni, fayllarni o‘chirishga qadar turli xil muammolarni keltirib chiqaradi.

• **Worm** (Chuvalchang) – o‘z-o‘zidan tarqaladigan chuvalchang foydalanuvchi aralashuvisiz tarmoq orqali tarqaladi, boshqa qurilmalarga o‘zini yuqtiradi va katta hujumlarni keltirib chiqaradi.

• **Keylogger (Keylogger) –** klaviaturada tugmalarni foydalanuvchi tomondan bosilishini yozib boradi, parollar va akkauntga kirish ma’lumotlari kabi boshqa shaxsiy ma’lumotlarni to‘playdi.

• **Advar (Adware)** – zerikarli foydasiz reklamalarni namoyish etadi, har bir foydalanuvchini klikidan foyda yig‘adi.

• **Phishing Attack** (Fishing hujumi) – soxta veb-saytlar yoki elektron pochta orqali foydalanuvchilarning maxfiy ma’lumotlarini, masalan, parollar va kredit karta ma’lumotlarini qo‘lga kiritish orqali aldashlar amalga oshiriladi.

Antivirus dasturlari

Antivirus dasturi – bu kompyuteringizni viruslar, troyan otlari, josuslarga qarshi dasturlar va boshqa tahdidlar kabi turli xil zararli dasturlardan himoya qilish uchun mo‘ljallangan dastur. Antivirus kompyuteringizdagi fayllar va dasturlarni zararli kodlarni tekshiradi, shubhali yoki zararli narsalarni aniqlaydi va yo‘q qiladi, xakerlik hujumlarining oldini oladi va maxfiy ma’lumotlarni himoya qiladi. Antivirus dasturini

o‘rnatish va muntazam ravishda yangilab turish kompyuteringiz xavfsizligini ta’minlash uchun muhim qadam hisoblanadi.

Antivirus dasturi:

• Antivirus – viruslarni, troyan otlarini, josus dasturlarni va boshqa zararli dasturlarni aniqlaydigan, bloklaydigan va yo‘q qiladigan dasturiy mahsulot.

• Antivirus dasturining asosiy vazifasi kompyuteringizdagi fayllar va dasturlarni zararli kodlarni skanerlash, tahdidlarni aniqlash va ularni zararsizlantirishdir. Antivirus dasturi, shuningdek, yangi viruslarning kompyuteringizga yuqishini oldini oladi yoki zararli dasturlarning tizimga kirishga urinishlarini bloklaydi.

• Antivirus – kompyuteringizga alohida dastur sifatida o‘rnatilishi yoki keng qamrovli antivirus dasturlarining bir qismi sifatida ishlatilishi mumkin.

Internetning reyting va sharhlarida tez-tez tilga olinadigan asosiy antivirus dasturlari:

• **Kaspersky Antivirus,** asosiy funksiyalari: antivirusdan himoya qilish, xakerlik hujumlari va fishingdan himoya qilish, zararli dasturlarni kuzatadi-nazorat qiladi.

• **Bitdefender Antivirus Plus**, asosiy xususiyatlari: kuchli antivirus himoyasi, onlayn tahdidlardan himoya qilish, zararli saytlarni blokirovka qilish.

• **Norton Antivirus,** asosiy funksiyalari: antivirusdan himoya qilish, tahdidlarni aniqlash va yo‘q qilish mexanizmlari, shaxsiy ma’lumotlarni himoya qilish.

• **Norton Antivirus,** asosiy funksiyalari: antivirusdan himoya qilish, tarmoq tahdidlaridan himoya qilish, ishlashni optimallashtirish.

• **Avast Antivirus,** asosiy funksiyalari: antivirus himoya qilish, josuslarga qarshi dastur va reklama qarshi himoya, brandmauer (Xavfsizlik devori).

• **ESET NOD32 Antivirus,** asosiy funsiyalari**:** tez va samarali ishlaydigan antivirus himoyasi, hujumlar va fishingning oldini olish mexanizmlari samararali qo‘llanilishi.

• **Malwarebytes Anti-Malware**, asosiy funksiyalari: zararli dasturlarni, shu jumladan josus operatsion tizimlarni va rutkitlarni aniqlash va olib tashlash.

• **Avira Antivirus**, asosiy funksiyalari: antivirusdan himoya qilish, fishing va onlayn tahdidlardan himoya qilish, tizimni optimallashtirish

• **Trend Micro Antivirus,** asosiy funksiyalari: antivirusdan himoya qilish, xavfli saytlarga kirishni boshqarish, Real vaqtda tahdidlardan himoya qilish.

• **AVG Antivirus,** asosiy funksiyalari: antivirusdan himoya qilish, fishing va onlayn tahdidlardan himoya qilish, tizimni optimallashtirish.

• **Avira Antivirus,** asosiy funksiyalari: kuchli antivirus himoyasi, ishlashni optimallashtirish va shaxsiy ma’lumotlarni himoya qilish uchun yordamchi dasturlar.

Ushbu antivirus dasturlarining har biri o‘ziga xos funksiyalari va xususiyatlariga ega va ma’lum bir dasturni tanlash foydalanuvchi ehtiyojlari va mablag‘iga bog‘liq.

Kompyuter va tarmoq viruslarining xususiyatlari

Kompyuter viruslari – bu shaxsiy kompyuterlarni tizim fayllari yoki dasturlariga kiritish orqali yuqtirishi mumkin bo‘lgan dasturlar. Ular kompyuteringizga zarar yetkazishi, shaxsiy ma’lumotlaringizni o‘g‘irlashi yoki boshqa tizimlarga hujum qilish uchun kompyuteringizdan foydalanishi mumkin.

Tarmoq viruslari – bu tarmoq bo‘ylab tarqaladigan va nafaqat alohida kompyuterni, balki tarmoqdagi barcha qurilmalarga ham yuqishi mumkin bo‘lgan dasturlar. Ular tarmoq protokollari yoki dasturiy ta’minotidagi zaifliklardan foydalanishi va butun tarmoqqa zarar yetkazishi mumkin.

Shunday qilib, kompyuter viruslari alohida kompyuterlarga zarar yetkazadi va tarmoq viruslari tarmoqlar bo‘ylab tarqaladi va bir vaqtning o‘zida bir nechta qurilmalarni zararlaydi.

Demak,

- kompyuter antivirus dasturlari alohida kompyuterda viruslar va zararli dasturlardan himoya qilish uchun mo‘ljallangan. Ular kompyuteringizdagi fayllarni viruslarga tekshiradi, ularni bloklaydi va o‘chiradi va real vaqtda yangi tahdidlardan himoya qiladi.
- tarmoq antivirus dasturlari, o‘z navbatida, tarmoqlarni va ularga ulangan barcha qurilmalarni himoya qilish uchun mo‘ljallangan. Ular tarmoq trafigini skanerlashi, zararli dasturlarni aniqlashi va bloklashi hamda butun tarmoq bo‘ylab tarqalishi mumkin bo‘lgan tahdidlardan himoya qilishi mumkin.

Shunday qilib, kompyuter va tarmoq antivirus dasturlari viruslardan himoya qilish vazifasini bajarsa-da, ularning funksionalligi va ko‘lami bitta kompyuterda yoki butun tarmoqdagi tahdidlardan himoya qilish ehtiyojlariga qarab farqlanadi.

Masalan, **Total 360 Security** - antivirus va brandmaueri, zararli dasturlarga qarshi himoya, ishlashni optimallashtirish va boshqa ko‘plab xususiyatlarni o‘z ichiga olgan keng qamrovli antivirus va xavfsizlik vositasi. **Total 360 Security** kompyuteringiz yoki mobil qurilmangizni viruslar, xakerlar, josuslarga qarshi dasturlar va boshqa tahdidlardan har tomonlama himoya qilish uchun mo‘ljallangan.

Xavfsizlik devori (brandmauerlar)

Brandmauer (“firewall”-ingliz tili, “xavfsizlik devori”).

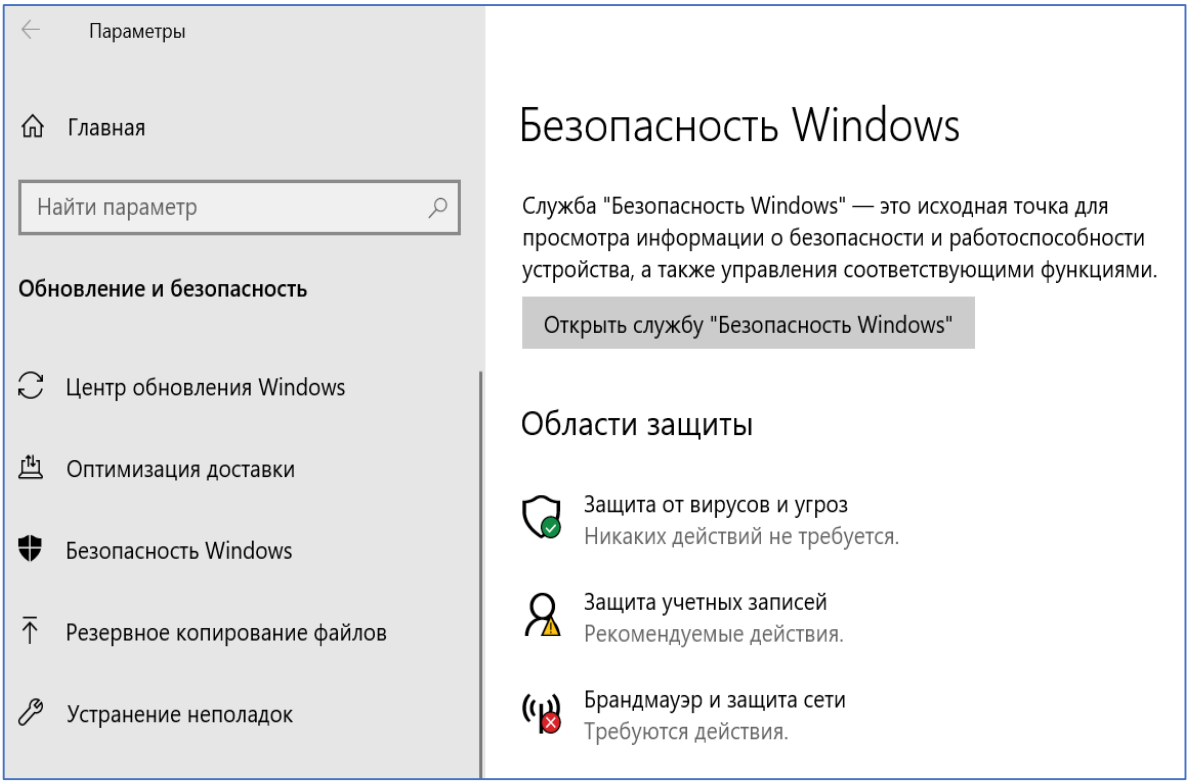
Brandmauer (xavfsizlik devori) – bu kompyuter tarmoqlarini ruxsatiz kirish, tarmoq trafigini boshqarish va filtrlashdan himoya qilish uchun mo‘ljallangan dasturiy va apparat vositasi. Brandmauer ichki tarmoq va tashqi tarmoqlar (masalan, Internet) o‘rtasida to‘siq yaratib, qanday ma’lumotlarni yuborish va qabul qilish mumkinligini aniqlaydi. Brandmauer, shuningdek, ba’zi portlarni yoki xizmatlarni blokirovka qilishi va tarmoqdagi hujumlarni aniqlashi va oldini olishi mumkin.

"Brandmauer" so‘zi kompyuter tarmog‘ini yoki tarmoq qurilmasini ruxsatiz kirish, hujumlar va zararli dasturlardan himoya qiluvchi tizimni anglatadi. Brandmauer – bu tarmoqdagi kiruvchi va chiquvchi trafikni tahlil qiladigan va filtrlaydigan, qaysi ma’lumotlar o‘tishi va qaysi biri bloklanishi kerakligini aniqlaydigan dasturiy ta’minot yoki apparat qurilmasi. Brandmauer, shuningdek, tarmoq resurslariga kirishni boshqarishni ta’minlaydi va xakerlardan himoya qiladi.

Masalan, **Windows 10** operatsion tizimida **Windows Defender Firewall** deb nomlangan o‘rnatilgan brandmauer mavjud. Ushbu brandmauer kompyuteringiz ichida ham, tashqarisida ham yo‘naltirilgan trafikni kuzatish va boshqarish orqali kompyuteringizni kiruvchi tarmoq ulanishlaridan himoya qiladi. **Windows Defender Firewall** brandmaueri tarmoq va dasturga kirish qoidalarini sozlash, tarmoq trafigining ayrim xavfli turlarini blokirovka qilish yoki ruxsat berish, tarmoq faoliyatini kuzatish va tekshirish imkonini beruvchi funksiyalarga ega.

Foydalanuvchi **Windows Defender Firewall** brandmauerni boshqarish paneli yoki Windows xavfsizlik sozlamalari orqali boshqarishi mumkin. U yerda siz maxsus dasturlar, portlar va protokollar uchun brandmauer qoidalarini sozlashingiz, shuningdek kompyuteringiz ishlaydigan tarmoq profillarini boshqarishingiz mumkin (shaxsiy, umumiy yoki ish tarmog‘i).

Masalan, **Windows 10** himoyasini ko‘rish uchun **Пуск–Параметры–**



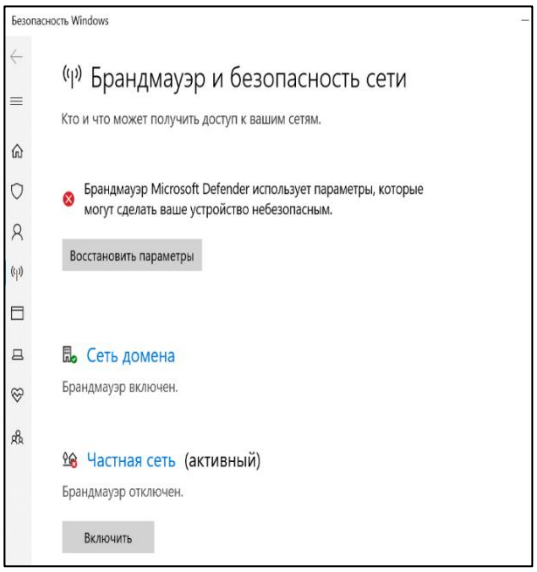
10.1.1- rasm.

(Система)–Обновление и безопасность–Безпастность Windows faollashtiriladi. Natijada **Windows** oynasi 10.1.1-rasmda keltirilgan ko‘rishni oladi. **Безпастность**

Windows (Windows xavfsizligi) oynasida **Защита от вирусов и угроз** (Viruslar va tahdidlardan himoya), **Защита учетных записей** (Hisobga olish qaydlarini himoyasi), **Брандмауэр и защита сети** (Brandmauer va tarmoq himoyasi) vkladkalar o‘rnatilgan. **Masalan, Брандмауэр и защита сети** faollashtirilsa **Брандмауэр и безопастность сети** oynasi ochilib tegishli sozlamalar o‘rnatiladi.

Windows 10 operatsion tizimiga o‘rnatilishi mumkin bo‘lgan ba’zi ommabop xavfsizlik devorlari:

1) Comodo Firewall,
2) ZoneAlarm Free Firewall (Brandmauer),
3) TinyWall,
4) GlassWire,
5) Avast Free Antivirus (Bepul antiviruD),
6) AVG Internet Security (Internet xavfsizligi),
7) FortKnox Personal Firewall (Brandmauer).



10.1.2- rasm.

Bu brandmauerlarning har biri o‘ziga xos xususiyatlar va funksionallikka ega, shuning uchun ularni kompyuterga o‘rnatishdan oldin ularni batafsil o‘rganish va qaror qabul qilish muhimdir.

Shunday qilib, brandmauer tarmoq trafigini kuzatish orqali kompyuteringiz tarmog‘ini tashqi tahdidlardan himoya qiladi, antivirus esa skanerlash va o‘chirish orqali kompyuteringizni zararli dasturlardan himoya qiladi. Kompyuteringizni har tomonlama himoya qilish uchun odatda brandmauer (xavfsizlik devori) va antivirusdan foydalanish tavsiya yetiladi.

Antivirus va brandmauer o‘rtasida...

Brandmauer va antivirus – bu sizning kompyuteringiz xavfsizligini ta’minlash uchun mo‘ljallangan, ammo turli funksiyalarni bajaradigan va turli xil himoya usullariga ega bo‘lgan ikki xil dastur.

- Brandmauer – bu Internet kabi tashqi manbalardan kompyuteringizga yoki tarmoqqa kirishni boshqaradigan va cheklaydigan dastur.
- Brandmauerning asosiy vazifasi tarmoq trafigini boshqarish va filtrlashdir. U qaysi ilovalar yoki xizmatlar kompyuteringiz bilan aloqa o‘rnatishi mumkinligini aniqlaydi, shubhali ulanishlarni bloklaydi va tarmog‘ingizni ruxsatiz kirish va hujumlardan himoya qiladi.
- Brandmauer operatsion tizimga o‘rnatilishi, alohida qurilma (brandmauer) sifatida mavjud bo‘lishi yoki kompyuterga dasturiy ta’minot sifatida o‘rnatilishi mumkin.

Demak, **Windows Defender Firewall** (Windows xavfsizlik devori, brandmauer)ni **Microsoft Defender Antivirus** antivirus dasturi bilan aralashtirib yubormaslik kerak. Ularning nomlari o‘xshash bo‘lsa-da, ular turli funksiyalarni bajaradilar.

Windows Defender Firewall (Windows xavfsizlik devori) kompyuteringizni Internetga ruxsatsiz kirishdan himoya qiluvchi dasturdir. U Windows operatsion tizimlariga o'rnatilgan.

Windows Defender Firewall xavfsizlik devorining asosiy vazifasi kompyuteringizdagi kiruvchi va chiquvchi tarmoq ulanishlarini kuzatish va belgilangan xavfsizlik qoidalariga muvofiq ularga ruxsat berish yoki blokirovka qilishdir. Bu sizning tizimingizga kirishga urinayotgan xakerlar, viruslar va boshqa zararli dasturlarning hujumlarini oldini olishga yordam beradi. **Windows Defender Firewall** xavfsizlik devori **Windows** operatsion tizimining muhim xavfsizlik komponentlaridan biri bo'lib, foydalanuvchi ma'lumotlari va shaxsiy ma'lumotlarini himoya qilishda asosiy rol o'ynaydi.

Microsoft Defender Antivirus (ilgari Windows Defender Antivirus nomi bilan tanilgan) **Microsoft** tomonidan ishlab chiqilgan antivirus dasturidir. U Windows 10 va Windows 11 operatsion tizimlariga o'rnatilgan va kompyuteringizni turli xil zararli dasturlardan himoya qilish uchun mo'ljallangan.

Antivirus va brandmauerlarni kompyuterga o‘rnatish

Antivirus dasturini o‘rnatish:

1) Antivirus dasturini tanlash: bozorda juda ko‘p turli xil antivirus dasturlari mavjud. O‘rnatishdan oldin sizning ehtiyojlaringiz va mablag‘ingizga to‘g‘ri keladigan dasturni tanlang.
2) Dasturni yuklab oling: siz tanlagan antivirus dasturini ishlab chiqaruvchining rasmiy veb-saytiga o‘ting va o‘rnatish faylini yuklab oling.
3) Boshqa dasturlarni yopish: antivirusni o‘rnatishni boshlashdan oldin kompyuteringizdagi barcha boshqa dasturlarni yoping.
4) O‘rnatishni boshlash: yuklab olingan o‘rnatish fayli bilan amallar bajaring. Ba’zi hollarda administrator huquqlarini tasdiqlashingiz kerak bo‘ladi.
5) Tilni tanlash va o‘rnatish: o‘rnatish darchasida foydalanish tili tanlab, so‘ng o‘rnatish tugmasini bosing. O‘rnatishning barcha bosqichlarini bajarish uchun ekrandagi ko‘rsatmalarga amal qiling.
6) Litsenziya shartnomasi: litsenziya shartnomasini o‘qing va agar rozi bo‘lsangiz, uning shartlarini qabul qiling.
7) O‘rnatish sozlamalari: agar dastur talab qilsa, o‘rnatish parametrlarini sozlang (masalan, o‘rnatish papkasini tanlash, yangilanishlarni sozlash va h.k.).

8) O‘rnatishni yakunlash: o‘rnatish tugagandan so‘ng antivirus dasturini ishga tushiring. Dastur viruslar ma’lumotlar bazalarini avtomatik ravishda yangilashni boshlashi va tizimni dastlabki skanerlashni amalga oshirishi mumkin.

9) Ro‘yxatdan o‘tish va faollashtirish: ba’zi antivirus dasturlari qayd ro‘yxatidan o‘tishni yoki to‘liq ishlash uchun litsenziyani faollashtirishni talab qilishi mumkin. Ushbu jarayonni yakunlash uchun dastur ko‘rsatmalariga amal qiling.

10) Skanerlash parametrlari va jadvalini sozlang: dastur o‘rnatilgach, muntazam skanerlash, skanerlash turlarini tanlash va boshqa sozlamalar uchun dastur parametrlarini sozlang.

Kompyuterni viruslar va boshqa tahdidlardan ishonchli himoya qilish uchun antivirus dasturlarini muntazam yangilab turish lozim.

Brandmauerni kompyuterga o‘rnatish odatda, oddiy protsedura bo‘lib, quyidagi amallarni o‘z ichiga oladi:

1) Kompyuteringiz uchun mos brandmauerni tanlang. Kompyuteringizni zararli dasturlardan va tizimingizga ruxsatiz kirishdan himoya qiladigan pullik va bepul ko‘plab xavfsizlik devorlari mavjud.

2) Brandmauerni o‘rnatish faylini ishlab chiquvchining rasmiy veb-saytidan yuklab oling. Bu soxta yoki zararli dasturlarni o‘rnatmaslik uchun muhimdir.

3) O‘rnatish faylini ishga tushiring va o‘rnatish ustasidagi ko‘rsatmalarga amal qiling. Odatda, siz litsenziya shartnomasini qabul qilishingiz, o‘rnatish yo‘lini tanlashingiz, o‘rnatishni boshlashingiz va jarayon tugashini kutishingiz kerak bo‘ladi.

4) Brandmauerni o‘rnatgandan so‘ng, uni talablaringizga ko‘ra sozlang. Bularga tarmoqqa kirish qoidalarini aniqlash, dasturlar va xizmatlarga ruxsat berish va xavfsizlik darajasini sozlash kiradi.

5) Brandmauer to‘g‘ri ishlayotganligini tekshiring, sinov ma’lumotlari paketlarini yuboring va brandmauer o‘z vazifalarini to‘g‘ri bajarayotganiga ishonch hosil qilish uchun tashqi manbalardan tarmoqqa ulanishga harakat qiling.

6) Brandmauer yangi tahdidlar va zararli dasturlarga qarshi samarali ishlashini ta’minlash uchun uni vaqti-vaqti bilan yangilab boring.

Brandmauer (Xavfsizlik devori) - bu kompyuter tarmog‘i yoki alohida qurilmani ma’lumotlar va resurslarga ruxsatsiz kirishdan, shuningdek zararli dasturlardan va Internetdan hujumlardan himoya qilish uchun xizmat qiluvchi maxsus dasturiy yoki apparat uskunasi.

Brandmauer devori kompyuterda dastur sifatida yoki tarmoqqa ulanadigan mustaqil qurilma sifatida amalga oshirilishi mumkin. U kiruvchi va chiquvchi ma’lumotlar trafigini tahlil qiladi, ularni filtrlaydi va shubhali yoki zararli ma’lumotlar paketlarini bloklaydi.

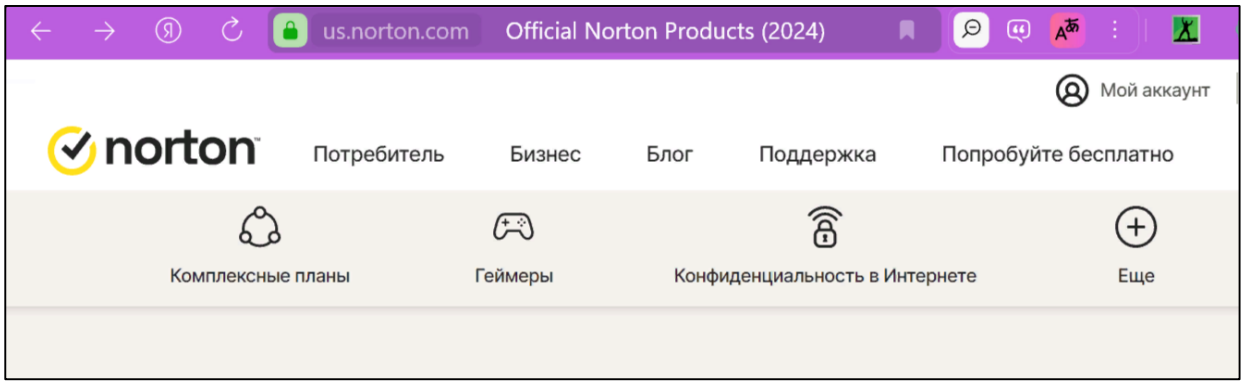
10.1.1-vazifa. Internet qidiruv tizimida “Bepul va pullik antivirus dasturlari” va “Bepul antivirus dasturlarining reytingi” va “Bepul va pullik antiviruslarning farqi nimada?” mavzularida qiliruvni amalga oshiring (10.1.3-rasm.). Qidiruv natijalari asosida Wordda referat tuzing.

10.1.3- rasm.

10.1.2-vazifa. Norton AntiVirusni (https://us.norton.com-Official Site) rasmiy saytiga o‘ting. Antivirus imkoniyatlari bilan tanishing. Saytda akkaunt oching. Saytlar bilan ishlashda “**Google Переводчик**” yoki “**Яндекс Переводчик**” tarjimon dasturlardan foydalaning.

10.1.3-vazifa. https://freesoft.ru/windows/avast - Avast Free Antivirus saytiga o‘ting. Avast antivirus dasturini ishlashini baholang.

10.1.4-vazifa. https://www.drweb.ru/ saytiga o‘ting. dr.web (Doktor Veb) antivirus dasturi imkoniyatlari bilan tanishing.



10.1.4-rasm.

Mavzuni o‘rganish uchun tavsiya etilgan adabiyotlar ro‘yxati va Internet axborot resurslari manzili:

1) Ro‘yxati keltirilgan dasturlardan qaysi biri antivirus dasturi hisoblanadi?
A) Microsoft Word
B) McAfee
C) Google Chrome

D) Adobe Photoshop

2) Ruxsati yo‘q shaxslar tomonidan o‘qilmasligi uchun ma’lumotlarni yashirish jarayoni qanday nomlanadi?

A) Shifrlash

B) Autentifikatsiya

C) Virus

D) Fishing

3) Ikki fAKTorli autentifikatsiya nima?

A) Barmoq izini avtorizatsiya qilish

B) Parol va SMS kod orqali avtorizatsiyalash

C) IP-manzil bo‘yicha avtorizatsiya qilish

D) Ovozli avtorizatsiya

4) Qaysi turdagi dasturiy ta’minot foydalanuvchi tomonidan kiritilgan barcha klavishlarni yozib olishi mumkin?

A) Antivirus dasturi

B) Spyware – zararli(josuC) dastur

C) Firewall -xavfsizlik devori

D) VPN

5) DDoS-ataka-hujumi deganda nima tushuniladi?

A) Uzoqlashgan (masofaviy) serverlarga hujum

B) Kompyuter virusiga hujum

C) Ma’lumotlar bazalari (MB) ga hujum

D) So‘rovlarga talab ko‘payishi (peregruzka zaprosoB) oqibatida serverga hujum

6) Hujumning qaysi turi foydalanuvchini shaxsiy ma’lumotlarini taqdim etishga majbur qiladi?

A) Virus

B) Fishing

C) Skam

D) Troyan

7) Qurilmalarning zaiflik va xavfsizlik xatolarini tekshirish jarayoni qanday nomlanadi?

A) Skanerlash

B) Virus

C) Shifrlash

D) Fishing

8) Ushbu omillardan qaysi biri xakerlar uchun nisbatan zaif hisoblanadi?

A) Murakkab parol

B) Ishonchli xavfsizlik devori

C) Kuchaytirilgan autentifikatsiya

D) Inson omili

9) Brandmauer-xavfsizlik devori qanday vazifani bajaradi?

A) Kompyuterda viruslarni tekshiradi

B) Tarmoqni ruxsatsiz kirishdan himoya qiladi

C) Internet-trafikni shifrlaydi

D) Spamni bloklaydi

10) Keltirilayotganlarning qaysi biri parollarni saqlashni xavfsiz usuli hisoblanadi?

A) Parolni klaviatura ostidagi qog‘ozga saqlash

B) Barcha xizmatlar uchun bir xil paroldan foydalanish

C) Parol menejeridan foydalanish

D) Forumlarda parolni ommaviy joylashtirish

Mavzu bo‘yicha nazorat savollari:

1. Axborot xavfsizligi nima?
2. Axborot xavfsizligiga qanday tahdidlar mavjud?
3. Ma’lumotlarini himoya qilish uchun qanday xavfsizlik choralarini ko‘rish mumkin?
4. Kiberxavfsizlik nima? Tasniflang.
5. Kiber hujumlarning qanday turlari mavjud?
6. Zararli dasturiy ta’minot nima va uni qanday oldini olish mumkin?
7. Wi-Fi jamoat tarmoqlarida foydalanish bilan bog‘liq qanday xavflar yuzaga keladi?
8. Qanday amaliyotlar shaxsiy ma’lumotlarini Internetda himoya qilishga yordam beradi?
9. Axborot xavfsizligini ta’minlash uchun ma’lumotlarni qanday shifrlash usullari qo‘llaniladi?
10. Fishing nima va uning tuzog‘iga tushishni qanday oldini olish mumkin?
11. Kompyuterni viruslar va xakerlik hujumlaridan qanday himoya qilish mumkin?
12. Antiviruslarni qanday himoya qilish vositalari mavjud?
13. Ikki fAKTorli autentifikatsiya nima va u xavfsizlikni qanday ta’minlaydi?
14. Bulutli xizmatlardan foydalanishda qanday xavfsizlik choralarini ko‘rish kerak?
15. Umumiy USB quvvatlovchi (zaryadlovchi) laridan foydalanish bilan bog‘liq qanday xavflar mavjud?
16. Mobil ilovalardan foydalanganda qanday tahdidlar paydo bo‘lishi mumkin?
17. Elektron pochtani spam va fishingdan qanday himoya qilish mumkin?
18. Elektron pochtanni himoya qilish uchun shifrlash qanday usullari qo‘llaniladi?

6. Mavzuni mustahkamlash uchun savollar

1. Axborotlarni himoyalashning dasturiy vositalari?_____
_____
_____
_____
_____

2. Axborotlarni himoyalashni apparat vositalari? _____
_____
_____
_____
_____

3. Axborotlarni kodlash haqida ma’lumot bering_____
_____
_____
_____
_____

4. Kriptografiya. _____
_____
_____
_____
_____

5. Kalit tushunchasi _____
_____
_____
_____

6. Kompyuter virusi? _____
_____
_____
_____
_____

7. Kompyuter virus turlari? _____
_____
_____
_____
_____

8. Axborotni himoyalash usullarini sinflanishi? _____
_____
_____
_____

_____

9. Axborotni ximoyalashning maqsadlari _____
_____
_____
_____
_____

10. Antivirus dasturiy vositalari turlarini _____
_____
_____
_____

Antivirus dasturlari	**Afzalliklari**	**Kamchiliklari**

Adabiyotlar ro‘yxati

Asosiy va qo‘shimcha o‘quv adabiyotlari va hamda axborot manbalari

Asosiy adabiyotlar

1. G‘ulomov S.S., Begalov B.A. Informatika va axborot texnologiyalari. Darslik. T.: “Fan” nashriyoti, 2010 yil.

2. Kenjaboev A.T., Ikramov M.M., Allanazarov A.Sh. Axborot-kommunikatsiya texnologiyalari. – Toshkent; O‘zbekiston faylasuflari milliy jamiyati nashryoti, 2017 yil.

3. Abdullaev Z.S., Mirzaev S.S., Shodmonova G., Shamsiddinov N.B. Informatika va axborot texnologiyalari. – Toshkent: Alisher Navoiy nomidagi O‘zbekiston Milliy kutubxonasi nashryoti. 2012 yil.

4. Zokirova T.A., Xodieva R.M., Shoaxmedova N.X. – Internet texnologiяlari. O‘quv qo‘llanma. – T.: TDIU, 2010 yil.

Xorijiy adabiyotlar

1. Misty E. Vermaat, Susan L. Sebok, Steven M. Freund. Jennifer T. Campbel, Mark Frydenberg. Discovering Computers: Tools, Apps, Devices, and the Impact of Technology (textbook). Cengage Learning. 20 Channel Center Street. Boston, MA 02210. USA, 2016.

2.Elochkin M.V., Branovskiy Ю.S., Nikolaenko I.D. Informaцionnыe texnologii. Uchebnik. M.: Oniks, 2012 god.

Qo‘shimcha adabiyotlar

X.Urdushev, M.Mavlyanov, S.Eshanqulov. Sohada axborot-kommunikatsiya texnologiyalari. II-qism. O‘quv qo‘llanma. – Samarqand: Samarqand davlat veterinariya meditsinasi, chorvachilik va biotexnologiyalar universiteti Nashr matbaa markazi, 2025. 200 b.

X.Urdushev, M.Mavlyanov, S.Eshanqulov. Sohada axborot-kommunikatsiya texnologiyalari. I-qism. O‘quv qo‘llanma. – Samarqand: Samarqand davlat veterinariya meditsinasi, chorvachilik va biotexnologiyalar universiteti Nashr matbaa markazi, 2024. 188 b.

Axborot manbalari:

1) https://library.ziyonet.uz
2) https://unilibrary.uz/
3) https://csec.uz/uz/recomendations/antivirus-ilovalari/
4) https://www.texnoman.uz/
5) Кибербезопасность. Учебник. https://open-source-peace.github.io/w3schoolsrus/cybersecurity/index.html#gsc.tab=0 Кибербезопасность. Учебник. Уроки для начинающих. W3Schools на русском
6) Морева С.Л. Защита информации: практикум /ВШТЭ СПбГУПТД. – СПб., 2020. – 57 с. https://nizrp.narod.ru/metod/kafinfizmtex/1632862450.pdf
7) С чего начать изучение информационной безопасности https://codeby.school/blog/informacionnaya-bezopasnost/s-chego-nachat-izuchenie-informacionnoy-bezopasnosti