55–56-DARSLAR. KOMPYUTER XAVFSIZLIGI VA ANTIVIRUS DASTURLARI

Zamonaviy kompyuter tizimlarining yaratilishi hamda Internet tarmoqlarining paydo bo'lishi axborotlarni himoya qilish muammosining xarakteri va ko'lamini keskin o'zgartirib yubordi.

TAYANCH TUSHUNCHALAR

Kompyuter xavfsizligi – kompyuterdagi ma'lumotlarni tasodifiy yoki qasddan o'chirish, o'zgartirish, zararlash yoki yo'q qilishdan himoyalash.
Zararli dastur – kompyuter tizimi va unda saqlanadigan fayllarga zarar yetkazish yoki buzish uchun mo'ljallangan kompyuter dasturi.

Yuqori ahamiyatga molik maxfiy axborotlardan foydalanish, ularni o'zgartirish, nusxalash kabi amallar jismoniy va yuridik shaxslar vakolatlari bilan aniqlanadi. Axborot o'ta muhim bo'lganligi sababli ular saqlanadigan kompyuter tizimlariga nisbatan salbiy harakatlar sodir etilishi mumkin. Masalan, buzg'unchi o'zini boshqa foydalanuvchi kabi ko'rsatishga intilishi, aloqa kanalini bildirmasdan eshitib olishi yoki tizim foydalanuvchilari o'zaro almashayotgan axborotni ushlab olishi va o'zgartirishi mumkin. Yomon niyatli odamlar maxfiy axborotlarni o'g'irlash, buzish yoki yo'q qilish kabi g'arazli maqsadlarini amalga oshirish uchun zamonaviy kompyuter tizimlari va tarmqlaridan foydalanib kelmoqda. Shunga o'xshash xavflardan himoyalanish uchun oldindan ularning amalga oshirilish yo'llarini aniqlash, so'ngra axborotni himoya qilishga mos tizimni ishga tushirish lozim.

Axborotning ishonchliligi va butunligini ta'minlash maqsadida turli usul va vositalarni ishlatish, choralar ko'rish va tadbirlar o'tkazish orqali kompyuter xavfsizligini ta'minlash mumkin. Kompyuterni zararli dasturlardan himoya qilish muammolari operatsion tizim, dasturlar, shuningdek, kompyuterga o'rnatilgan qurilmalar yordamida hal etiladi.

Axborotlarni muhofaza qilishga bo'lgan asosiy tahdidlaridan biri – kompyuterga "kirib olgan" zararli dasturlardir. Ular ma'lumotlarning yaxlitligiga tahdid solishi mumkin. Zararli dasturlarning eng keng tarqalgan turi – kompyuter viruslari. Kompyuter virusi dastur, hujjat yoki axborot tashuvchi qurilmalarning ma'lum bir qismiga kirib oluvchi parazitar dastur kodi hisoblanadi.

TAYANCH TUSHUNCHALAR

Kompyuter virusi – o'z-o'zidan ko'payuvchi, kompyuter tarmoqlari va axborot tashuvchilari orqali erkin tarqaluvchi hamda kompyuter, unda saqlanayotgan axborot va dasturlarga zarar yetkazuvchi dastur kodi yoki buyruqlar ketma-ketligi.

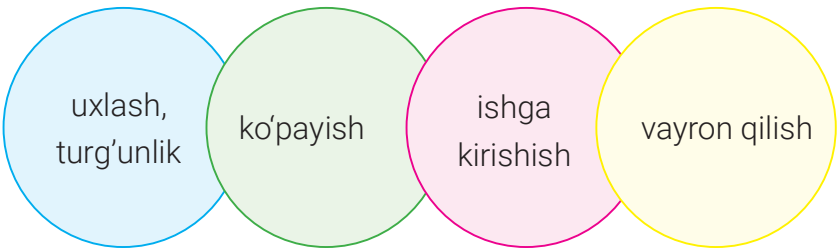
Parazitar dastur kodi kompyuterda turli zararli ishlarni amalga oshiradi. O'zidan nusxa ko'chirish, axborotdan ruxsatsiz foydalanishni amalga oshirish

xususiyati, asosan, virusli dasturlarga xos. Virus, aksariyat hollarda, nosozlik va buzilishlarga sabab bo'ladi. U qandaydir hodisa yuz berishi bilan, masalan, oldindan belgilangan aniq kun (vaqt) kelishi bilan ishga tushishi mumkin. Ko'plab virusli dasturlar ma'lumotlarni yo'q qiladi yoki kompyuterining normal ishlashiga yo'l bermaydi.

Viruslar qayerdan paydo bo'ladi? Ularni malakali darsturchilar o'z g'arazli niyatlarini amalga oshirish, kimdandir o'ch olish, turli tashkilot va korxonalarda raqobat va zararlarni keltirib chiqarish hamda pul ishlash maqsadida "yozadi". Virus "yozuvchi" shaxs ***virmeyker*** deb ataladi.

1-rasm. Zararli dasturlarning kompyuterga kirishi yo'llari

Virusning kompyuterdagi "hayot tarzi", asosan, 4 bosqichda kechadi:



Foydalanuvchi kompyuteridagi Internet yoki tanishlaridan olgan virusli dasturni ishga tushiradi. Bu bosqichda virus dasturi ishlamaydi, faqat foydalanuvchi kompyuteri yoki dasturiy ta'minotiga kirib oladi va hech qanday harakat qilmaydi.

Dasturni yuklashdan oldin yoki keyin virus faollashadi va ko'payishni boshlaydi. Virus o'z nusxalarini boshqa dastur yoki diskdagi ma'lum tizim maydonlariga joylashtiradi. Virus kompyuterga zarar yetkazishi mumkin bo'lgan barcha fayllarni topadi va o'zini faylning boshi yoki oxiriga yozib qo'yadi. Hujum qiladigan belgilangan sana kelganda, virus vayronkorlik harakatlarini amalga oshiradi. Belgilangan sana tugaguncha virus turli kichik-kichik zararlarni amalga oshiradi, masalan, qattiq diskdagi kichik maydonlarni "shifrlashi" mumkin.

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

Kompyuterga zararli dasturlar kirganligining bir qancha belgilari mavjud:

- ekranga ko'zda tutilmagan xabar, tasvirlarni chiqarish hamda ovozli xabarlarning berilishi;
- disk yurituvchilarning o'z-o'zidan ochilib-yopilishi, tez-tez qattiq diskka kirish;
- turli dasturlarning o'z-o'zidan ishga tushirilishi;
- oldin muvaffaqiyatli ishlagan dasturlarning ishlamay qolishi yoki noto'g'ri ishlashi;
- kompyuterning sekin ishlashi;
- operatsion tizimning yuklanmasligi;
- diskdagi fayllar sonining keskin oshib ketishi;
- fayl va kataloglarning yo'qolib qolishi;
- kompyuter ishlash jarayonida tez-tez bo'ladigan "osilib qolish", buzilish va hokazolar.

Internetning rivojlanishi viruslarning tarqalishiga ham kuchli ta'sir ko'rsatdi. Avvallari virmeykerlarning asosiy maqsadi kompyuterni yo'q qilishdan iborat bo'lgan bo'lsa, endi viruslarning asosiy faoliyati kompyuterdan turli ma'lumotlarni o'g'irlash, unga begonalarning kirishiga ruxsat berishga aylandi.

Ma'lumotlarni o'g'irlovchi viruslar kompaniya maxfiy hujjatlarini tarqatish orqali ularga jiddiy zarar yetkazishi mumkin. Bunday viruslar bank, harbiy soha yoki davlat siyosatiga taalluqli maxfiy ma'lumotlar saqlanadigan kompyuterlarga tushsa, nima bo'lishini tasavvur qilishning o'zi qo'rqinchli hol. Masalan, kompyuter viruslari har yili jahon iqtisodiyotiga 1,5 trillion dollar miqdorida moliyaviy zarar yetkazar ekan. Statistik ma'lumotlarga ko'ra, har yili har uchta kompyuterdan bittasi yiliga kamida bir marta virusli hujumlarga uchrar ekan.

BU QIZIQ!

Zararli dastur yaratilgan dastlabki vaqtlarda oddiy foydalanuvchi ishiga xalal beruvchi hazil-viruslar mashhur bo'lgan ekan. Ulardan biri "Bir vaqtning o'zida L + A + M + E + R + F1 + Alt tugmachalar birikmasini bosing" kabi xabarni aks ettiribdi. Foydalanuvchi ko'rsatmaga amal qilishi bilan, fayl joylashuvi jadvali qattiq diskdan o'chirilgani va tezkor xotiraga yozilgani, agar foydalanuvchi barmoqlarini birorta tugmachadan olsa, o'sha zahoti qattiq diskdagi barcha ma'lumotlar bilan "xayrlashishi" mumkinligi, agar shu holatda 1 soat tura olsa, barchasi avvalgi holatiga qaytarilishi haqida xabar chiqqan. Bir soat o'tgach esa buning hazil ekanligi ma'lum bo'lgan.

Zararli dasturlarning turlari ko'p. Ularning ayrimlari bilan tanishib chiqamiz:

Qurtlar (ingl. *Worm*) nomiga mos ravishda juda tez o'z-o'zidan ko'payuvchi viruslardir. Odatda, bunday viruslar Internet yo'li Intranet tarmoqlari orasida tarqaladi. Tarqalish usuli sifatida elektron xat yoki boshqa tez tarqaluvchi mexanizmlardan foydalanadi. Ular kompyuterdagi ma'lumotlarga hamda kompyuter xavfsizligiga katta ziyon yetkazadi. Qurtlar operatsion tizimning nozik joylaridan foydalanish yoki zararlangan elektron xatlarni ochish yo'li bilan kompyuterga o'rnashib olishi mumkin.

Rutkit virusi (ingl. *Rootkit viruses*) – jabrlanuvchi kompyuteriga administrator sifatida kirish huquqini beruvchi kompyuter dasturi. Virusning bu turi eng xavfliligi va yashirinishga mohirligi bilan alohida ajralib turadi. U, odatda, jabrlanuvchi parolining buzilgani sababli o'rnashib oladi. Ba'zi rutkitlarni antivirus dasturlari ham aniqlay olmaydi, chunki ular o'zlarini operatsion tizim fayllari sifatida ko'rsatadi. Rutkitlar, odatda, kompyuterga troyanlar tomonidan o'rnatiladi.

Josus dastur (ingl. *Spyware*), ko'pincha, odamlar harakatini onlayn tarmoq orqali kuzatib borish uchun ishlatiladi. U zararli dasturlarning ko'pchiligini qamrab oladi va foydalanuvchiga bildirmasdan, uning xatti-harakati, xulq-atvori, manzili, paroli, kredit karta tafsilotlari haqidagi ma'lumotlarni to'playdi. Ularni, asosan, ma'lumotlar qiziqtiradi. Josus dasturlarining keng tarqalgan turi ***klaviatura josusidir***. U klaviaturada bosilgan tugmachalarni yozib olish, qurboni haqida shaxsiy ma'lumot to'plash va uni dasturni o'rnatgan kiberjinoyatchiga yetkazish imkonini beruvchi dasturiy ta'minot hisoblanadi.

Zombi (ingl. *Zombie*) kiberjinoyatchiga foydalanuvchi kompyuterini boshqarishga ruxsat beradi. Zombi virusli dastur bo'lib, u Internetga ulangan kompyuterga kirganidan so'ng tashqaridan boshqariladi va kiberjinoyatchilar tomonidan boshqa kompyuterlarga hujum uyushtirish maqsadida ishlatiladi. Foydalanuvchi uning kompyuterini kiberjinoyatchi ishlatayotganini bilmasligi ham mumkin.

Reklamali dastur (ingl. *Adware*) – foydalanuvchiga yo'naltirilgan reklama e'lonlarini namoyish qilish uchun ishlatiladigan dasturiy ta'minot. U foydalanuvchi kirgan veb-saytlarni tahlil qilishi va ularga xuddi shunday mazmundagi reklamalarni yo'naltirishi mumkin. Odatda, reklama dasturlari bepul tarqatiladigan dasturlarga joylashtirilgan. Reklama esa ishchi interfeysda joylashgan. Ko'pincha bu dasturlar foydalanuvchi haqidagi shaxsiy ma'lumotlarni to'playdi va ishlab chiqaruvchiga yuboradi.

Troyan (ingl. *Trojan*) eng xavfli va zararli kompyuter dasturi bo'lib, u zararsiz (masalan,

o'yin yoki yordamchi) dasturlarda yashirinadi. Dastur ishga tushirilgach, virus kabi harakat qila boshlaydi va kompyuterdagi fayllarni yo'q qiladi yoki buzadi. Foydalanuvchi troyan yashiringan eng zararsiz dasturni ishga tushirmaguncha, u hech qanday xavf tug'dirmaydi, uni aniqlab ham bo'lmaydi. Ko'pincha troyan foydalanuvchining shaxsiy ma'lumotlarini o'g'irlash, o'zgartirish yoki o'chirish uchun ishlatiladi. Troyan virusi boshqa dasturlarga o'xshab o'z-o'zidan ko'paymaydi.

Zamonaviy antivirus dasturlari turli virusli dasturlarni aniqlash, zararsizlantirish va foydalanuvchi kompyuterini ishonchli himoya qilish uchun zarur funksiyaga ega.

Virus hujumining oldini olishning eng samarali yo'li muhim ma'lumotlarni zaxiralashdir. Virusli hujum belgilari aniqlanganda, kompyuter muhitini to'liq tozalash kerak. Ma'lumotni zaxira muhitidan uzatish kompyuter tizimining normal holatini tiklash imkonini beradi.

Kompyuter viruslaridan himoyalanishni 3 bosqichda tashkil etish mumkin:

1-bosqichda	viruslarning kompyuterga kirishi oldini olish;
2-bosqichda	virusli hujumlarning oldini olish;
3-bosqichda	virusli hujumlar ta'sirini kamaytirish.

Xavfsizlik choralari natijasida kompyuterga viruslarning kirib kelish xavfi kamayadi. Shubhali manbalardan olingan dasturiy ta'minotdan qochish kerak. Ma'lumot almashish paytida virusga xos bo'lgan baytlarni aniqlash va viruslarga xos bo'lgan harakatlarni qayd etish ularni qidirishning asosi hisoblanadi.

Mavjud axborotlarni himoyalash uchun kompyuter viruslariga qarshi dasturiy vositalar bozorida kompyuter viruslaridan himoyalanish, ularni yo'q qilish va aniqlash uchun bir necha maxsus dasturlar yaratilgan. Bunday dasturlar ***antivirus dasturlari*** deb ataladi.

Taqqoslash uchun zarur ma'lumotlar antivirus dasturining ma'lumotlar bazasida saqlanadi. Antivirus bazasini doimiy ravishda yangi viruslar haqidagi ma'lumotlar bilan to'ldirish, boshqacha aytganda, viruslar bazasini yangilash antivirus dasturlari muvaffaqiyati ishlashining asosiy omilidir.

Antivirus dasturlarining turlari

Detektorlar aniq virusning xarakterli holatini qidiradi, operativ xotira yoki fayldagi kerakli ma'lumotni aniqlaydi. Kamchiligi: ular o'zlariga ma'lum virusnigina aniqlaydi, yangi viruslarni esa aniqlay olmaydi (Aidstest, Doctor Web, MicroSoft AntiVirus).

Doktorlar (faglar) detektorlarga xos ishni bajargan holda zararlangan fayldan viruslarni

chiqarib tashlaydi va faylni oldingi holatiga qaytaradi. Doktor dasturlar ko'p miqdordagi viruslarni aniqlash va yo'q qilish imkoniyatiga ega (AVP, AidsTest, Scan, Kaspersky Antivirus, Norton Antivirus, Doctor Web, Panda).

Revizorlar – eng ishonchli himoyalovchi vosita. Dastlab dastur va diskning tizimli sohasi haqidagi ma'lumotlarni xotiraga oladi, so'ngra ularni dastlabkisi bilan solishtiradi. Mos kelmagan holatlar haqida foydalanuvchiga ma'lum qiladi (ADinf, Kaspersky Monitor).

Vaksinalar dasturlar ishlashini davom ettirib, ularni viruslar yuqtirgandek qilib o'zgartiradi. Natijada, viruslar bu dasturni zararlangan, deb hisoblaydi va bunday fayllarga "yopishmaydi". Faqat ma'lum viruslarga nisbatangina vaksina qilinishi uning kamchiligi hisoblanganligi sababli bunday antivirus dasturlar keng tarqalmagan (Anti Trojan Elite, Trojan Remover, Dr.Web CureIt, Web WinWord).

Filtrlar kompyuter tezkor xotirasida qo'riqlovchi dasturlar ko'rinishida (rezident kabi) joylashadi, viruslar tomonidan zararni ko'paytirish va ziyon yetkazish maqsadida operatsion tizimga qilinayotgan murojaatlarni ushlab qoladi hamda bu haqida foydalanuvchiga ma'lum qiladi. Foydalanuvchi ushbu amalni bajarish yoki bajarmaslikka ko'rsatma beradi. Filtr-dasturlar foydali bo'lib, u virus ko'payib ulgurmasidan oldin aniqlab beradi. Ular disk va fayllarni tozalay olmaganligi sababli, viruslarni yo'q qilish uchun boshqa dasturlar kerak bo'ladi (Flushot Plus, Antirus, Outpost Security Suite, Agnitum Outpost Firewall).

Yangi viruslarning to'xtovsiz paydo bo'lib turishini hisobga olib, antivirus bazalarini

KOMPYUTERNI VIRUSLARDAN SAQLASH UCHUN QUYIDAGI QOIDALARGA AMAL QILING:

- kompyuteringizga sinalgan antivirus dasturini o'rnating;
- tashqi xotira qurilmalarini ishlatishdan oldin har doim virusga qarshi tekshiring;
- har doim qimmatli axborotlaringiz zaxira nusxasini saqlang.

doimiy ravishda yangilab turish hamda kompyuter (protsessor, operativ xotira, operatsion tizim)ga mos antivirus dasturlarining oxirgi versiyalaridan foydalanish talab qilinadi.

Kompyuterda viruslarni qidirish ma'lumot tashuvchilarni skanerlash (ingl. ***scan***) orqali amalga oshiriladi. Skanerlash vaqtida operativ xotira va saqlash vositalarining virus bilan zararlangan yoki zararlanmaganligi tekshiriladi. Skanerlash natijasida aniqlangan viruslar o'chiriladi yoki bartaraf etiladi. O'zgartirilgan (zararlangan) fayllar imkon qadar asl holatiga qaytariladi.

Quyidagilar hozirgi kunda eng keng tarqalgan antivirus dasturlari hisoblanadi:

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA


Avast Free Antivirus


AVG AntiVirus FREE2021


Avira Free Antivirus


Bitdefender Total Security


ESET NOD32 Smart Security


Kaspersky Internet Security


360 Total Security


Panda Dome


Comodo Antivirus


Dr.Web Antivirus


Norton AntiVirus


McAfee VirusScan Enterprise


Microsoft Security Essentials


Adaware Free Antivirus


ClamWin Free Antivirus

Bu antivirus dasturlarining aksariyati to'lovli mahsulotlar hisoblanadi, lekin shaxsiy kompyuterlar uchun ularning bepul analoglari ham mavjud.

ESET NOD32 virus, zararli dastur, qurt, rootkit, ekspluatatsiya, ransomware, fishing dasturlari kabi zararli dasturlardan himoya qiladi. U kam joy egallaydi, bu esa kompyuter sekinlashuvining oldini oladi.

(Eslatma! Dasturni https://dr.rtm.uz yoki https://www.esetnod32.ru saytlaridan ham ko'chirib olishingiz mumkin).

AMALIY FAOLIYAT

TOPSHIRIQLAR

1-topshiriq. Internetdan Eset Nod32 Internet Security antivirus dasturini yuklab oling va o'rnating.

1. https://www.esetnod32.ru saytiga kiring va ESET NOD32 Internet Security dasturini yuklab olish uchun СКАЧАТЬ tugmachasini bosing.
2. Kompyuterning "Загрузки" papkasiga ko'chirib olingan fayllar ro'yxatidan eset_internet_security_live_installer .exe o'rnatish faylini toping va o'rnatuvchi faylni ishga tushiring.
3. Ochilgan muloqot oynasidagi "Да" (dasturni kompyuterga o'rnatish uchun rozilik) tugmachasini bosing.
4. So'ngra tilni tanlang va "Продолжить" tugmachasini bosing.
5. Foydalanuvchi litsenziya shartnomasini qabul qilganingizni tasdiqlash uchun "Я принимаю" tugmachasini bosing.

Eslatma! Agar kompyuteringizda boshqa antivirus yoki xavfsizlik dasturlari o'rnatilgan bo'lsa, o'rnatish ustasi buni ko'rsatadi. Siz bu dasturlarni kompyuterdan o'chirib tashlashingiz va o'rnatishni qaytadan bajarishingiz kerak.

6. Dastur sizga ba'zi sozlamalarni sozlab olishni taklif etadi. Ular quyidagilar:

- bo'lim ishlash prinsipi bizdagi shubhali, ya'ni virus sifatida ko'rinmaydigan, lekin xatti-harakatlari virusga o'xshashni boshlaydigan dasturlar haqida ma'lumot yig'adi va uni antivirusning viruslarni o'rganuvchi bazasiga yuboradi. Agar bunday funksiya ishlamasligini xohlasangiz, uni o'chirib qo'yishingiz mumkin;
- kompyuterning ba'zi dasturlari bo'lib, ular virus hisoblanmaydi, ammo uning tarkibidagi ayrim funksiyalar virus ko'rinishida bo'lishi yoki kompyuterga o'rnatilganidan so'ng uni sekinlashtirishi yoki xavfsizligiga tahdid qilishi mumkin. Ular haqida ogohlantirish olishni istasangiz, uni belgilash lozim.

Kerakli tanlovlarni amalga oshirgandan keyin "Далее" tugmachasini bosing.
7. So'ngra ESET NOD32 Internet Security antivirus dasturining o'rnatilish jarayoni boshlanadi.
8. Keyingi ochilgan oynadan "Пропустить вход" tugmachasini bosing.

Eslatma: Agar kompyuteringiz Internetga ulangan bo'lsa, u holda qurilmani myESET hisob qaydnomangizga ulashingiz mumkin. Hozircha siz "Пропустить активацию" tugmachasini bosib, faollashtirishni o'tkazib yuboring. Dastur to'liq ishlash uchun ESET NOD32 Internet Security o'rnatilganidan keyin faollashtirilgan bo'lishi lozim. Dasturni faollashtirish uchun Internetga ulangan bo'lishingiz zarur.

9. Dasturning bepul versiyani faollashtirish uchun "Готово" tugmachasini bosing va dastur yuklanishini kuting.
10. O'rnatish muvaffaqiyatli tugallanganidan so'ng, kompyuterni qaytadan yuklang.

2-topshiriq. Flesh-diskni ESET NOD32 Internet Security dasturida skanerlang.

- **Ish stoli, vazifalar paneli yoki bosh menyudan ESET NOD32 Internet Security dasturiga tegishli belgini bosish orqali dasturni ishga tushiring.**
- **Flesh-diskni USB-portga o'rnating.**
- **Hosil bo'lgan oynadan "Сканировать сейчас" buyrug'ini tanlang va skanerlash jarayonini kuzating.**
- **Skanerlash jarayoni tugagach, quyidagi ko'rinishda oyna hosil bo'ladi:**
- **Skanerlash natijasida aniqlangan va tozalangan fayllar haqida ma'lumot olish uchun "Просмотреть очищенные обнаружения" tugmachasini bosing.**

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

Eslatma! Kompyuterga axborot tashuvchi vositalar (kompakt disk, USB-qurilma va h. k.) ulanganda, ESET Internet Security dasturi avtomatik skanerlash imkoniyatiga ega. Bu jarayon kompyuter administratoriga foydalanuvchilar axborot tashuvchi vositalari orqali kirib kelishi mumkin bo'lgan zararlangan fayllardan "omon qolishda" yordam beradi.

Dastur nomi	Dastur belgisi	Dastur turi
Avira Free Antivirus		Detektorlar
Norton AntiVirus		
Panda Dome		Filtrlar
AVG AntiVirus		
Dr.Web Antivirus		Doktorlar Vaksinalar
Microsoft Security Essentials		
ESET NOD32 Smart Security		Revizorlar
Avast Free Antivirus		

1. Kompyuteringizni antivirus dasturi bilan tekshiring.
2. Ko'plab mamlakatlarda zararli dasturlarni yaratish, ulardan foydalanish va tarqatish qonun bilan taqiqlangan. Masala yuzasidan ma'lumot to'plang. Bu sohada O'zbekistonda qanday ishlar olib borilmoqda?
3. Jadvalni to'ldiring:

Antivirus dasturlari	Afzalliklari	Kamchiliklari

UYGA VAZIFA