7 – AMALIY ISHI

MAVZU: AXBOROTGA XUJUMLARNI TAXLILLASH VA HIMOYA VOSITALARINI

Ishning maqsadi: Talabalarga axborot xavfsizligi va axborotlarni ximoyalash usullari haqida tushunchalar berish.

Qisqacha nazariy ma'lumotlar:

Nazariy ma'lumot.

Axborot xavfsizligini ta'minlash - foydalanuvchi ma'lumotlarini himoya qilish bo'yicha standartlar va talablarning bajarilishi.

Axborot xavfsizligi - axborot va axborot kommunikatsiya tizimi ob'ektlarini axborotdan foydalanuvchilarga va ko'plab axborot tizimlariga zarar etkazuvchi tabiiy yoki sun'iy xarakterdagi tasodifiy va uyushgan ta'sirlardan himoya qilish.

Axborot xavfsizligini ta'minlash tamoyillari quyidagilar xisoblanadi:

–**Ma'lumotlar butunligi** – axborotni yo'qotilishiga olib keluvchi buzilishlardan, shuningdek ma'lumotlarni mualliflik huquqi bo'lmagan holda hosil qilish yoki yo'q qilishdan himoya qilish.

–**Axborotning konfedentsialligi** – axborot va uning tashuvchisining holatini belgilaydi va unda axborot bilan ruxsatsiz tanishishning yoki uni ruxsatsiz nusxa ko'chirishning oldini olish ta'minlangan bo'ladi.

–**Foydalanish huquqlariga** – ya'ni mualliflikka ega barcha foydalanuvchilar axborotdan foydalana olishliklari.

Axborotlarni xavfsizligini ta'minlashda ma'lumotlarni arxivlash va ularning ahamiyati quyidagicha.

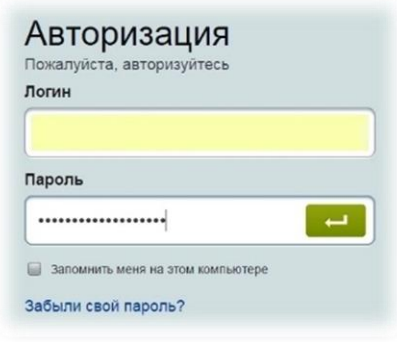
Login ya'ni Kirish tushunchasi.

Login - bu shaxs tomonidan o'zini axborot kommunikatsiya tizimiga tanishtirish jarayonida foydalaniladigan belgilar ketma-ketligi bo'lib, foydalanuvchining axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lgan maxfiy bo'lmagan yozuvidir.

Parol tushunchasi.

Parol - bu uning egasining haqiqiyligini aniqlash jarayonida tasdiqlash ma'lumoti sifatida ishlatiladigan belgilar ketma-ketligi. U alfanumerik yoki alfanumerik kod ko'rinishidagi maxfiy so'zdan iborat bo'lib, u kompyuter bilan aloqani boshlashdan oldin klaviatura yoki identifikatsiya kartasi yordamida kiritiladi.

Avtorizatsiya tushunchasi.



Avtorizatsiya - foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni. Bunday holda, foydalanuvchiga hisoblash tizimida muayyan vazifalarni bajarish uchun ma'lum huquqlar beriladi. Avtorizatsiya shaxsning harakatlari doirasini va u foydalanadigan resurslarni belgilaydi.

Ro'yxatdan o'tish tartibi.

Ro'yxatdan o'tish - foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlardan foydalanish huquqini berish jarayoni. Ba'zi veb-saytlar foydalanuvchilarga qo'shimcha xizmatlarni olish va pullik xizmatlarga obuna bo'lish uchun ro'yxatdan o'tishni taklif qiladi, ya'ni o'zlari haqida ba'zi ma'lumotlarni kiritish, shaklni to'ldirish, login va parolni olish.

Foydalanuvchi ro‘yxatdan o‘tgandan so‘ng, tizimda uning uchun hisob qaydnomasi yaratiladi va foydalanuvchi ma’lumotlari unda saqlanadi.

Login va parolga ega bo‘lish shartlari.

Shaxs o‘z login va paroliga ega bo‘lishi uchun avvalo axborot kommunikatsiya tizimida ro‘yxatdan o‘tgan bo‘lishi, so‘ngra o‘z login va parolini yaratishi yoki tizim tomonidan taqdim etilgan login paroliga ega bo‘lishi kerak. bo‘lishi mumkin. Login va parollar ma’lum uzunlikdagi belgilar ketma-ketligidan iborat. Login va parollarning uzunligi va murakkabligi uning qanchalik xavfsizligini ta’minlaydi, ya’ni uni buzish mumkin emas.

Login va parolni buzish.

Login va parolni buzish – axborot kommunikatsiya tizimi obyektlaridan qaysidir maqsadda foydalanish uchun foydalanuvchilarga tegishli login va parollarni xakerlik qilishdir. Login va parollar maxsus dastur yordamida yaratiladi. Login va parollarning uzunligi bu jarayonning uzoq davom etishi yoki yaratib bo‘lmasligidan dalolat beradi.

Login va parolni o‘g’irlash.

Login va parolni o‘g’irlash - foydalanuvchilarning login va parollar kabi maxfiy ma’lumotlariga kirishni maqsad qilgan internet-firibgarlikning bir turi. Bu mashhur brendlar, ijtimoiy tarmoqlar, banklar va boshqa xizmatlar nomidan ommaviy elektron pochta xabarlarini yuborish orqali amalga oshiriladi. Xatda odatda saytga haqiqiy havola mavjud bo‘lib, u tashqi ko‘rinishida asl saytdan farq qilmaydi. Bunday saytga tashrif buyurgan foydalanuvchi hisob va bank hisob raqamlariga kirish uchun firibgarga maxfiy ma’lumotlarni taqdim etishi mumkin.

Fishing - bu foydalanuvchilarning tarmoq xavfsizligi asoslarini bilmasligiga asoslangan ijtimoiy muhandislik shakli. Xususan, ko‘pchilik oddiy haqiqatni bilishmaydi: xizmatlar hech qachon sizga hisob ma’lumotlarini, parolni va hokazolarni yuborishingizni so‘rab xat yubormaydi.

Resurslardan ruxsatsiz foydalanish va uning oqibatlari.

Axborot aloqa tizimining ixtiyoriy tarkibiy qismlaridan biri bo‘lib, axborot tizimi tomonidan taqdim etilgan resurslardan belgilangan qoidalarga rioya qilmasdan resurslardan foydalanish qoidalariga rioya qilmasdan foydalanish ushbu resurslardan ruxsatsiz foydalanish toifasiga kiradi.

Bunday foydalanish natijasida quyidagi oqibatlarga olib kelishi mumkin:

- ❖ Axborotni o‘g’irlash;
- ❖ Axborotni o‘zgartirish;
- ❖ Axborotni yo‘qotish;
- ❖ Noto‘g’ri ma’lumotlar kiritish;
- ❖ Axborotni soxtalashtirish va boshqalar.

Kompyuter virusi.

Kompyuter virusi - bu o‘zini ko‘paytiruvchi, kompyuter tarmoqlari va axborot tashuvchilari orqali erkin tarqaladigan, kompyuterga, unda saqlangan ma’lumotlar va dasturlarga zarar etkazadigan dastur kodi yoki buyruqlar ketma-ketligi. Kompyuter viruslari quyidagi xususiyatlarga ega: o‘z-o‘zidan nusxa ko‘chirish, ma’lumotlardan ruxsatsiz foydalanish. U o‘z nusxalarini kompyuterlar yoki kompyuter tarmoqlarida ko‘paytiradi va tarqatadi va qonuniy foydalanuvchilar uchun nomaqbul harakatlarni amalga oshiradi. Ko‘pgina hollarda, virus noto‘g’ri ishlash va ishdan chiqishga olib keladi va hodisa. **Masalan:** Ma’lum bir kunning kelishi bilan qo‘zg’alishi mumkin.

Viruslarning turlari va vazifalari.

Viruslarni quyidagi asosiy belgilarga ko‘ra tasniflash mumkin:

- ✓ Yashash maydoni;
- ✓ Operatsion tizim;
- ✓ Ishlash algoritmi xususiyati.

Kompyuter viruslarini yashash muhitiga ko‘ra tasniflash, boshqacha aytganda, viruslar kiritilgan kompyuter tizimi ob’ektlarining turi asosiy va keng tarqalgan tasnifdir.

Fayl viruslari bajariladigan fayllarga turli usullar bilan kiritiladi. Viruslarning eng keng tarqalgan turlari fayl yo‘ldoshlari bo‘lib, ular hamroh viruslarni yaratadi yoki fayl tizimi viruslari xususiyatidan foydalanadi.

Yuklash viruslari o‘zlarini diskning yuklash sektorida yoki Vinchesterning tizim yuklovchisi Master Boot Record bo‘lgan sektorda yozadi. Yuklab olish viruslari tizimni yuklashda boshqaruvni o‘z zimmasiga oladigan dastur kodi sifatida ishlaydi.

Makro viruslar zamonaviy axborotni qayta ishlash tizimlarining makro dasturlari va fayllarini, xususan, MicroSoft Word, MicroSoft Excel va boshqalarni zararlaydi.

Tarmoq viruslari o‘zini tarqatish uchun kompyuter tarmoqlari va elektron pochta protokollari va buyruqlaridan foydalanadi. Tarmoq viruslari ba’zan qurtlarga o‘xshash dasturlar deb ataladi. Tarmoq viruslari Internet qurtlari Internet bo‘ylab tarqaladi.

Kompyuter viruslarining vazifalari odatda to‘rt bosqichni o‘z ichiga oladi:

- Virusni xotiraga yuklash;
- Jabrlanuvchini qidirish;
- Topilgan jabrlanuvchini zaharlash;
- Buzg’unchi funktsiyalarni bajarish.

Viruslarga qarshi kurash usullari.

Hozirgi vaqtda kompyuter viruslarini aniqlash va ulardan himoya qilish uchun bir necha turdagi maxsus dasturlar ishlab chiqilgan va bu dasturlar kompyuter viruslarini aniqlash va yo‘q qilish imkonini beradi. Bunday dasturlar antivirus dasturlari yoki antiviruslar deb ataladi. Antivirus dasturlariga AVP, Doctorweb, Nod32, Kaspersky kirishi mumkin. Umuman olganda, barcha antivirus dasturlari zararlangan dasturlarni va yuklash sektorlarini avtomatik ravishda tiklashni ta’minlaydi.

Viruslarga qarshi kurashning asosan quyidagi usullari mavjud:

1. Muntazam profilaktika choralarini o‘tkazish, ya’ni virusni tekshirish.
2. Ma’lum virusni zararsizlantirish.
3. Noma’lum virusni zararsizlantirish.

Hujum tushunchasi.

Hujum tushunchasi - bu axborot kommunikatsiya tizimlarining mavjud himoya tizimlarini buzishga qaratilgan bosqinchi harakatidir.

Axborot hujumlari va oldini olish qoidalari.

Axborot hujumlari odatda 3 ga bo‘linadi:

1. Ob’ekt ma’lumotlarini yig’ish (razvedka) hujumi.
2. Obyektga kirish hujumi.
3. Xizmat hujumini rad etish.

Axborot xurujlarining oldini olish uchun, birinchi navbatda, axborot kommunikatsiya tizimi ob’ektlariga hujumlarni aniqlash mexanizmlari va vositalaridan foydalanish zarur. Bunga misollar qatoriga xavfsizlik devorlari **FIREWALL** va kirishni aniqlash IDS vositalari kiradi. Shuningdek axborotlarni ximoyalashning Antivirusli himoya usuli ham mavjud.

Bular quyidagilar xisoblanadi.

- Litsenziyalangan antiviruslardan foydalanish;
- Muntazam profilaktika o‘tkazish;
- Viruslarni zararsizlantirish.

Axborot xavfsizligi tahdidlarining turlari sun’iy va tabiiy tahdidlardir.

SUN’IY.

- Tasodifiy.
- Qasddan.

Axborot xavfsizligiga sun'iy tahdidlar.

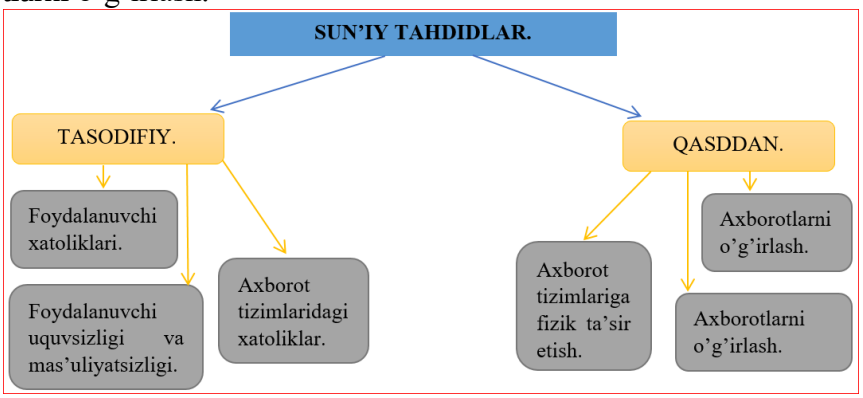
Tasodifiy:

- Foydalanuvchilarning xatoliklari.
- Foydalanuvchilarning uquvsizligi va mas'uliyatsizligi.

Axborot tizimlaridagi xatoliklar.

Qasddan:

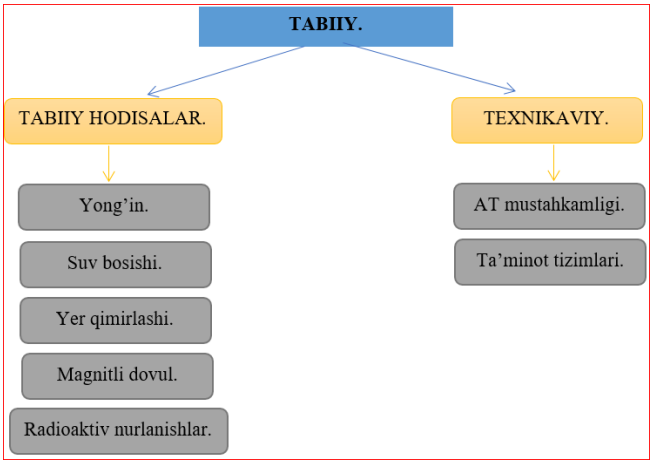
- Axborot tizimlariga fizik ta'sir etish.
- Axborotlarni o'g'irlash.



TABIIY.

- Tabiiy hodisalar.
- Texnikaviy.

Tabiiy xarakterdagi tahdidlar.



Zararli dasturiy mahsulotla.

Zararli dasturiy maxsulotlar – bu axborot tizimlaridagi ma'lumotlarni hamda dasturiy mahsulotlarni o'zgartirish, ko'chirib olish, o'chirish, foydalanuvchilarni maxfiy ma'lumotlaridan noqonuniy foydalanishdir.

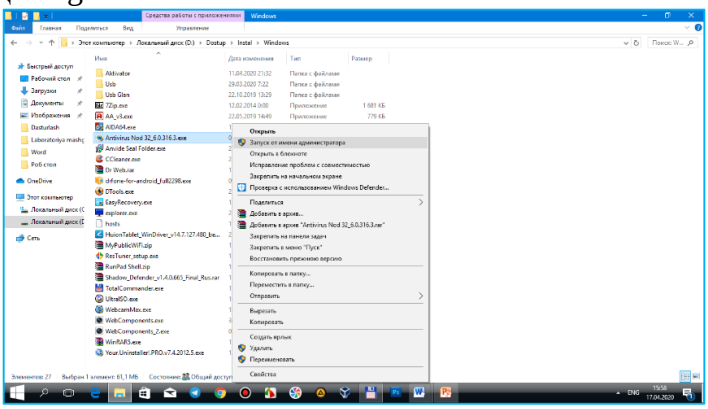
Shuningdek axborotlarni ximoyalashning Antivirusli himoya usuli ham mavjud. Bular quyidagilar xisoblanadi.

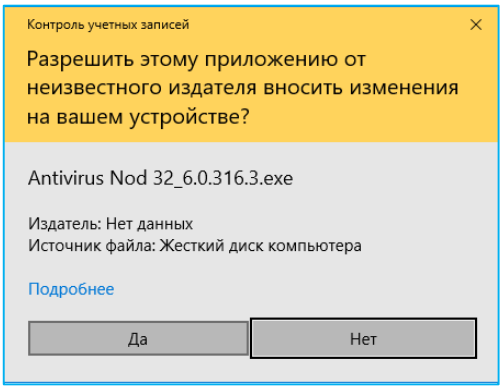
- Litsenziyalangan antiviruslardan foydalanish;
- Muntazam profilaktika o'tkazish;

Viruslarni zararsizlantirish.

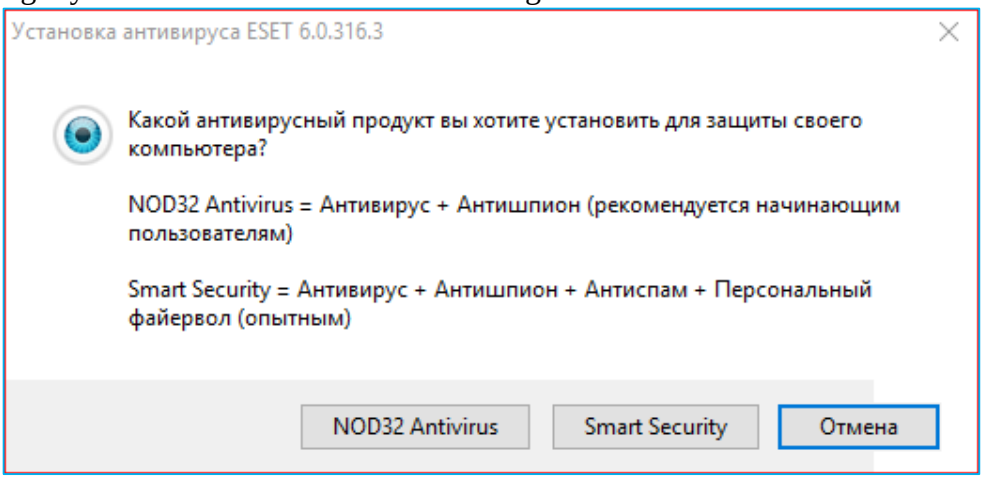
Antiviruslarning keng tarqalgan turi bu **ESET NOD32** antivirusidir. Antivirus orqali viruslardan himoyalanish quyidagicha amalga oshiriladi.

Eng birinchi navbatda **ESET NOD32** dasturini internet orqali yuklab olamiz yoki yuklanib olingan tayyor dastur bolsa antivirus dasturi ustida sichqonchaning chap tugmasi 2 – marotaba bosamizi yoki ushbu dastur ustida sichqonchaning o‘ng tugmasi bilan 1 – marotaba bosib xosil bo‘lgan **kontekst yordamchi menyu**sidan **Запуск от имени администратора** buyrug’ini tanlaymiz. Yoki antivirus dasturini sichqonchani chap tugnasini 1 – marotaba bosib tanlab olib klaviaturadan **ENTER** tugmasi bosiladi va dastur ishga tushiriladi So‘ngra xosil bo‘lgan oynadan **ДА** tugmasi bosiladi.

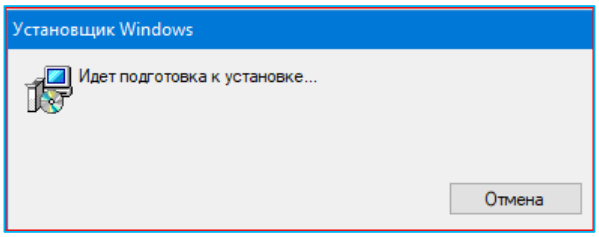


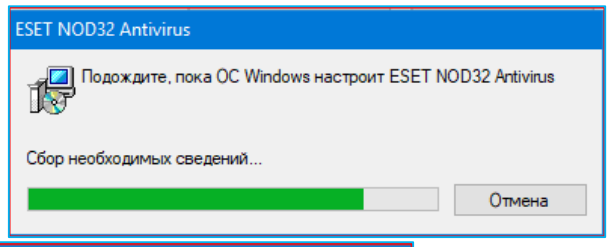


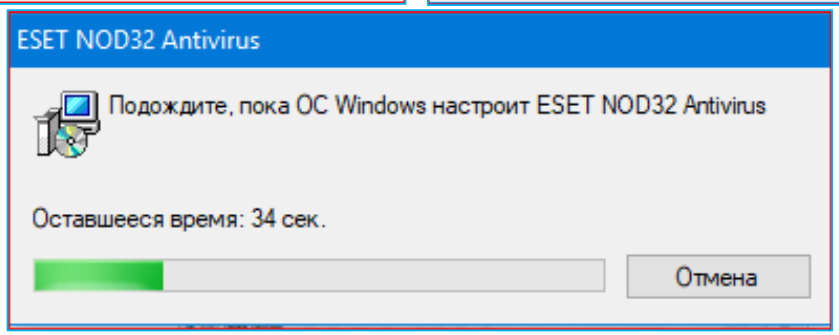
Keyingi oynadan **ESET NOD32** Antivirus tugmasi bosiladi.



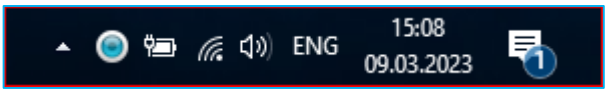
Dasturning o‘rnatilishi jarayoni boshlanadi. Bu ko‘p vaqt talab etmaydi.



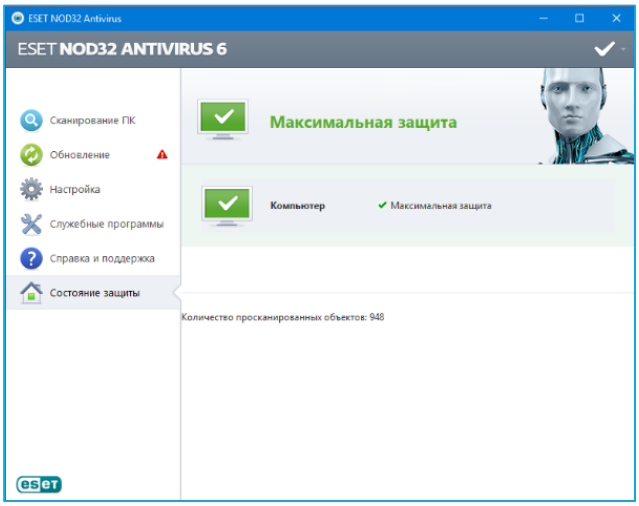




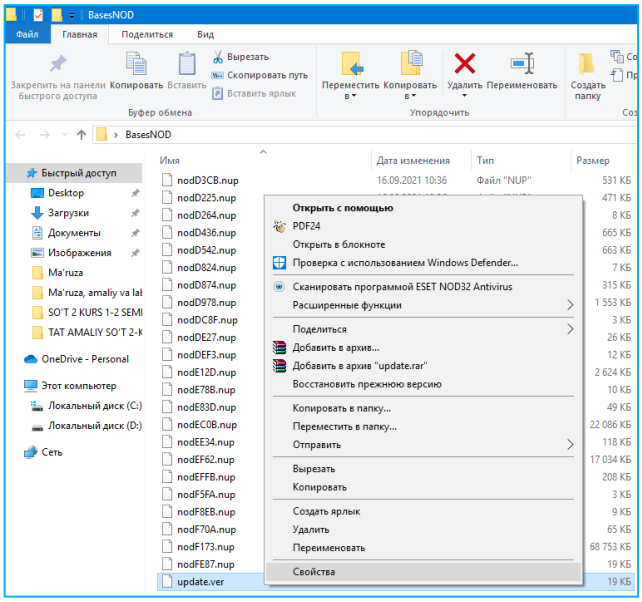
Dasturning o‘rnatilishi jarayoni yakunlanadi menyu satrida antivirus **ESET NOD32** yorlig’i paydo bo‘ladi.

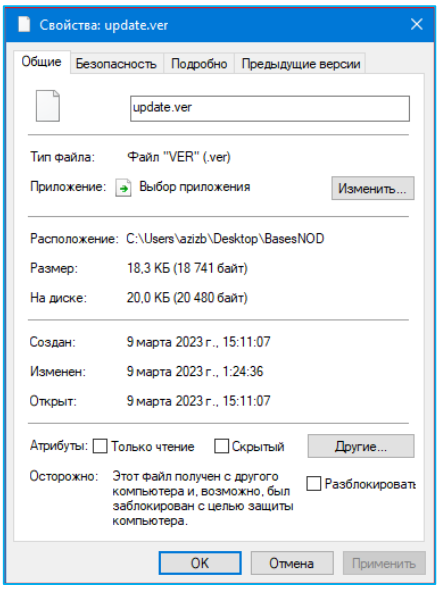


Antivirus dasturini ishga tushirib olamiz. **ESET NOD32** antivirus dasturining dastlabki oyna ko‘rinishi quyidagi rasmda tasvirlangan.

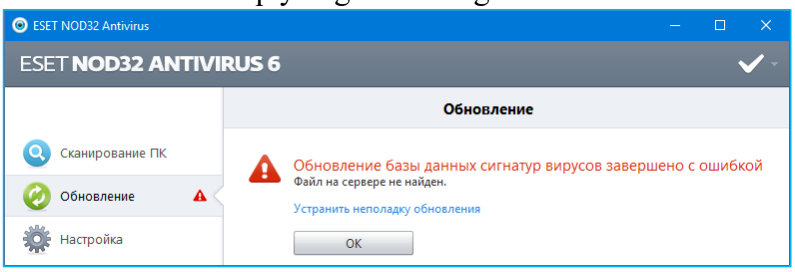


Barcha ishlar normal holatda bajarilgandan so‘ng bizning keyingi qiladigan ishimiz bu antivirusimizga internet tarmog’i orqali antivirus bazasini yuklab olishimiz kerak bo‘ladi. Yuklab olingan bazaning qaysi sanada yaratilgan ekanligi uning sig’imi necha megabaytdan iborat ekanligini bilishimiz uchun yuklab olingan **BasesNOD** papkasining ichidagi **VER** kengaytmalik fayl ustida sichqonchaning o‘ng tugmasini bosib yordamchi kontekst menyudan **Свойства** bandini tanlaymiz va ochilgan oynadan yuqorida ta’kidlangan ma’lumotlarni quyida keltirilgan rasmlarda ko‘rishimiz mumkun.

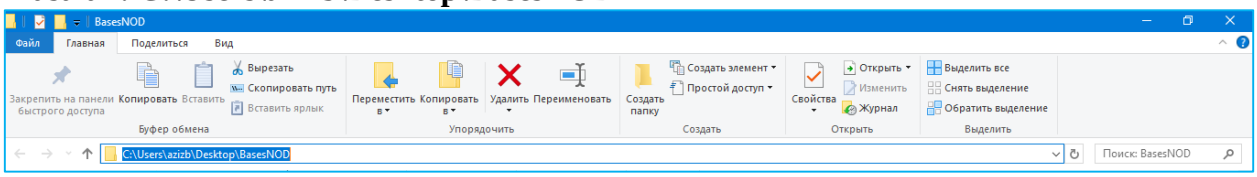




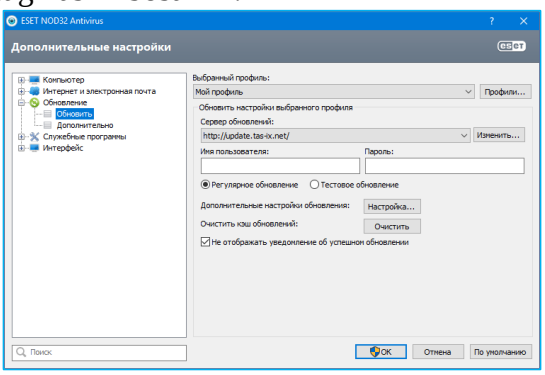
Antivirus asosiy oynasiga qaytib u yerdan 2 – bandi ya’ni **Обновление** bo‘limiga o‘tib yangi bazani o‘rnatamiz. Bu amallar quyidagicha amalga oshiriladi.

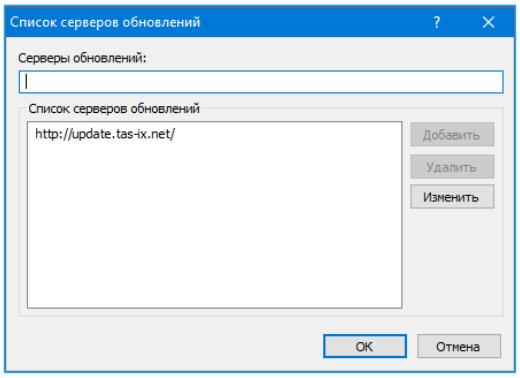


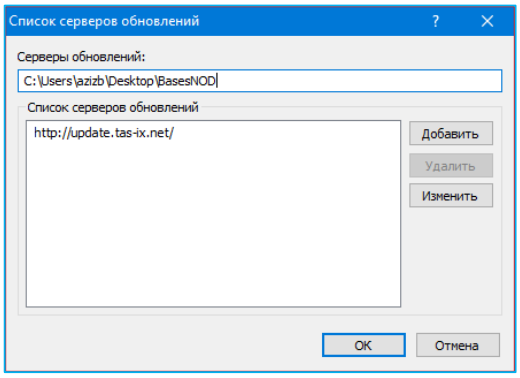
Yuklab olingan **BasesNOD** papkasiga kiramiz va oynaning o‘rta yuqori manzil yozilgan qismiga sichqonchaning chap tugmasini 1 – marotaba bosib manzilni belgilab va undan nusxa olamiz. Papka kompyuterning qayerida joylashgan bo‘lsa o‘sha joyning manzili chiqadi. **Masalan: C:\Users\azizb\Desktop\BasesNOD**

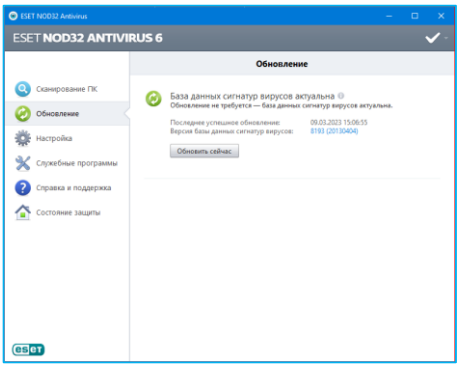


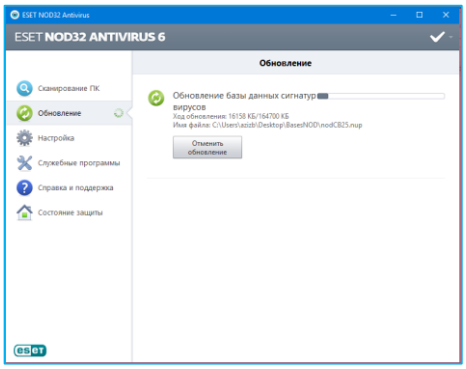
Olingan nusxani antivirus dasturi ustida klaviaturadan **F5** tugmasini bosib manzil qo‘yilishi lozim bo‘lgan yerga manzilni joylaymiz **Добавить** tugmasini keyin esa **OK** tugmasini bosib chiqib so‘ngra **Обнавить** tugmasini bosamiz.

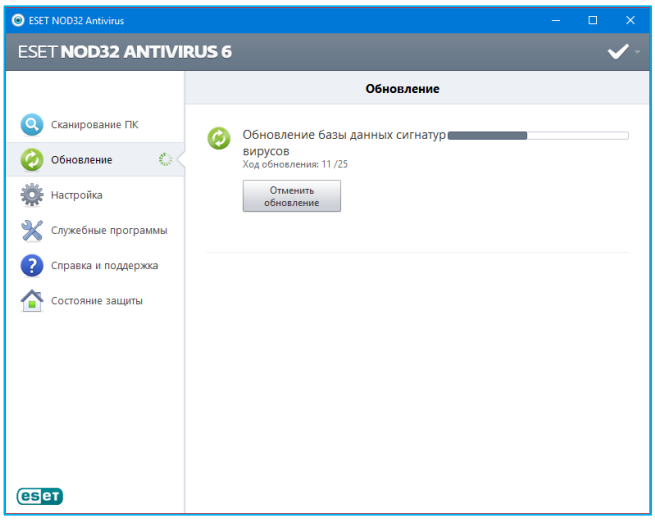




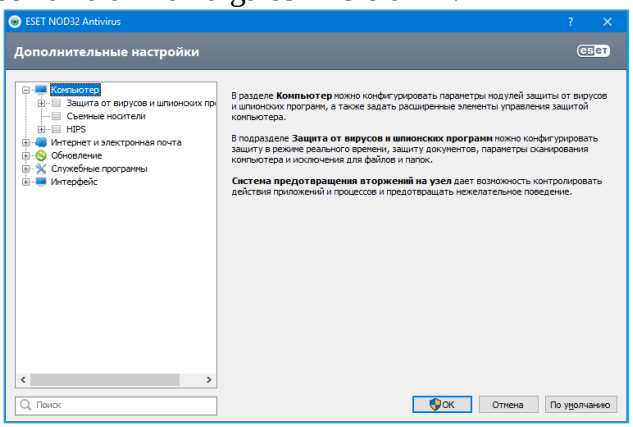


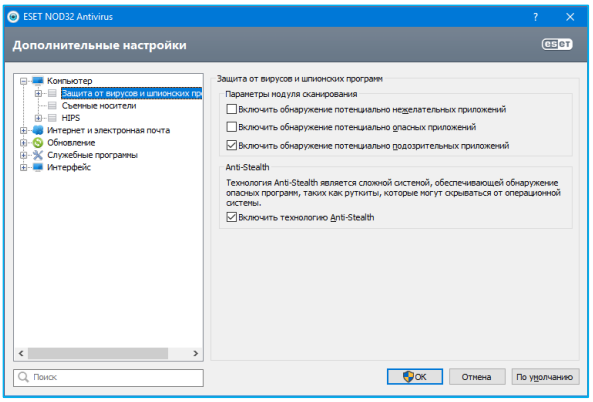


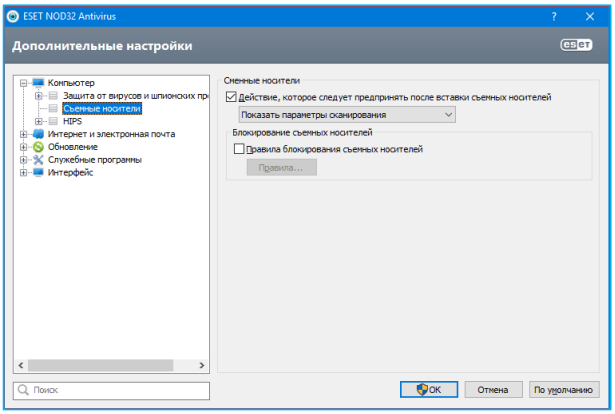


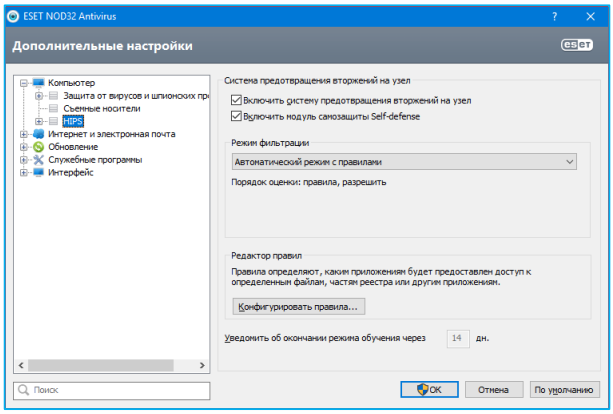


Настройка bo‘limiga o‘tib u yerdan **Перейти к расширенным параметраммы** bo‘limini tanlaymiz va natijada **Дополнительный настройки** oynasi ochiladi. U yerdan **Компьютер** bo‘limi tanlanib ushbu bo‘limga tegishli bo‘lgan **Защита от вирусов и шпионских программ, съемные носители, HIPS** oynalarida quyidagi rasmlarda keltirilgan sozlamalarni amalga oshirib olamiz.



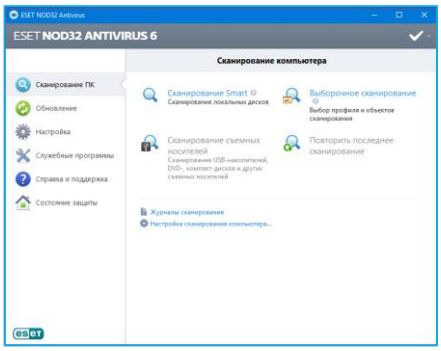


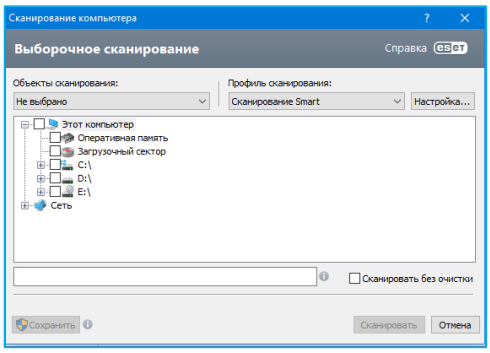




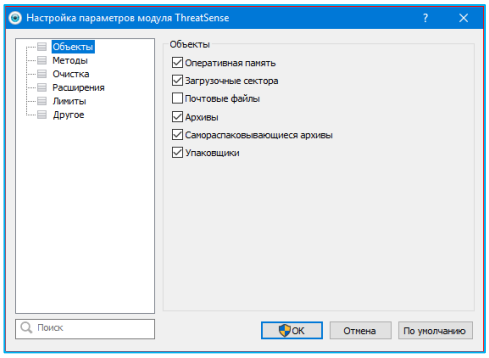
Sozlamalar yakunlangandan so‘ng endi kompyuterimizni to‘lliq tekshiruvdan **Сканировать ПК** bo‘limidan o‘tkazib olamiz. Bu bo‘lim kompyuetrni barcha disklarini, sektorlarini viruslardan tekshirib agarda virus topilsa ularni bartaraf qilib beradi. Demak yuqoridagi amallar quyidagi tartibda bajariladi.

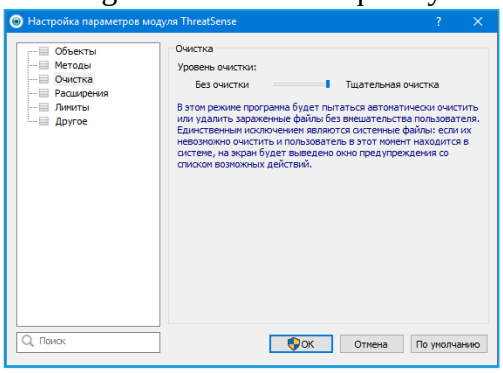
Birinchi navbatda **Сканировать ПК** bo‘limi ochiladi va **Выброчное сканирование** qisni tanlanadi. Keyingi bajaradigan ishimiz ochilgan oynadan **Профиль сканирования** bo‘limidan **Деталбное сканирование** bandi tanlanadi. So‘ngra **Этот компьютер** old tomoniga mayoqcha belgisi o‘rnatilib **Настройка** tugmasini bosamiz.



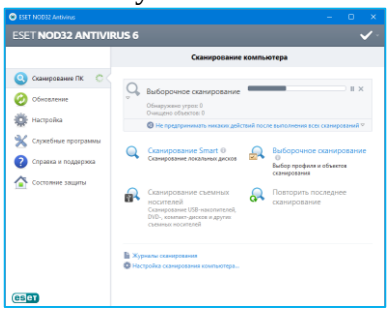


Ochilgan **Настройка** oynasidan **Очистка** undan so‘ng **Уровень очистки** oynasidagi rolikni **Тщательная очистка** tomon suramiz va **OK** tugmasini bosib tasdiqlab oynani yopamiz.





Har gal kompyuterni to‘liq antivirus tekshiruvdan o‘tkazganimizda yuqoridagi sozlamalarni qaytadan bajarmasligimiz uchun **Сохранить** so‘ngra **Сканировать** tugmasini bosib kompyuterni antivirusda tekshirishni boshlaymiz. Bu amal biro z vaqtni o‘z ichiga oladi.



Amaliy mashg’ulotlarini o‘tkazish qoidalari va xavfsizlik choralari.

Berilgan nazariy ma’lumot bilan tanishib chiqiladi va topshiriqlar variantlari ketma – ket bajariladi va natijalar olinadi.

Kompyuter xonasida xavfsizlik texnikasi qoidalari va sanitariya – gigiyena talablariga amal qilinadi.

Topshiriqlar variantlari (masala, misol, keyslar).

1. ESET NOD32 dasturini internet tarmog’i orqali yuklab oling va dasturni kompyuterga o‘rnating.

2. Antivirus ESET NOD32 dasturi to‘laligicha kompyuter xotirasiga o‘rnatilgandan so‘ng dasturning bazaviy holatini yangilang.

3. ESET NOD32 dasturi sozlamalarini amalga oshiring.

4. ESET NOD32 dasturi orqali shaxsiy kompyuter xotirasidagi mavjud viruslarni izlab toppish va ularnin zararsizlantiruvchi skanerdan o‘tkazing.

Nazorat savollari.

1. Axborot xavfsizligi haqida tushuncha bering.
2. Axborot xavfsizligiga tahdid turlari qanday?
3. Login tushunchasi va Parol tushunchasi.
4. Axborot xavfsizligining tabiiy va suniy tahdidlari haqida tushuncha bering qaysilar.
5. Avtorizatsiya haqida tushuncha bering.
6. Qanday antivirus turlari mavjud?