## 5-laboratoriya ishi mavzu: Antivirus dasturlaridan foydalanish.

**Reja:**

10.1. Antivirus dasturidan foydalanish yo'llari.
10.2. Offis dasturlani hujjatlarini himoyalash.

**Laboratoriya ishini maqsadi:** Talabalarda kompyuterlarda axborot xavfsizligini ta'minlashda antivirus dasturidan foydalanish ko‘nikmalarini hosil qilish.

**Orgtexnika jixozlari:** Zamonaviy kompyuterlar; videoproektor; video ekran (doska); Internet tarmog‘i. Zamonaviy operatsion tizimlari o‘rnatilgan kompyuterlar; Videoproektor, Brouzerlar, Antivirus ilovalari.

### Nazariy qism. Axborot xavfsizligini.

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

**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.

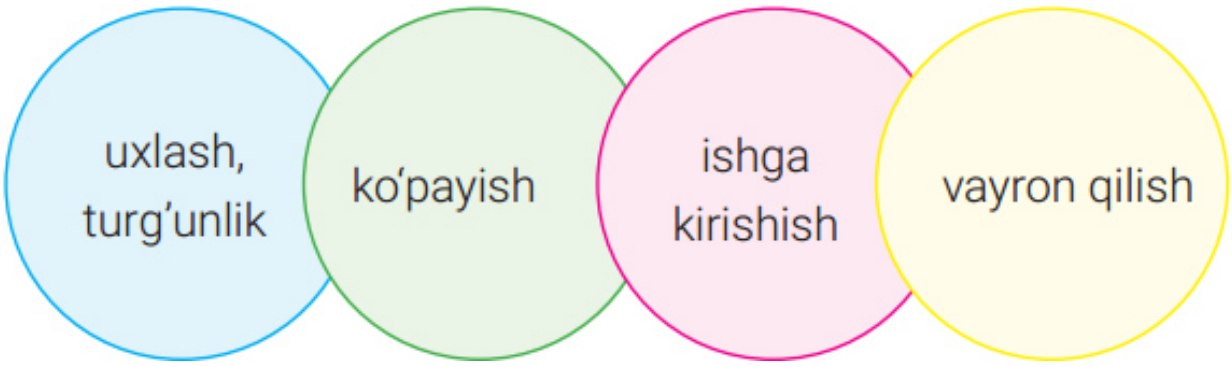
Axborotlarni muhofaza qilishga bo‘lgan asosiy tahdidlaridan biri – kompyuterga "kirib olgan" zararli dasturlardir. Ular ma'lumotlarning yaxlitligiga tahdid solishi mumkin. Zararli dasturlarning eng keng tarqalgan turi – kompyuter viruslari.

Kompyuter virusi dastur, hujjat yoki axborot tashuvchi qurilmalarning ma’lum bir qismiga kirib oluvchi parazitar dastur kodi hisoblanadi.Parazitar dastur kodi kompyuterda turli zararli ishlarni amalga oshiradi. O‘zidan nusxa ko‘chirish, axborotdan ruxsatsiz foydalanishni amalga oshirish Axborot xavfsizligini ta’minlash muammolarining dolzarbligi va muhimligiga quyidagilar sabab bo’lmoqda:

**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. 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.


4.1- rasm. Zararli dasturlarning kompyuterga kirishi yo‘llari

Virusning kompyuterdagi “hayot tarzi”, asosan, 4 bosqichda kechadi:




**4.2-rasm.**

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.

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.

Zararli dasturlarning turlari ko‘p.

**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.

**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.

**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.

**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.

**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.

**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.

**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.

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 dasturlarideb 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 viruslarnichiqarib 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).

Filtrlarkompyuter 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 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:


4.3-rasm.

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.

## Amaliy qism.

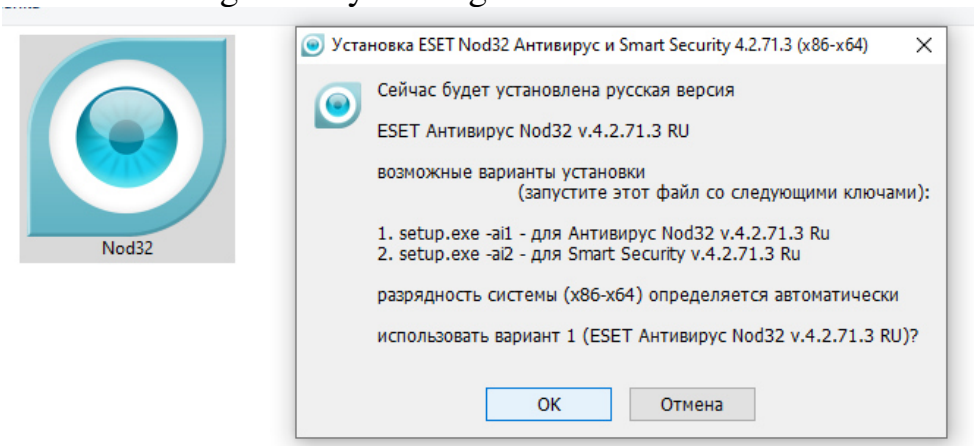
### Laboratoriya topshirig‘ini bajarish.

### 1- topshiriq.

ESET NOD32 antivirusi dasturi xozirgi kunda keng tarqalgan antivirus dasturi xisoblanib eng qo’lay antivirus dasturi xisoblanadi bu dasturdan foydalanish uchun unu kompyuterga o’rnatib olishimiz kerak bo’ladi

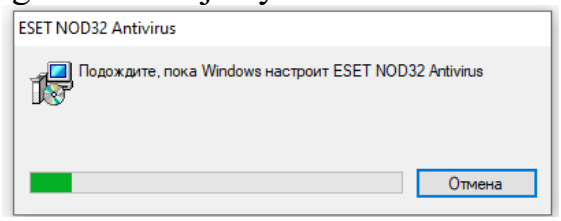
### 1-qadam.

Eset nod 32 dasturining .exe faylini ishga tushiramiz 5.1-rasm.



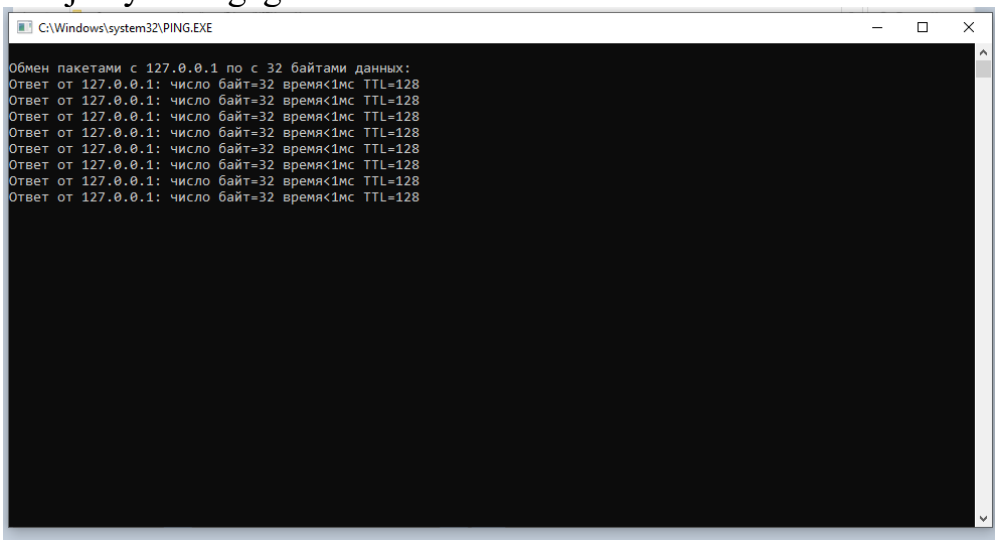

5.1-rasm.

Eset nod 32 dasturining o’rnatilish jarayoni boshlanadi 5.2-rasm.




5.2-rasm.

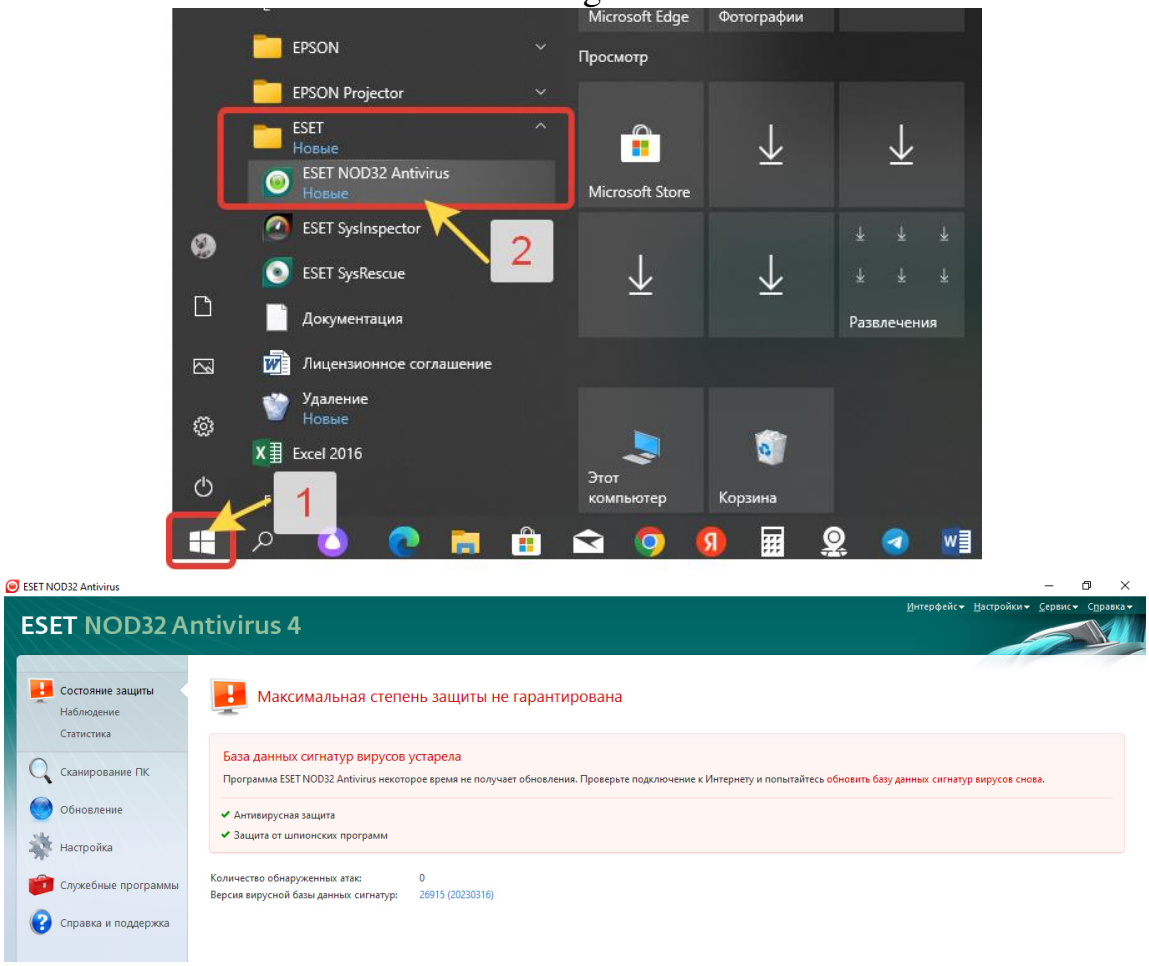
O’rnatilish jarayoni tugaguncha kutamiz 5.3-rasm.




5.3-rasm.

**2- qadam.**

Eset nod 32 dasturini ishga tushiramiz 5.4-rasm.

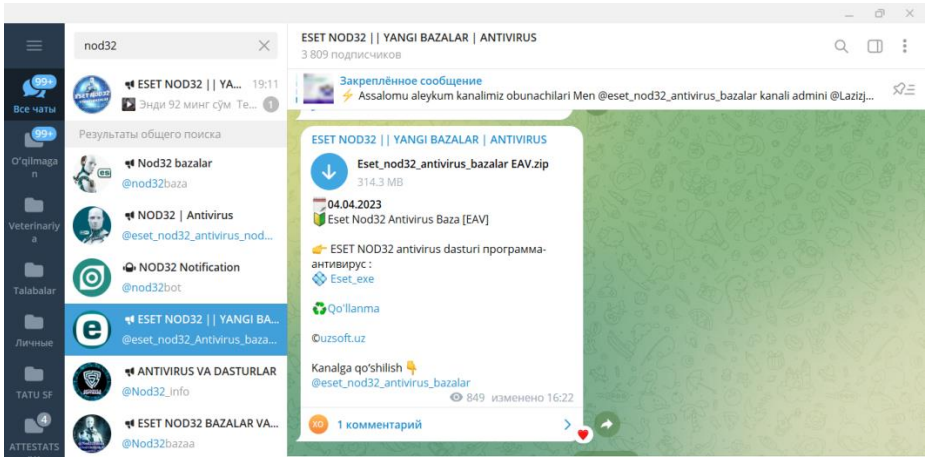



5.4-rasm.

Eset nod 32 dasturini viruslaga qarishi kurashish uchun uning bazasini internet tarmog'idan yuklab olib yangilab borishimiz zarur bo'ladi bunig uchun quydagi amallarni bajaramiz.

**3-qadam.**

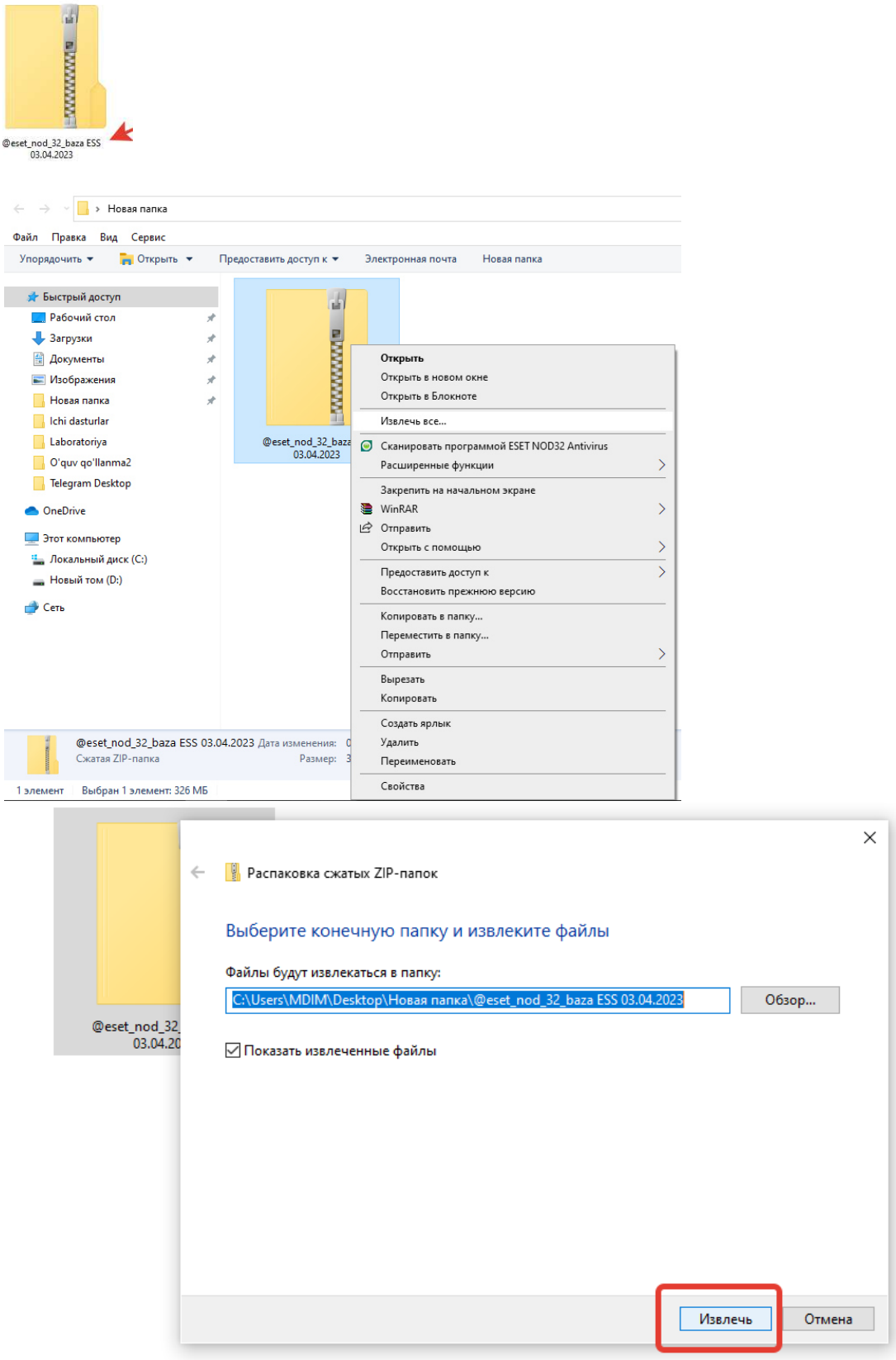
Eset nod 32 anitivirus dastunini bazasini telegramdagi t.me/eset_nod32_Antivirus_bazalar (https://t.me/eset_nod32_Antivirus_bazalar) kanalidan yuklab olishimiz mumkin 5.5-rasm.




5.5-rasm.

**4-qadam.**

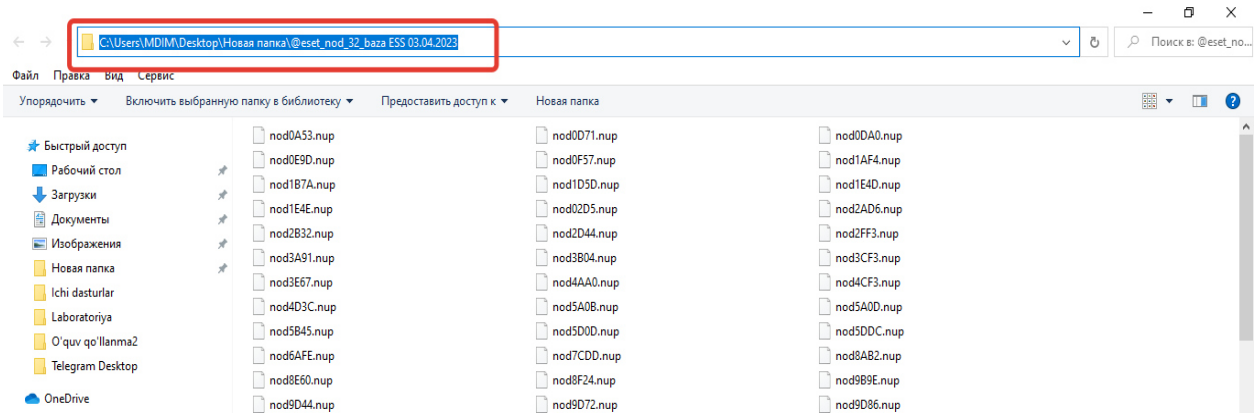
Eset nod 32 anitivirus dasturi bazasi arixivlangan papka ko’rinishida bo’ladi. Biz bu papkani arxivdan chiqarib olishimiz kerak 5.6-rasm.




5.6-rasm.

**5-qadam.**

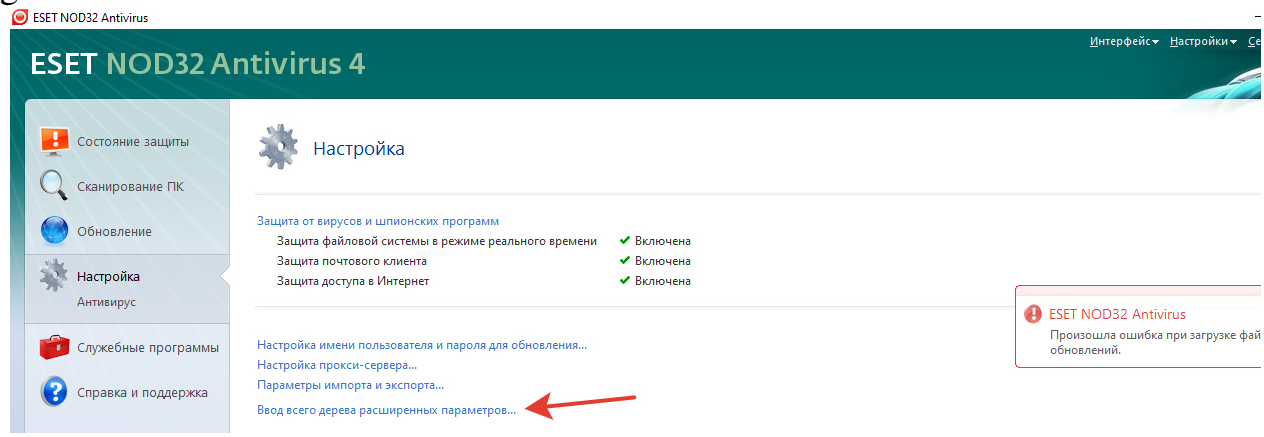
Arxivlangan papkadagi fayllar arxivdan chiqarilgandan so’ng papka yuqorisidagi manzilni nusxalab olamiz. 10.7-rasm.




5.7-rasm.

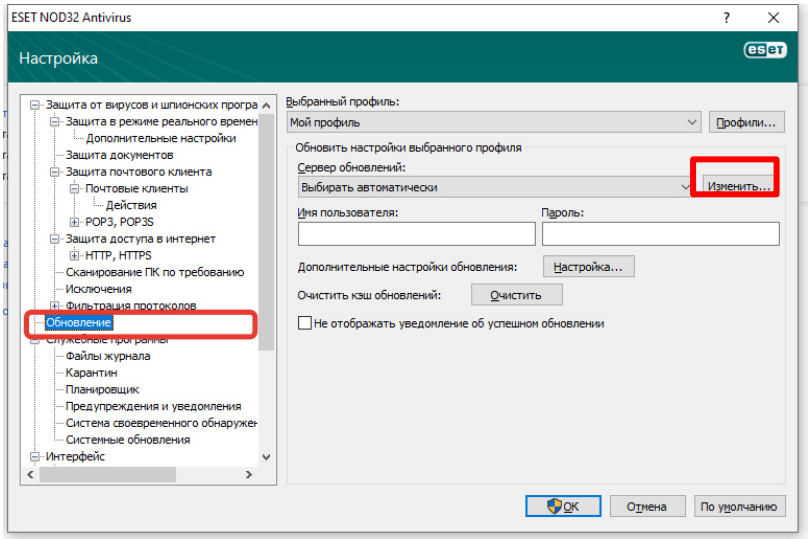
**6-qadam.**

Eset nod 32 anitivirusning sozlamalar bo’limiga o’tamiz va klaviyaturadagi F5 tugmasini bosamiz. 5.8-rasm.



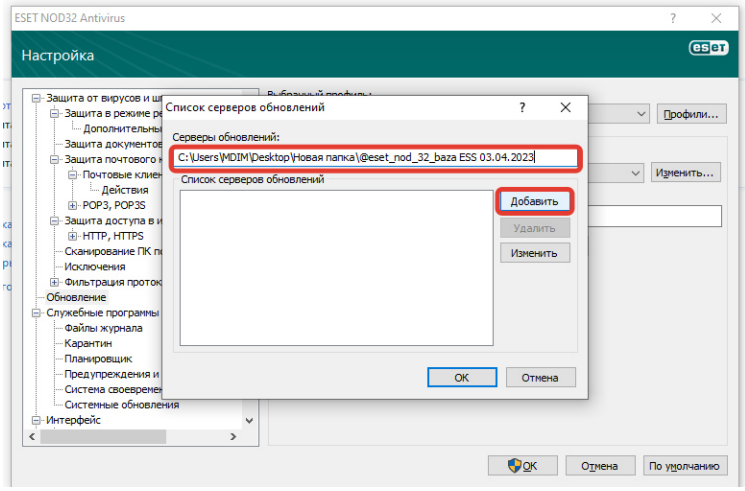

5.8-rasm.

Hosil bo’lgan oynadan *обновление* bo’limiga o’tamiz va изменить tugmasini bosamiz tanlaymiz. 5.9-rasm.



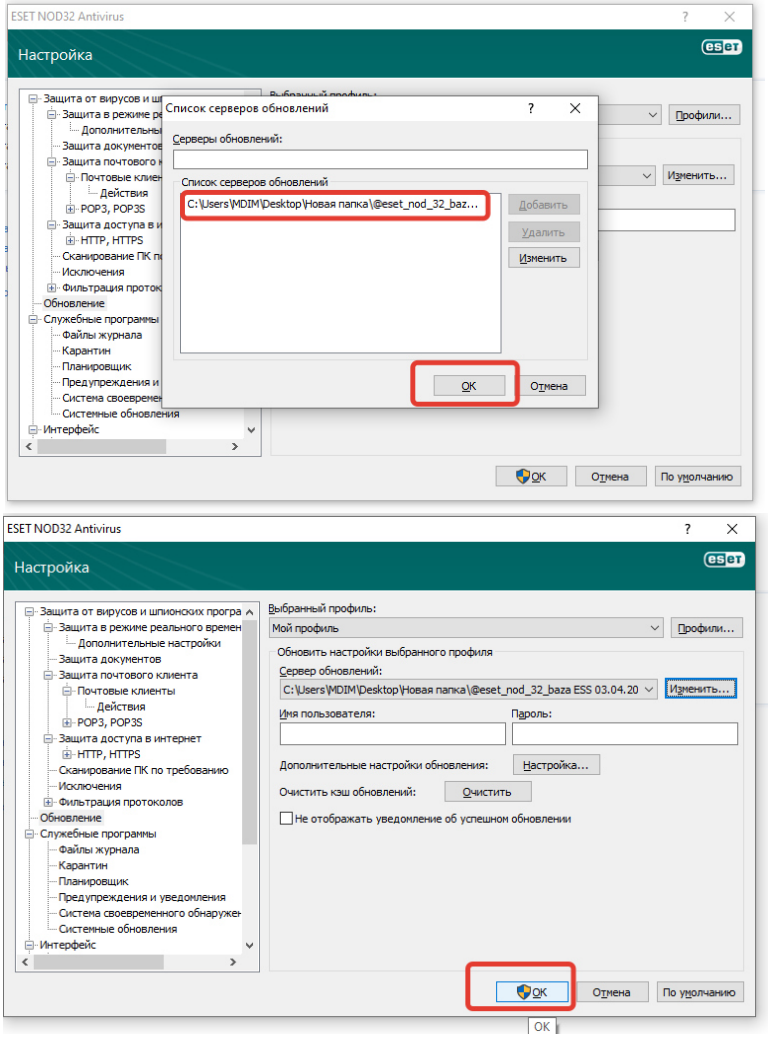

5.9-rasm.

Hosil bo’lgan oynaning ko’rsatilgan maydonga (5.7-rasm)dagi papka manzili nusxasini tashlaymiz va Добавить tugmasini bosamiz. 5.10-rasm.




5.10-rasm.

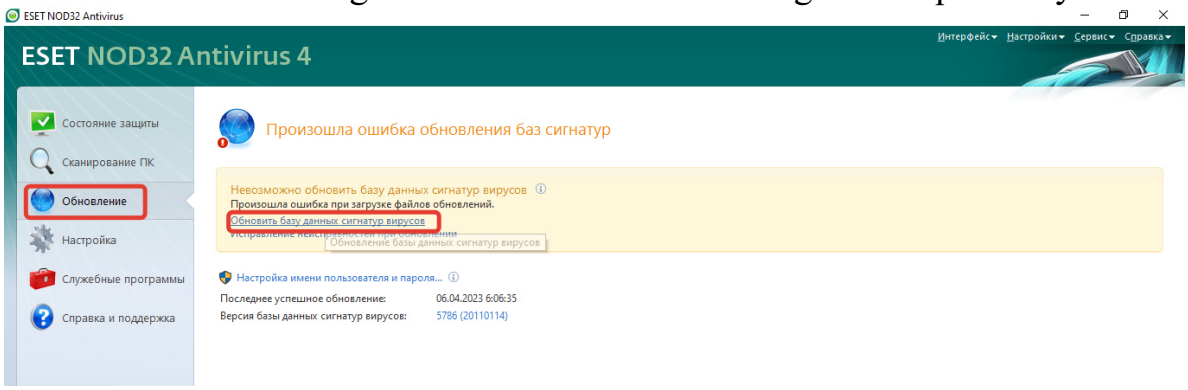
Natijada 5.11-rasm ko’rinishiga o’tadi va **ok** tugmalarini bosamiz.




5.11-rasm.

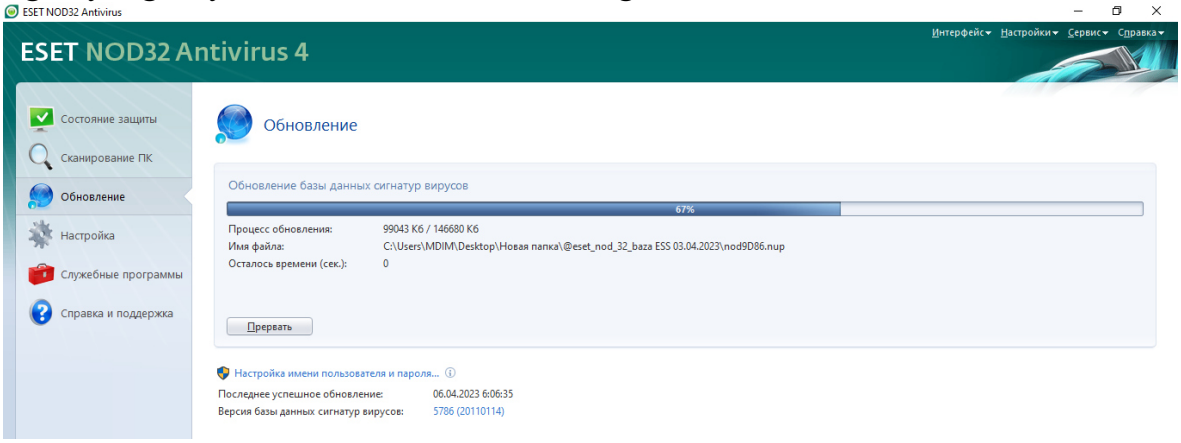
**7-qadam.**

*Обновление* bo’limiga o’tib 5.12-rasmda ko’rsatilgan buruqni tanlaymiz.



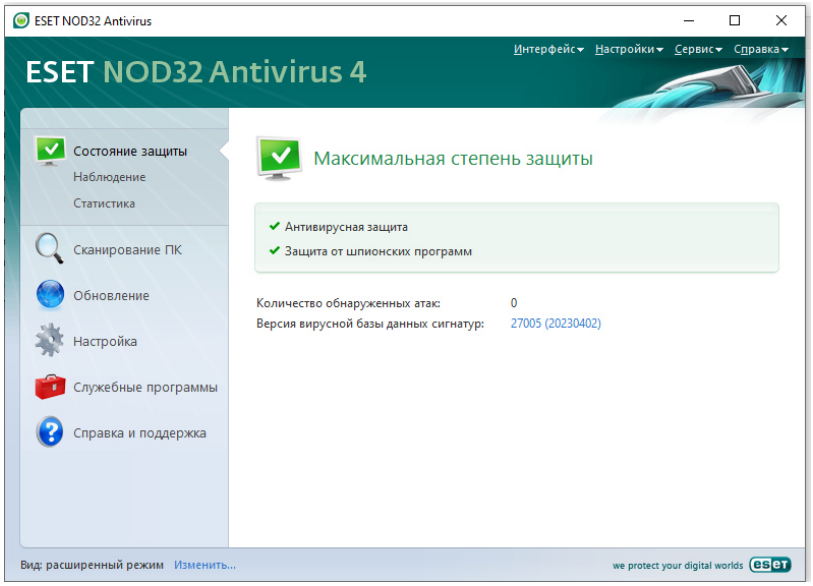

5.12-rasm.

*Обновление* jarayoni 17 ta bosqichdan o’tadi anitivirus dasturi o’ziga kerakli bo’lgan yangi fayllarni nusxasini bo’ bazasiga ko’shib oladi. 5.13-rasm.




5.13-rasm.

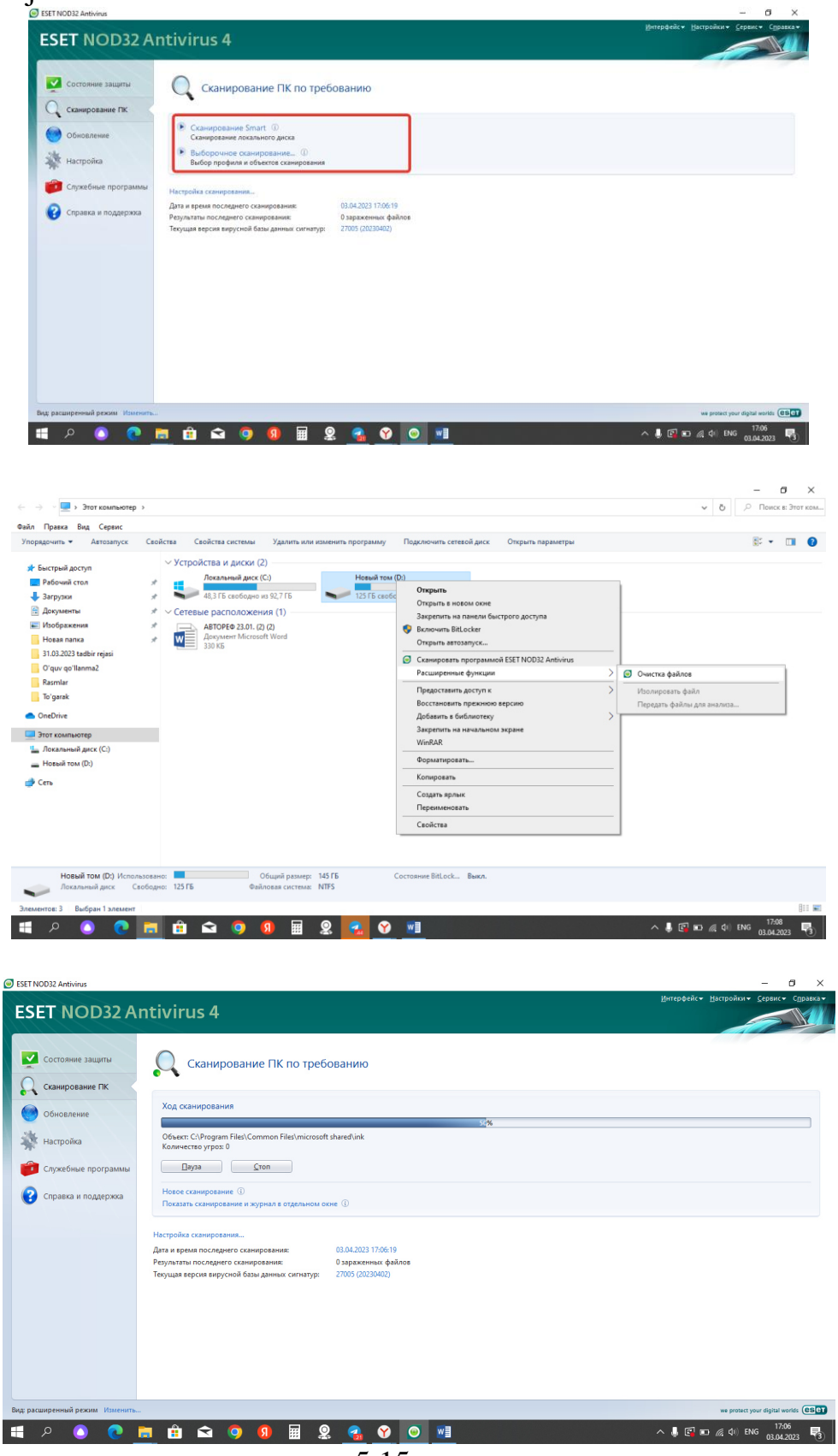
va nixoyat Eset nod 32 anitivirus dasturi maksimal darajada yangilanadi. 5.14-rasm.




5.14-rasm.

**8-qadam.**

Kompyuterimizni viruslardan tozalash uchun 5.15-rasmda ko’rsatilgan amallarni bajaramiz.



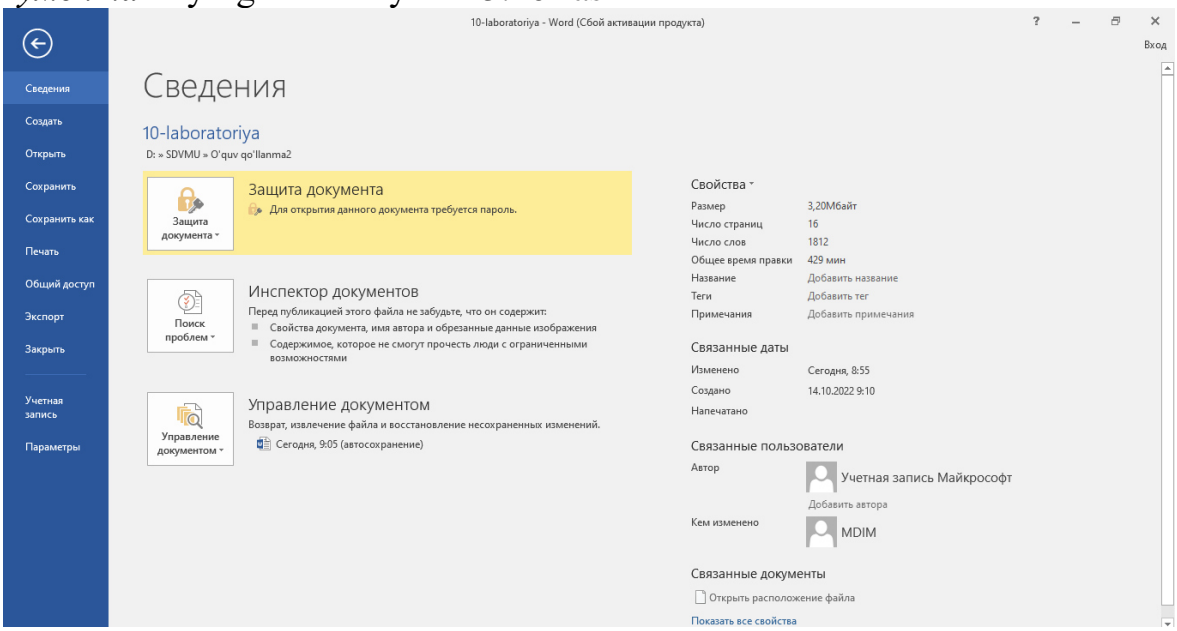

5.15-rasm

## Laboratoriya topshirig‘ini bajarish

Microsoft Office dasturlari yordamida yaratilgan sohga doir hujjatlarni himoyalash uchun quyidagi amallarni bajaramiz.

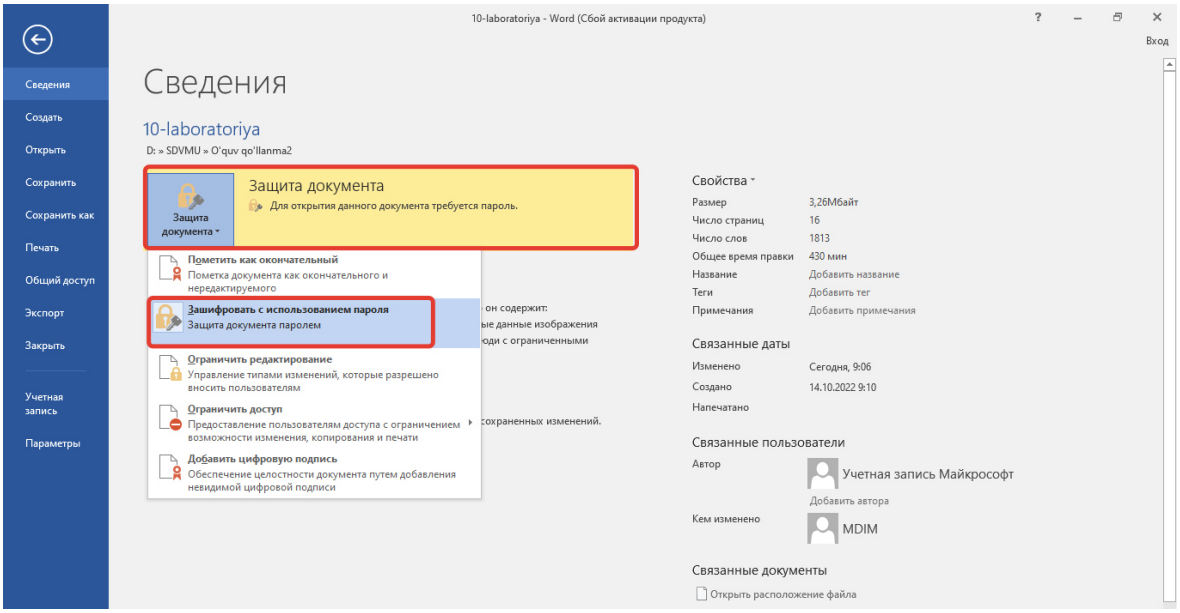
1-qadam.

Menyular qatoridan *Файл* bo’limiga kiramiz *сведения* bandidan *защита документа* buyrug’ini tanlaymiz. 5.16-rasm



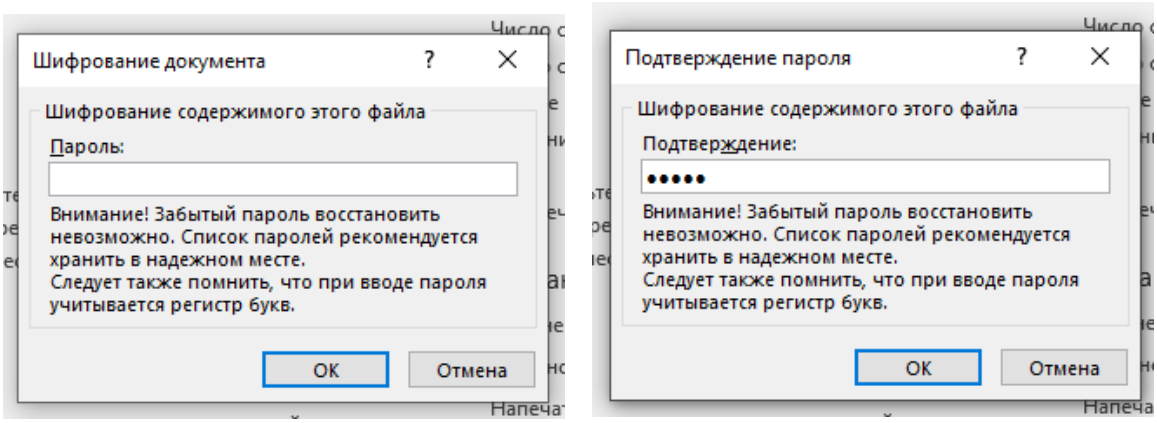

5.16-rasm.

va зашифровать с использованием пароля buyrug’ tanlanadi 10.17-rasm.



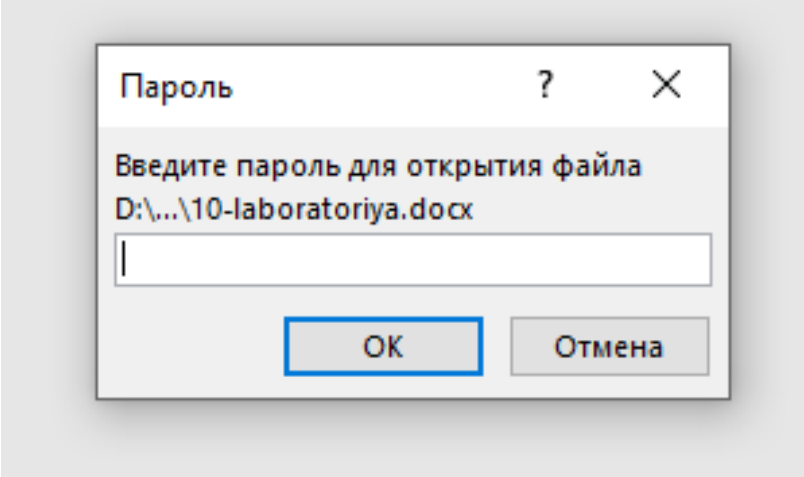

5.17-rasm.

Hosil bo’lgan oynaga xohlagan nomdagi matin yani harf yoki raqamlarni kiritamiz. Parolni ikki marta takror birxil matn kiritamiz va ok tugmasini bosamiz 5.18-rasm.




5.18-rasm.

Natijada ushbu parollangan hujjatga murojat etganimizda 10.19-rasmdagi oyna hosil bo’ladi biz parolni to’g’ri behato kiritib ok tugmasini bosamiz va hujjat ochiladi. Bundan ko’rinib turibdiki parolni bilmagan foydalanuvchi bu hujjatdan foydalana olmaydi bu esa bizning hujjatlarimizni havfsizligini ta’minlaydi.




5.19-rasm.

**6. laboratoriya ishi uchun vazifalar:**

**1-topshiriq:** Internetdan Eset Nod32 antivirus dasturini yuklab oling va o‘rnating.

**2-topshiriq:** Internetdan Eset Nod32 antivirus dasturini yuklab oling va o‘rnating.

**3-topshiriq:** Flesh-disk va Kompyuteringizni antivirus dasturi bilan tekshiring.

**4-topshiriq:** Jadvalni to‘ldiring

| **Antivirus dasturlari** | **Afzalliklari** | **Kamchiliklari** |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

Mavzuni mustahkamlash uchun savollar.

1. Axborotlarni himoyalashning texnik va dasturiy vositalari
2. Fizik vositalar.
3. Axborotlarni himoyalashni apparat vositalari
4. Kodlashtirish
5. Kriptografiya
6. Stenografiyaning
7. Kalit tushunchasi
8. Almashtirish
9. Gammalashtirish
10. Taxliliy o’zgartirish
11. Axborotni ximoyalashning maqsadlari
12. Antivirus vositalari quyidagi masalalarni hal etish uchun qo‘llaniladi:
13. kompyuter tizimlarida viruslarni topish;
14. virus – dasturlar ishini blokirovka qilish;
15. viruslar ta’sirining oqibatlarini bartaraf qilish.