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

SAMARQAND DAVLAT VETERINARIYA MEDITSINASI, CHORVACHILIK VA BIOTEXNOLOGIYALAR UNIVERSITETI

Axborot texnologiyalari va tabiiy fanlar kafedrasi o‘qituvchisi

Ravshanov Sanjar Tolibjonovichning

Agrotexnologiya fakulteti
Agronomiya (yem-xashak ekinlari) yo‘nalishi
1-bosqich 103-guruh talabalari uchun
Sohada axborot kommunikatsiya texnologiyalari fanidan

Axborot xavfsizligi mavzusidagi

LABORATORIYA MASHG‘ULOTI ISHLANMASI

Samarqand 2024

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

Taqrizchilar:
H.O‘.Akbarov – Samarqand agroinnovatsiyalar va tadqiqotlar instituti, Raqamli texnologiyalar va buxgalteriya hisobi kafedrasi mudiri, i.f.f.d., dotsent v.b.

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

Laboratoriya mashg‘ulotining texnologik xaritasi.

Talabalar soni 19	2 soat
Mashg‘ulot shakli	Laboratoriya mashg‘ulot.
Laboratoriya mashg‘ulot rejasi	10.1. Axborot xavfsizligi. 10.2. Axborotlarni himoyalashning texnik va dasturiy vositalari. 10.3. Axborotlarni himoyalash usullari.
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, laboratoriya ish bajarish.
O‘qitish vositalari	Doska, videoproyektor, topshiriqlar, tarqatma materiallar, kompyuterlar.
O‘qitish shakllari	Frontal, kollektiv,
O‘qitish sharoiti	Kompyuter bilan ta’minlangan auditoriya.
Monitoring va baholash	Kuzatish, og‘zaki baholash, savol- javob, kompyuterda laboratoriya ish bajarishiga qarab.

T/r	Mashg‘ulot bosqichlari	Ajratilgan vaqt	Mashg‘ulot mazmuni	Ta’lim metodlari	Ta’lim vositalari
1.	**Tashkiliy qism.**	**5**	Salomlashish. Yo‘qlama qilish. Guruh tayyorgarligini tekshirish, xona tozalagini tekshirish	Kuzatuv	Doska, mel, kompyuter daftarlar
2.	**Kirish qismi (motivasiya).**	**10**	O‘quvchilarga axborotlarni himoyalashning muhimligi haqida tushunchalar berish.	Baholash mezoni Insert	Kompyuter
3.	**Yangi mavzuni bayoni.**	**30**	Axborot xavfsizligi. Axborotlarni himoyalash usullari bilan tanishtirish ishlari olib boriladi.	Kompyuter	Tarqatma materiallar, doska, kompyuter
4.	**Mustahkamlash (qo‘llash).**	**30**	Talabalarga yangi mavzu bo`yicha vazifalar topshirilib. Vazifalar asosida mavzu mustaxkamlanadi, o`quvchilar baholanadi.	Mavzuni mustaxkamlash uchun savollar.	Kompyuter doska, bor
5.	**Yakuniy qism.**	**5**	Uyga vazifa: Bugungi yangi mavzuni mustahkamlash va qo‘shimcha ma’lumotlar topish.		

10- Laboratoriya mashg‘ulot

Mavzu: Axborot xavfsizligi

Reja:

4. Nazariy qism.

10.1. Axborot xavfsizligi.

10.2. Axborotlarni himoyalashning texnik va dasturiy vositalari.

10.3. Axborotlarni himoyalash usullari.

5. Laboratoriya qism.

1- Laboratoriya ish.

2- Laboratoriya ish.

6. Mavzuni mustahkamlash uchun savollar.

1. Laboratoriya mashg‘ilotning maqsadi: Axborot xavfsizligi haqida tushunchaga ega bo‘lish. Virus va antivirus turlari bilan ta’nishish, Axborotlarni himoyalash usullarini o‘rganish.

2. Laboratoriya mashg‘ilot uchun qo‘llaniladigan texnik vositalar: Zamonaviy kompyuterlar; kompyuter tarmoqlari, videoproektor; Antivirus dasturlari;

3. Tayanch tushunchalar:

Axborot xavfsizligi – axborotni ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o‘zgartirish, tadqiq qilish, yozib olish yoki yo‘q qilishning oldini olish amaliyotidir.

Kodlashtirish – axborotni bir tizimdan boshqa tizimga ma’lum bir belgilar yordamida belgilangan tartib bo‘yicha o‘tkazish.

Kriptografiya – maxfiy xabar mazmunini shifrlash, ya’ni malumotlarni maxsus algoritm bo‘yicha o‘zgartirib, shifrlangan matnni yaratish yo‘li bilan axborotga ruxsat etilmagan kirishga to‘siq qo‘yish.

Kompyuter virusi – maxsus yozilgan dastur bo‘lib, kompyuterda ishlashda barcha mumkin bo‘lgan xalaqitlarni yaratish, fayl va kataloglarni buzish, dasturlarni ishdan chiqarish maqsadida hisoblash tizimlariga, kompyuterning tizimli sohalariga, fayllarga tadbiq qilinadigan, o‘zlarining nusxalarini yaratish, boshqa dasturlarga o‘z-o‘zidan birikib oladigan maxsus dastur.

4. Nazariy qism.

10.1. Axborot xavfsizligi.

Axborot-kommunikasiya texnologiyalari turli xil axborotlarni saqlash, uzatish, uni qayta ishlash, natijalarni foydalanuvchilarga matn, grafik, ovoz shaklida taqdim etish, ma’lumolar bazasi tizimlari va boshqa masalalarni yechish uchun vosita hisoblanadi.

Axborot xavfsizligini ta’minlash muammolarining dolzarbligi va muhimligiga quyidagilar sabab bo‘lmoqda:

- zamonaviy kompyuterlar hisoblash quvvatining kun sayin oshib borishi;

• Kompyuterlar yordamida to‘planayotgan, saqlanayotgan, ishlanayotgan va uzatilayotgan axborotlarning lokal va global tarmoqlardan foydalanishning keskin o‘sishi;

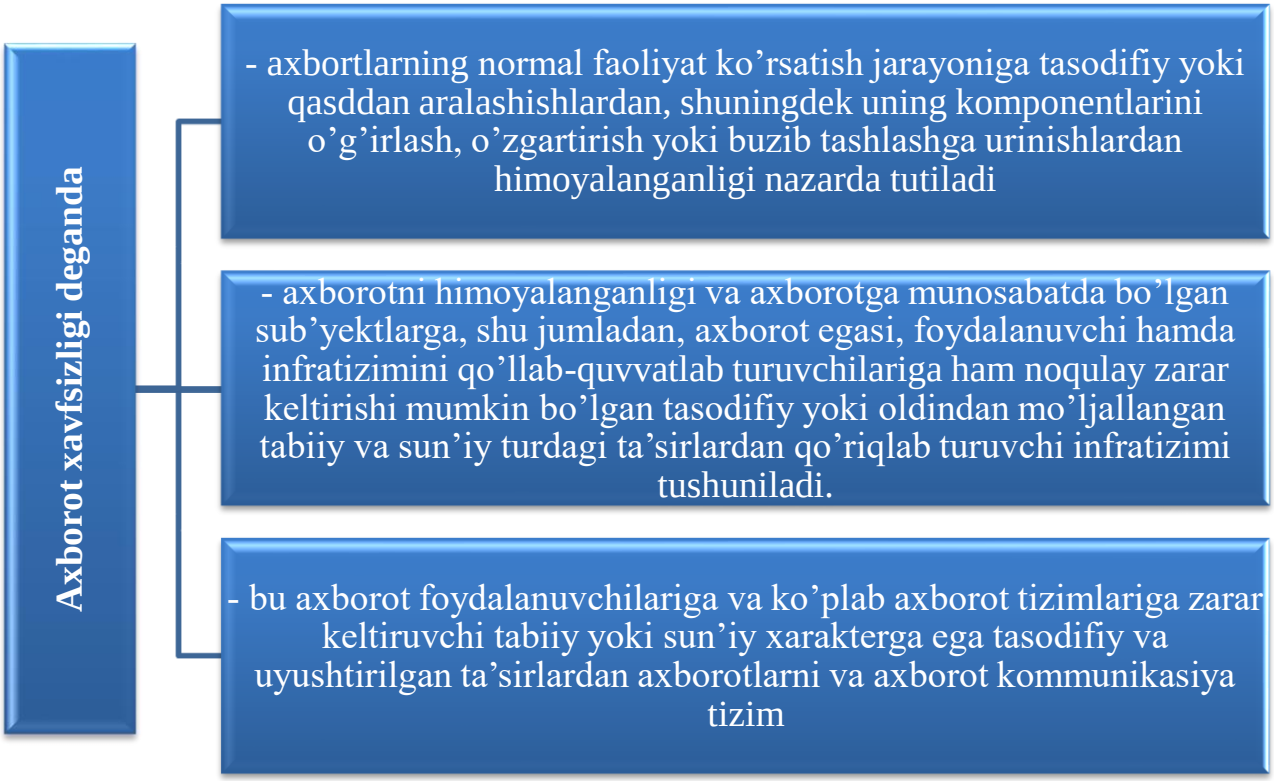
• serverlarda turli sohaga oid ma’lumotlarning bazasi sifatida jamlanganligi;

• turli predmet sohalarida ishlatilayotgan Kompyuterlar sonining keskin o‘sishi; hisoblash zahiralari va ma’lumot massivlariga bevosita kirish imkoniga ega bo‘lgan foydalanuvchilar doirasining keskin kengayib borayotgani;

• minimal darajadagi xavfsizlik talablariga ham javob bera olmayotgan dasturiy vositalarning mavjudligi;

• tarmoqli texnologiyalarning hamma joyga tarqalishi va lokal tarmoqlarning globallashuvi;

• Internet tarmog‘idan foydalanuvchilar sonining tez suratlar bilan oshishi.



Axborot tizimlariga ta’sir ko‘rsatishlar tabiati nihoyatda turli-tuman bo‘ladi. Bular tabiiy ofatlar (yer qimirlashlar, bo‘ronlar, yong‘inlar) ham, axborot xavfsizligi tarkibiy qismlarining ishdan chiqishlari ham, xodimlar yo‘l qo‘ygan xatolar ham, suiqasdchining kirishga bo‘lgan intilishlari ham bo‘lishi mumkin.

Axborot xavfsizligiga ishlanayotgan axborotning maxfiyligi va butligini, shuningdek tizimning tarkibiy qismlari va zahiralarining butligini ta’minlash bo‘yicha choralar ko‘rish orqali erishiladi.

Ma’lumotlarning maxfiyligi bu ushbu ma’lumotlarga taqdim etilgan va ularning talabdagi himoyasini belgilab beradigan maqomdir. Mohiyat e’tibori bilan axborot maxfiyligi bu axborotning faqatgina tekshiruvdan o‘tgan va kirish huquqiga ega bo‘lgan tizim sub’yektlariga ma’lum bo‘lish xususiyatidir.

Sub’yekt tizimning faol tarkibiy qismi bo‘lib, axborotlarning ob’yektdan sub’yektga oqib o‘tishining yoki tizim holati o‘zgarib ketishining sababchisi bo‘lishi mumkin. Ob’yekt esa tizimning axborotlarni saqlovchi, qabul qiluvchi yoki

uzatuvchi passiv tarkibiy qismidir. Ob'yektga murojaat unda saqlanayotgan axborotlarga murojaatni bildiradi.

Tizimdagi ma'lumotlar ma'no jihatdan dastlabki ma'lumotlardan farq qilmasa, ya'ni ular tasodifiy yoki qasddan qilingan ma'no o'zgartishlar yoki buzilishlarga uchramagan bo'lsagina, axborot butligi ta'minlangan hisoblanadi.

Tasodifiy yoki qasddan qilingan buzib ko'rsatishlar yoki buzib tashlovchi ta'sirlar sharoitida ishlayotgan tizim o'z tarkibiy qismi yoki zahirasini ma'no jihatdan o'zgartirmasa, bu hol ushbu tizim o'z tarkibiy qismi yoki zahirasining butligini saqlab qolish xususiyatiga ega ekanligidan darak beradi.

Tizimning tarkibiy qismi yoki zahirasining kirish uchun qulayligi deganda ushbu tarkibiy qism yoki zahiraning muallifi ma'lum bo'lgan qonuniy tizim sub'yektlari uchun kirishga qulayligi nazarda tutiladi.

Axborot xavfsizligiga tahdid deganda uning xavfsizligiga bevosita yoki bilvosita zarar yetkazishi mumkin bo'lgan barcha ehtimoliy ta'sirlar tushuniladi. Xavfsizlikka zarar yetkazish deganda Axborot xavfsizligida saqlanayotgan va ishlanayotgan axborotlarning himoyalanganlik holati buzilgani tushuniladi.

Axborot xavfsizligi zaifligi bu tizimning biron bir qoniqarsiz xususiyati bo'lib, u tahdidning paydo bo'lishi va amalga oshishini keltirib chiqarishi mumkin.

Kompyuter tizimiga xujum deganda buzg'unchining tizimdagi u yoki bu zaif jihatlarni izlab topib, ulardan o'z niyatida foydalanishga qaratilgan xatti-harakatlari nazarda tutiladi.

Axborotlarga ishlov berish tizimlarini himoya qilishda maqsad ularning xavfsizligiga tahdidlarning oldini olishdan iborat.

Xavfsiz yoki himoyalangan tizimlar deb xavfsizlikka tahdidlarga muvaffaqiyatli va samarali qarshi tura oladigan himoya vositalariga ega bo'lgan tizimlarga aytiladi.

Xavfsizlik siyosati deganda xavfsizlikka tahdidlarning ma'lum bo'lgan barcha turlaridan Axborot xavfsizligini himoyalash vositalari ishini boshqarib turuvchi me'yorlar, qoidalar va amaliy ko'rsatmalar majmui tushuniladi.

10.2. Axborotlarni himoyalashning texnik va dasturiy vositalari

Funksional vazifasiga ko'ra axborotlarni muhandis-texnik himoyalash vositalari quyidagi guruhlarga ajratiladi:

1. Fizik vositalar. Bu vositalarga mexanik, elektromexanik, elektron, elektron-optik, radio- va radiotexnik va boshqa qurilmalar mansub bo'ladi. Bu

vositalarning vazifasi axborotlarga ruxsatsiz kirishni va tajouzkorlikni boshqa mumkin bo‘lgan harakatlarni oldini olishdan iborat.

Bu vositalar quyidagi vazifalarni amalga oshirish uchun qo‘llaniladi:

- korxona hududini qo‘riqlash va uni kuzatish uchun;
- binolarni qo‘riqlash va uni nazorat qilish uchun;
- jihozlarni, mahsulotlarni, moliyaviy natijalar va axborotlarni qo‘riqlash uchun;
- bino va inshoatlarni nazorat qiluvchi vositalarga kirishni himoya qilish uchun.

Fizik vositalar- mexanik, elektromexanik, elektron, elektron-optik, radio- va radiotexnik va boshqa qurilmalar

- **Vazifalari:**
- korxona hududini qo’riqlash va uni kuzatish;
- binolarni qo’riqlash va uni nazorat qilish;
- jihozlarni, mahsulotlarni, moliyaviy natijalar va axborotlarni qo’riqlash;
- bino va inshoatlarni nazorat qiluvchi vositalarga kirishni himoya qilish

Barcha ob’yektlarni himoya qilishni fizik vositalarini uchta kategoriyaga ajratish mumkin: ogohlantirish vositalari (ob’yekt o‘ralgan devorlar); tahdidni aniqlash vositalari (signalizasiya va kuzatish uchun o‘rnatilgan televizorlari) va tahdidni bartaraf qilish tizimlari (o‘t o‘chirish vositalari)

Umuman olganda bu kategoriyalarni quyidagi guruhlarga ajratish mumkin:

- qo‘riqlash va qo‘riqlash-o‘t o‘chirish tizimlari;
- qo‘riqlash televizorlari;
- qo‘riqlash yoritgichlari;
- fizik himoyalash vositalari;
- apparat vositalari.

2. Axborotlarni himoyalashni apparat vositalari

Axborotlarni himoyalashni apparat vositalari quyidagi vazifalarni amalga oshirishga imkoniyat beradi:

- axborotni ruxsatsiz chiqib ketish kanallarini aniqlash maqsadida texnik vositalarni maxsus tekshiruvlardan o‘tkazish;
- turli hil ob’yektlarni axborotlarni ruxsatsiz chiqib ketish kanallarini aniqlash;
- axborotni ruxsatsiz chiqib ketishi aniqlangan kanallarini lokallashtirish (ajratib olish);
- sanoat shipionaji vositalarini qidirish va aniqlash;
- konfidensial bo‘lgan axborotlar va boshqa manbalarga ruxsatsiz kirishga qarshi harakatlarning konfidisial bo‘lishi.

3. Dasturiy vositalar. Axborotlarni dasturiy himoyalash – bu axborotlarni himoya qilish vazifasini amalga oshiruvchi maxsus dasturlar tizimidir. Konfidensial axborotlarning xavfsizligini ta’minlovchi dasturlari quyidagi yo‘nalishlarga ajratilib ko‘rsatiladi:

- axborotlarni ruxsat berilmagan kirishlardan himoyalash;
- axborotlarni nusxa olishdan himoyalash;
- axborotlarni viruslardan himoyalash;
- aloqa kanallarini dasturiy himoyalash

Dasturiy vositalar

- **Axborotlarni dasturiy himoyalash** – bu axborotlarni himoya qilish vazifasini amalga oshiruvchi maxsus dasturlar tizimidir
- **Vazifalari:**
- axborotlarni ruxsat berilmagan kirishlardan himoyalash;
- axborotlarni nusxa olishdan himoyalash;
- axborotlarni viruslardan himoyalash;
- aloqa kanallarini dasturiy himoyalash

Axborotlarni ruxsat berilmagan kirishlardan himoyalashni dasturiy vositalarini bajaradigan funksiyalari quyidagilardan iborat bo‘ladi:

1. ob’yektlar va sub’yektlarni identifikasiyalash;
2. hisoblash resurslari va axborot resurslariga kirishga cheklovlar o‘rnatish;
3. axborot va dasturlar bilan bo‘ladigan harakatlarni nazorat va registrasiya qilish.

Axborotlarni himoyalashni apparat vositalari

- **Vazifalari:**
- axborotni ruxsatsiz chiqib ketish kanallarini aniqlash maqsadida texnik vositalarni maxsus tekshiruvlardan o’tkazish;
- turli hil obyektlarni axborotlarni ruxsatsiz chiqib ketish kanallarini aniqlash;
- axborotni ruxsatsiz chiqib ketishi aniqlangan kanallarini lokallashtirish (ajratib olish);
- sanoat shipionaji vositalarini qidirish va aniqlash

10.3. Axborotlarni himoyalash usullari

Kompyuter tizimlari va tarmoqlarida axborotni himoya qilishning **tashkiliy**, **xuquqiy** va **texnik** usullari mavjud.

Axborotni himoya qilishning xuquqiy usullari, ixtiyoriy vazifali himoya qilish tizimini rasmiy ravishda ko‘rish va ishlatishning asosi bo‘lib xizmat qiladi.

Axborotni himoya qilishning xuquqiy usullari
• kompyuter jinoyatchiligi uchun jazolash me’yorlarini ishlab chiqish; dastur tuzuvchilarning mualliflik xuquqlarini himoya qilish; jinoiy va fuqarolik qonunchiligi sohasida sud ishini mukammallashtirish; kompyuter tizimlarini ishlab chiquvchilar ustidan jamoat nazoratini o’rnatish hamda mos halqaro shartnomalarni qabul qilish va h.k

Tashkiliy usullar bir nechta xavflarni bartaraf etish uchun ishlatilsa, texnik usullar tashkiliy va texnik tadbirlarga asoslangan holdaa ko‘pchilik axborotlarni himoya qiladi.

Axborotni himoya qilishning tashkiliy usullari
• kompyuter tizimlarini qo’riqlash; xodimlarni tanlab olish; O’ta muhim ishlarni faqat bitta odam tomonidan olib borilishi holatlarini inkor qilish; ishdan chiqqandan keyin tizimni tiklash rejasining mavjudligi; axborot xavfsizligi tizimini ta’minlaydigan shaxslarga javobgarlikni berish; kompyuter markazini o’rnatishga joy tanlash va h.k

Axborotni himoya qilishning texnik usullari apparatli, dasturli va apparat-dasturliga bo‘linadi. Texnik usullarda quyidagi harakterdagi masalalar ko‘rib chiqiladi: kompyuter tizimlari va tarmoqlarida axborotga ruxsatsiz murojaat qilishdan himoya etish; virusdan himoya qilish; elektrmagnit, akustik maydon va nurlanishlar orqali «ushlab» olishni bartaraf etish; kriptografik usul asosida xabarlarni yuqori darajada yopiqligini

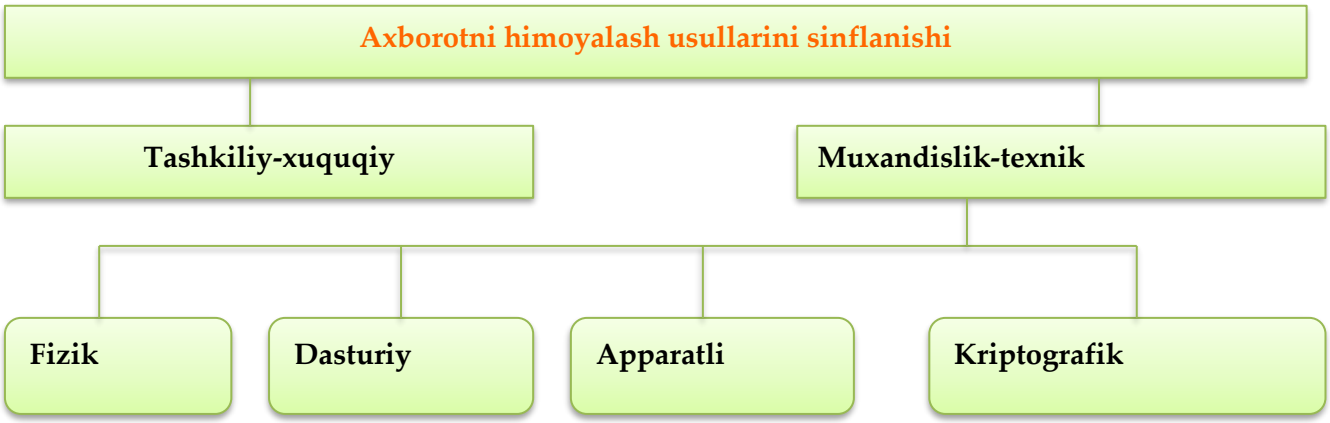
Kriptografik vositalar
• **Kriptografik vositalar**-tizim va tarmoq bo’yicha uzatiladigan, EHMlarda saqlanadigan va turli xil usullar bilan shifrlanadigan axborotlarni himoya qilishning maxsus matematik va algoritm vositalaridir

Identifikasiya va autentifikasiya masalalari

Autentikasiya

Autentikasiya, deganda sub’yekt tomonidan taqdim qilingan identifikatorni unga mansub ekanligini tekshirish va uning xaqiqiy ekanligini tasdiqlash. Autentikasiya - axborot zaxirasi kim ekanliligini o‘rnatish. Boshqacha so‘z bilan

aytganda autentikasiya: axborot resurslariga kirmoqchi bo‘lgan sub’yektning identifikatorini unga mansubligini tekshirishni ifodalaydi.



Odatda autentifikasiya metodlari qo‘llaniladigan vositalariga binoan sinflanadi. Bu holatda ko‘rsatilgan metodlar to‘rtta guruhga ajratiladi:

1. Tizim resurslariga kirish huquqiga, ayrim sirli axborotlarga (parol) ega bo‘lish kabi, shaxsning bilimga asoslanish;
2. Jeton, elektron karta, plastik karta va boshqa shu kabilar, unikal predmetlarga asoslanish;
3. Tirik organizimlarning fiziologik atributlarini hisoblangan insonning biometrik parametrlari o‘lchashlarga asoslanish;
4. Foydalanuvchi xaqidagi axborotlarga asoslanish.

Axborotlarni himoyalashda birinchi navbatda eng keng qo‘llanilgan dasturiy vositalar hozirgi kunda ikkinchi darajali himoya vositasi hisoblanadi. Bunga misol sifatida parol tizimini keltirish mumkin.

Identifikasiya

- **Sub’yekt va obyektlarga kirish uchun shaxsiy identifikatorni berish va uni identifikatorda berilganlar bilan solishtirish identifikasiya deyiladi.**
- **Identifikasiya quyidagi funksiyalarni bajarilishini ta’minlaydi:**
- **sub’yektni haqiqiyligini aniqlash va sub’yektni tizimga kirishda vakolatini aniqlash;**
- **ishlash seansi jarayonida o’rnatilgan vakolatlarni nazorat qilish;**
- **harakatlarni registrasiya qilish va bosh**

Bevosita tarmoq bo‘yicha uzatiladigan ma’lumotlarni himoyalash maqsadida quyidagi tadbirlarni bajarish lozim bo‘ladi: uzatiladigan ma’lumotlarni ochib o‘qishdan saqlanish; uzatiladigan ma’lumotlarni tahlil qilishdan saqlanish; uzatiladigan ma’lumotlarni o‘zgartirishga yo‘l qo‘ymaslik va o‘zgartirishga urinishlarni aniqlash; ma’lumotlarni uzatish maqsadida qo‘llaniladigan dasturiy uzilishlarni aniqlashga yo‘l qo‘ymaslik; firibgarlik yo‘li ulanishlarning oldini olish.

Ushbu tadbirlarni amalga oshirishda asosan kriptografik usullar qo‘llaniladi. Axborotni himoyalash uchun **kodlashtirish** va **kriptografiya** usullari qo‘llaniladi.

Kodlashtirish deb axborotni bir tizimdan boshqa tizimga ma’lum bir belgilar yordamida belgilangan tartib bo‘yicha o‘tkazish jarayoniga aytiladi.

Kriptografiya deb maxfiy xabar mazmunini shifrlash, ya’ni malumotlarni maxsus algoritm bo‘yicha o‘zgartirib, shifrlangan matnni yaratish yo‘li bilan axborotga ruxsat etilmagan kirishga to‘siq qo‘yish usuliga aytiladi.

Stenografiyaning kriptografiyadan boshqa o‘zgacha farqi ham bor. Ya’ni uning maqsadi — maxfiy xabarning mavjudligini yashirishdir. Hozirgi vaqtda axborotni himoyalash eng ko‘p qo‘llanilayotgan soha bu — kriptografik usullardir. Kriptografiya nuqtai – nazaridan shifr — bu kalit demakdir va ochiq ma’lumotlar to‘plamini yopiq (shifrlangan) ma’lumotlarga o‘zgartirish kriptografiya o‘zgartirishlar algoritmlari majmuasi hisoblanadi.

Kalit — kriptografiya o‘zgartirishlar algoritmining ba’zi-bir parametrlarining maxfiy holati bo‘lib, barcha algoritmlardan yagona variantini tanlaydi. Kalitlarga nisbatan ishlatiladigan asosiy ko‘rsatkich bo‘lib kriptomustahkamlik hisoblanadi. Kriptografiya himoyasida shifrlarga nisbatan quyidagi talablar quyiladi: yetarli darajada kriptomustaxkamlik; shifrlash va qaytarish jarayonining oddiyligi; axborotlarni shifrlash oqibatida ular hajmining ortib ketmasligi; shifrlashdagi kichik xatolarga tasirchan bo‘lmasligi.

Ushbu talablarga quyidagi tizimlar javob beradi: o‘rinlarini almashtirish; almashtirish; gammalashtirish; analitik o‘zgartirish.

O‘rinlarini almashtirish shifrlash usuli bo‘yicha boshlang‘ich matn belgilarining matnning ma’lum bir qismi doirasida maxsus qoidalar yordamida o‘rinlari almashtiriladi.

Almashtirish shifrlash usuli bo‘yicha boshlangich matn belgilari foydalanilayotgan yoki boshqa bir alifbo belgilariga almashtirilali.

Gammalashtirish usuli bo‘yicha boshlang‘ich matn bel¬gilari shifrlash gammasi belgilari, ya’ni tasodifiy belgilar ketma-ketligi bilan birlashtiriladi.

Taxliliy o‘zgartirish usuli bo‘yicha boshlang‘ich matn belgilari analitik formulalar yordamida o‘zgartiriladi, masalan, vektorni matrisaga ko‘paytirish yordamida. Bu yerda vektor matndagi belgilar ketma-ketligi bo‘lsa, matrisa esa kalit sifatida xizmat qiladi.

O‘rinlarni almashtirish usullari. Ushbu usul eng oddiy va eng qadimiy usuldir. O‘rinlarni almashtirish usullariga misol sifatida quyidagilarni keltirish mumkin: shifrlovchi jadval; sehrli kvadrat. Shifrlovchi jadval usulida kalit sifatida quyidagilar qo‘llaniladi: jadval o‘lchovlari; so‘z yoki so‘zlar ketma-ketligi; jadval tarkibi xususiyatlari

Axborotni ximoyalashning maqsadlari kuyidagilardan iborat:

• axborotning kelishuvsiz chiqib ketishi, o‘g‘irlanishi, yuqotilishi, uzgartirilishi, soxtalashtirilishlarning oldini olish;

• shaxs, jamiyat, davlat xavfsizliligiga bo‘lgan xavf – xatarning oldini olish;

• axborotni yo‘q qilish, o‘zgartirish, soxtalashtirish, nusxa ko‘chirish, to‘siqlash bo‘yicha ruxsat etilmagan harakatlarning oldini olish;

• xujjatlashtirilgan axborotning miqdori sifatida xuquqiy tartibini ta’minlovchi, axborot zaxirasi va axborot tizimiga har qanday noqonuniy aralashuvlarning ko‘rinishlarining oldini olish;

• axborot tizimida mavjud bo‘lgan shaxsiy ma’lumotlarning shaxsiy maxfiyligini va konfidensialligini saqlovchi fuqarolarning konstitusion xuquqlarini himoyalash;

• davlat sirini, qonunchilikka mos hujjatlashtirilgan axborotning konfidensialligini saqlash.

Kompyuter tarmoqlariga ruxsatsiz ulanish, yovuzni harakatlar va tarmoqda ishlash qoidalarini buzish

Axborotlarga kirish deganda axborot bilan tanishish, unga ishlov berish, xususan undan nusxa ko‘chirish, uni modifikasiya qilish yoki yo‘q qilib tashlash tushuniladi.

Axborotlarga ruxsat etilgan va etilmagan kirishlar bilan farqlanadi.

Axborotlarga ruxsat etilgan kirish deganda kirishni chegaralashning belgilangan qoidalarini buzmaslik tushuniladi.

Kirishni chegaralash qoidalari kirish sub’yektlarining kirish ob’yektlariga kirishish huquqlarini belgilab beradi.

Axborotlarga ruxsat etilmagan kirish buning uchun belgilangan qoidalarni buzish demakdir. Axborotlarga ruxsat etilmagan kirishni amalga oshirayotgan shaxs yoki jarayon murojaatni chegaralash qoidalarining buzuvchilari hisoblanadi. Ruxsat etilmagan kirish kompyuter buzg‘unchiliklarining eng keng tarqalgan ko‘rinishidir.

Hozirgi kunda ma’lumotlarni ruxsatsiz chetga chiqib ketish yo‘llari quyidagilardan iborat: elektron nurlarni chetdan turib o‘qib olish;

• aloqa kabellarini elektromagnit to‘lqinlar bilan nurlatish; yashirin tinglash qurilmalarini qo‘llash; masofadan rasmga tushirish; printerdan chikadigan akustik to‘lqinlarni o‘qib olish; ma’lumot tashuvchilarni va ishlab chiqarish chiqindilarini o‘g‘irlash; tizim xotirasida saqlanib qolgan ma’lumotlarni o‘qib olish;

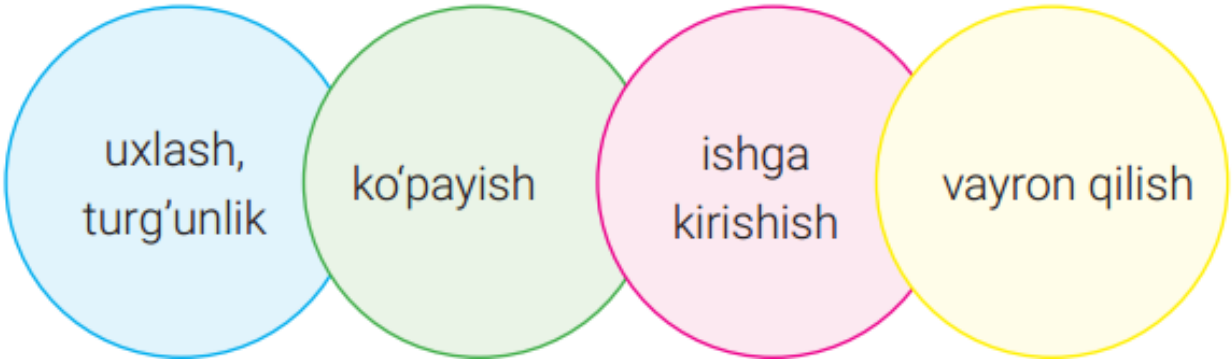
• himoyani yengib ma’lumotlarni nusxalash;

• qayd qilingan foydalanuvchi niqobida tizimga kirshi;

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.

Laboratoriya qism.

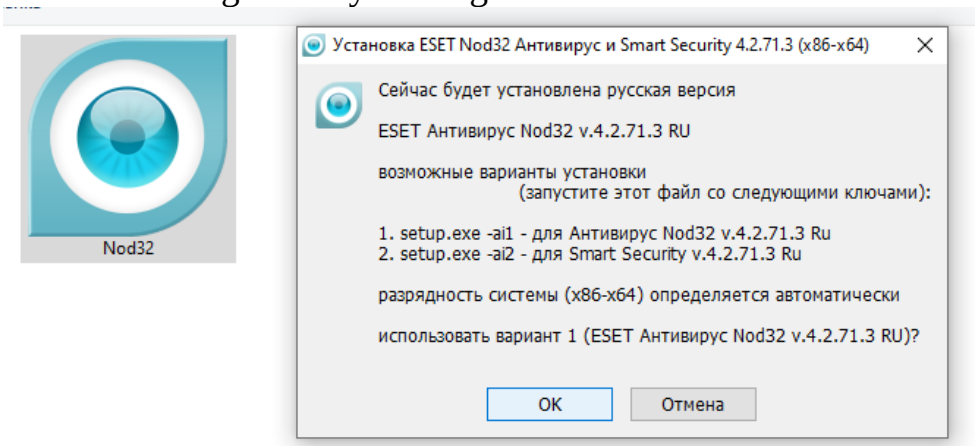
1- laboratoriya ish.

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

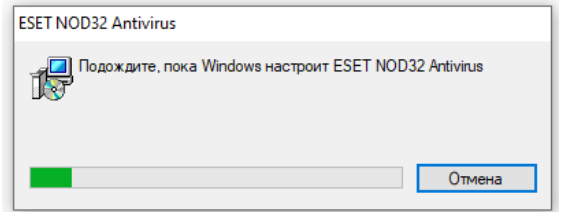
1-qadam.

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



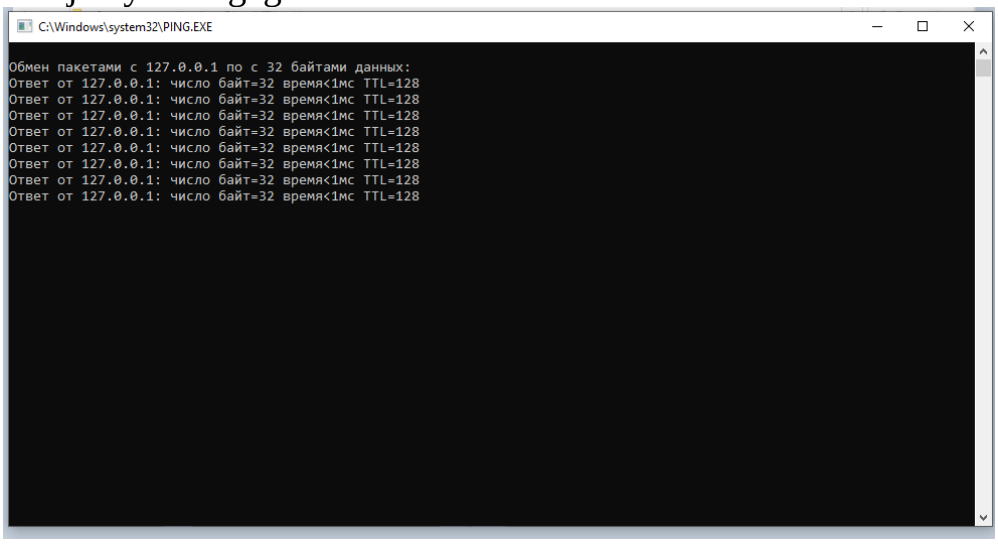
5.1-rasm.

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



5.2-rasm.

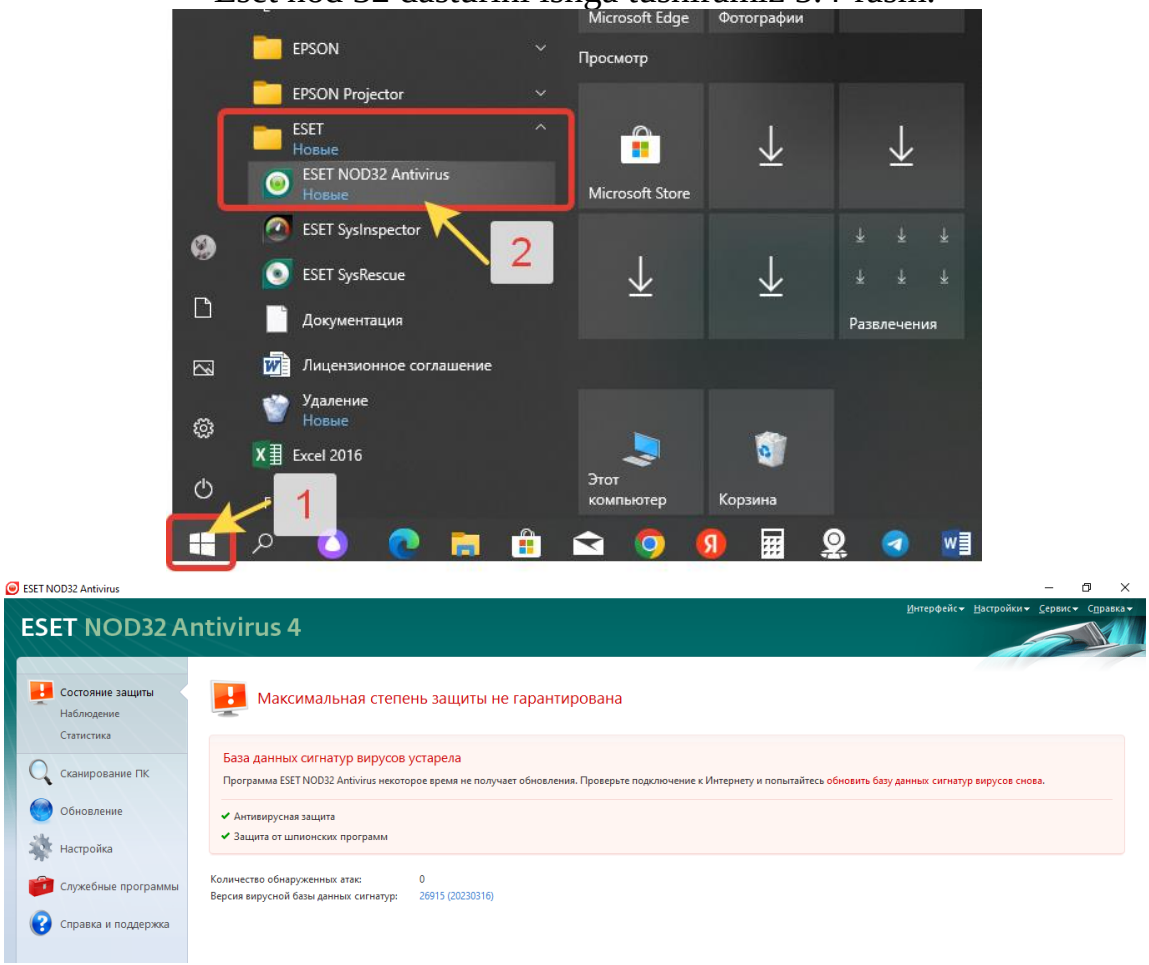
O‘rnatilish jarayoni tugaguncha kutamiz 5.3-rasm.



5.3-rasm.

2- qadam.

Eset nod 32 dasturini ishga tushiramiz 5.4-rasm.

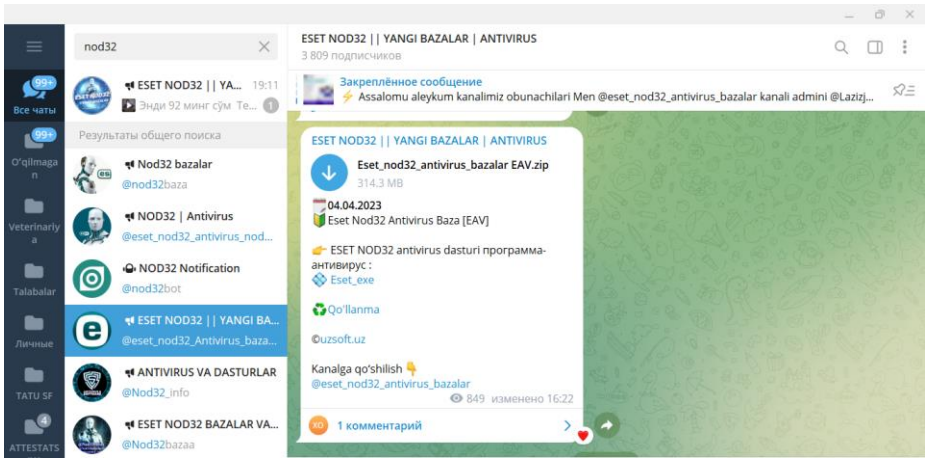


5.4-rasm.

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.

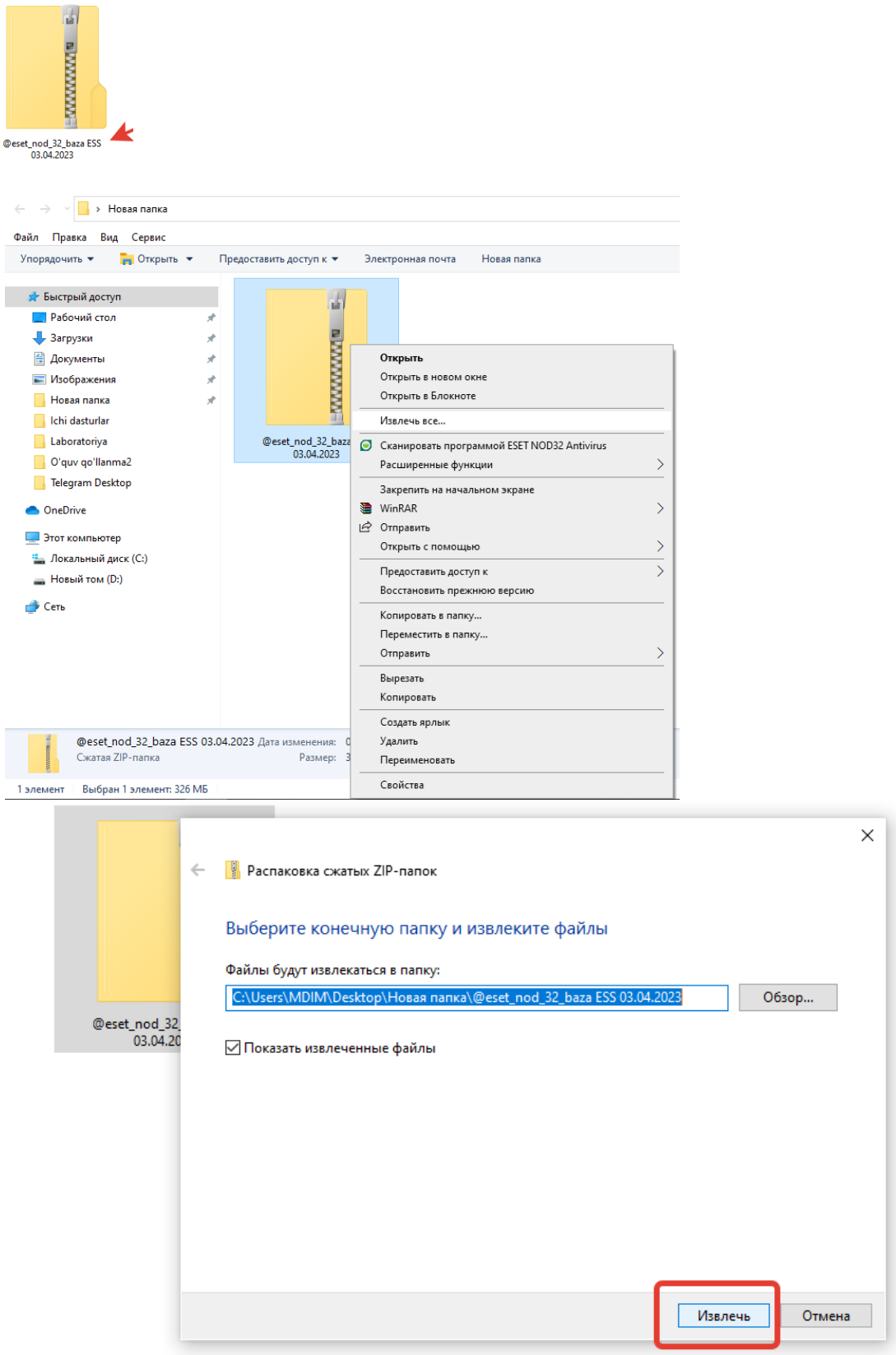
Eset nod 32 anitivirus dastunini bazasini telegramdagi t.me/eset_nod32_Antivirus_bazalar (https://t.me/eset_nod32_Antivirus_bazalar) kanalidan yuklab olishimiz mumkin 5.5-rasm.



5.5-rasm.

4-qadam.

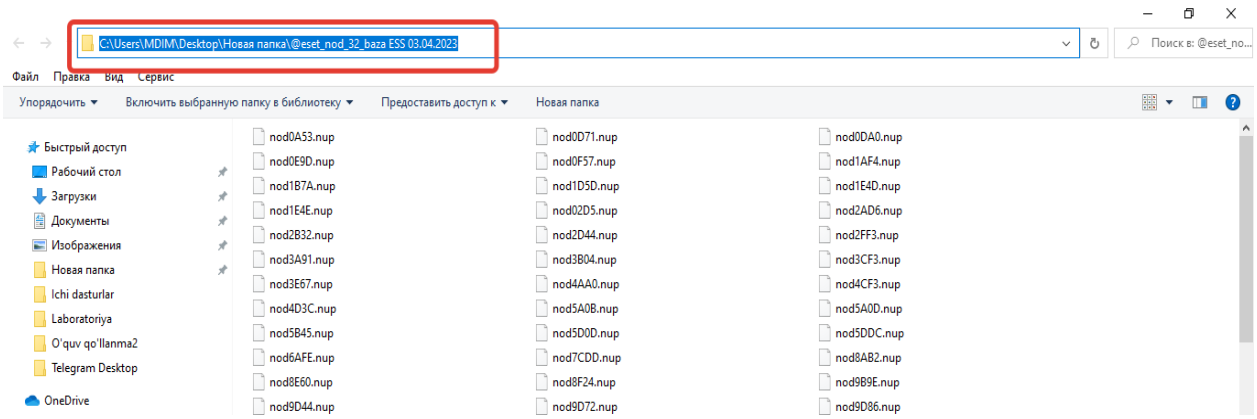
Eset nod 32 anitivirus dasturi bazasi arixivlangan papka ko‘rinishida bo‘ladi. Biz bu papkani arxivdan chiqarib olishimiz kerak 5.6-rasm.



5.6-rasm.

5-qadam.

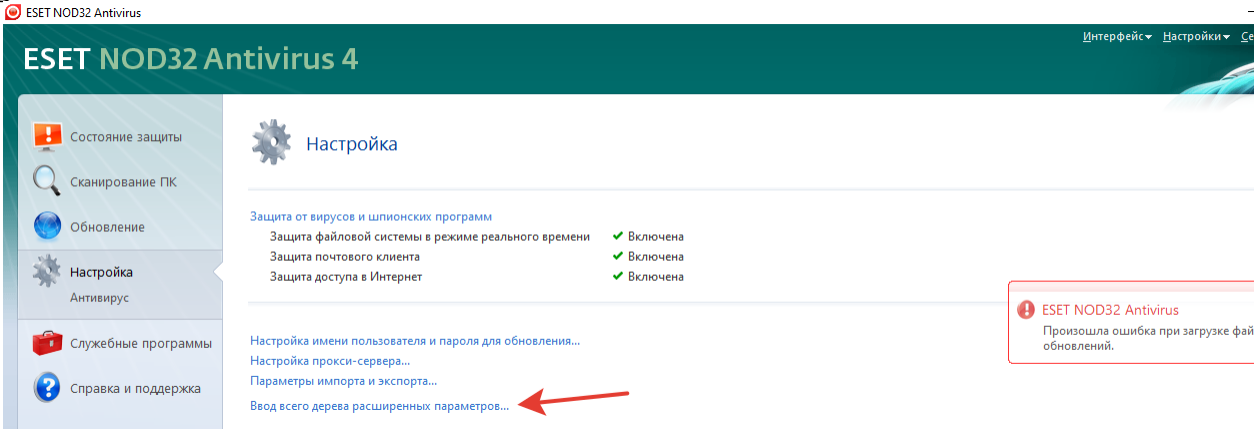
Arxivlangan papkadagi fayllar arxivdan chiqarilgandan so‘ng papka yuqorisidagi manzilni nusxalab olamiz. 10.7-rasm.



5.7-rasm.

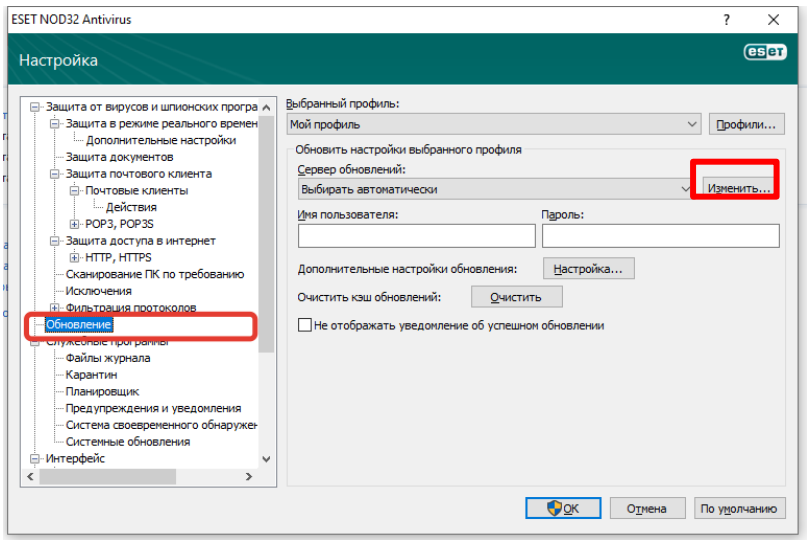
6-qadam.

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



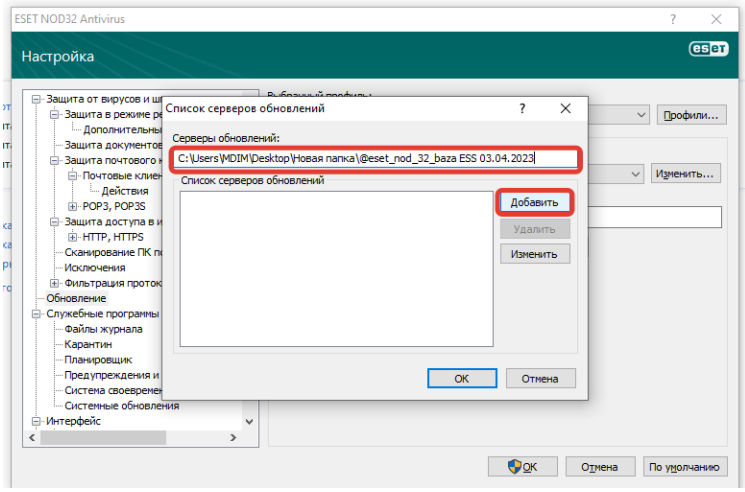
5.8-rasm.

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



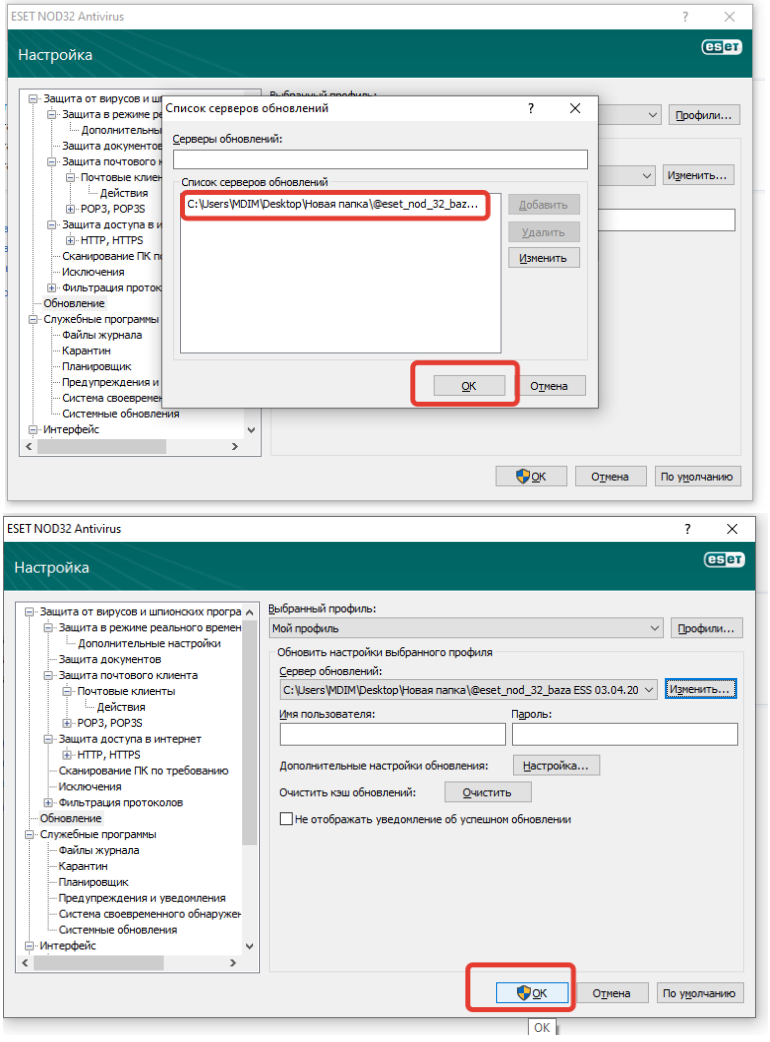
5.9-rasm.

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.

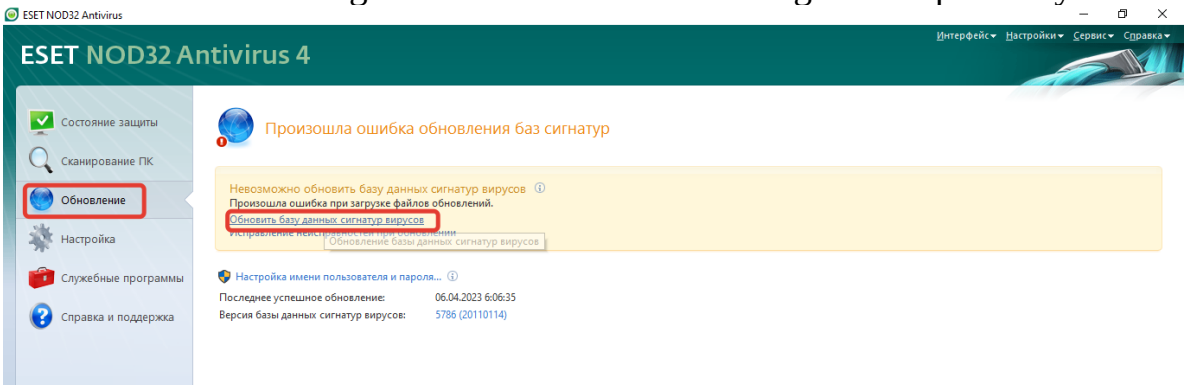
Natijada 5.11-rasm ko‘rinishiga o‘tadi va **ok** tugmalarini bosamiz.



5.11-rasm.

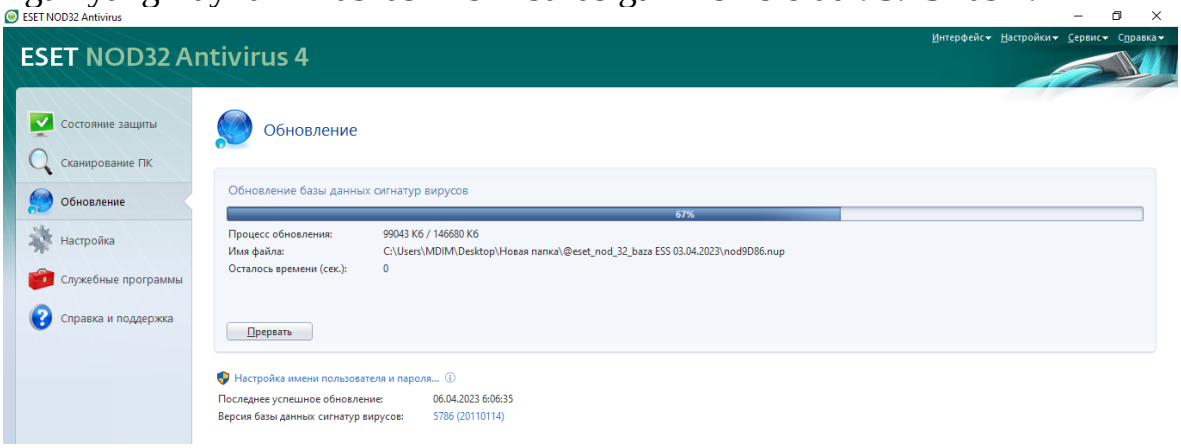
7-qadam.

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



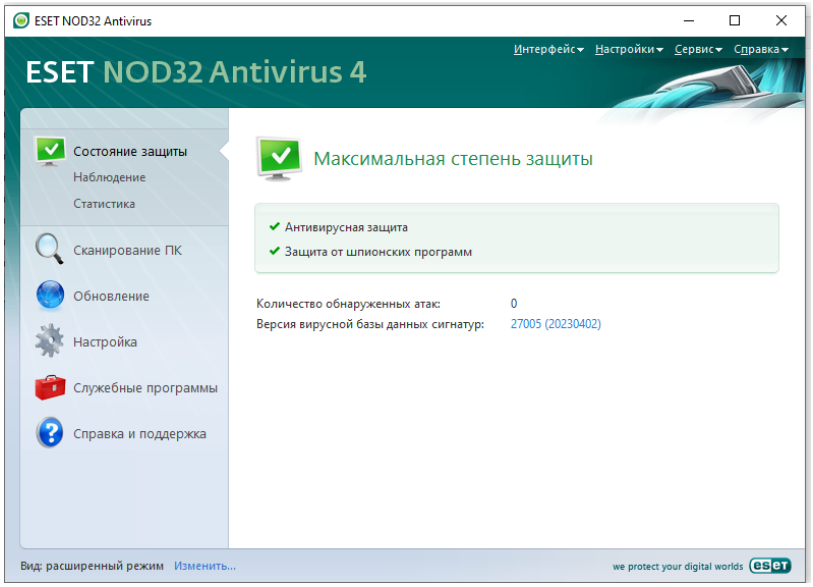
5.12-rasm.

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.

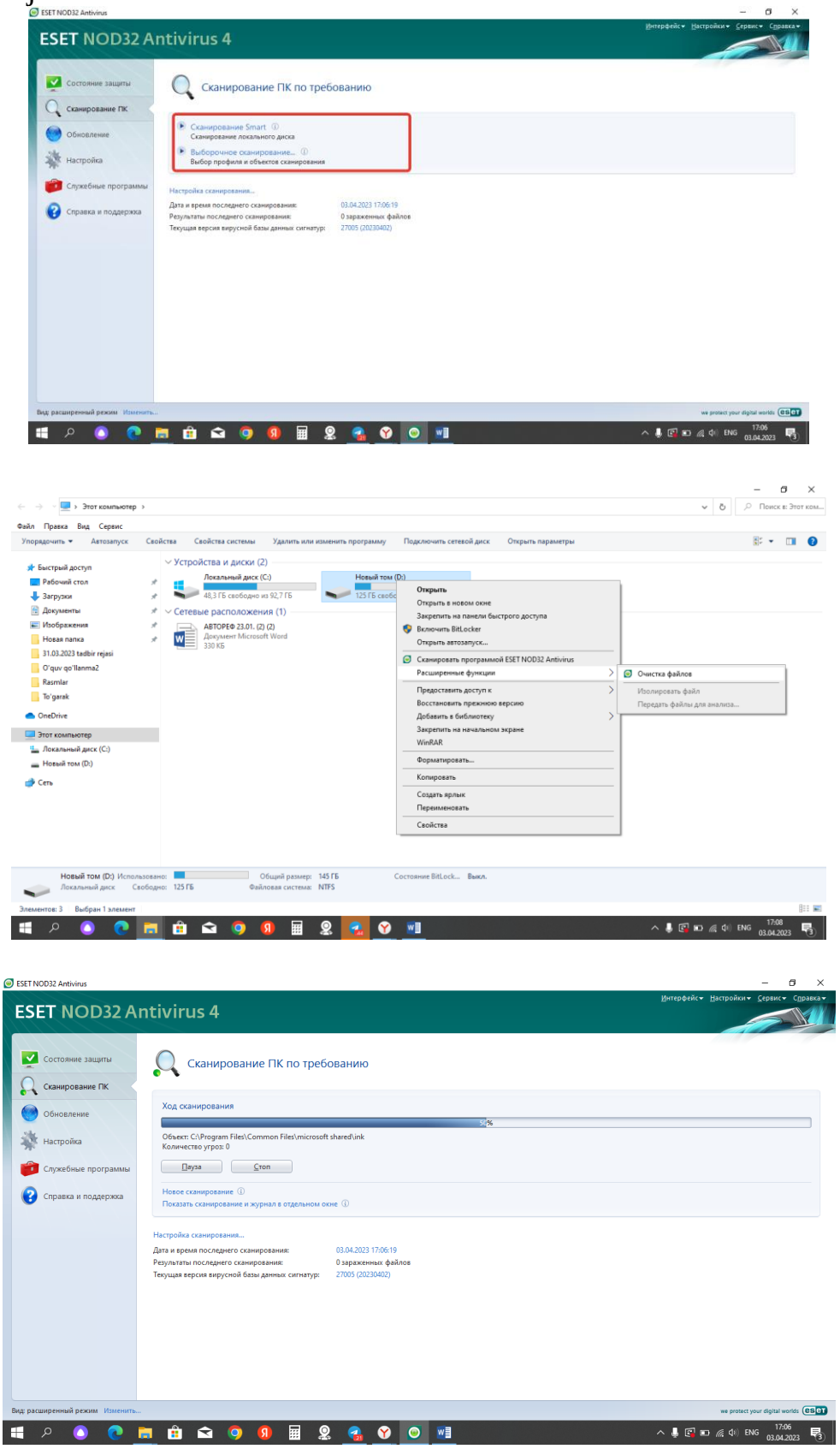
va nixoyat Eset nod 32 anitivirus dasturi maksimal darajada yangilanadi. 5.14-rasm.



5.14-rasm.

8-qadam.

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



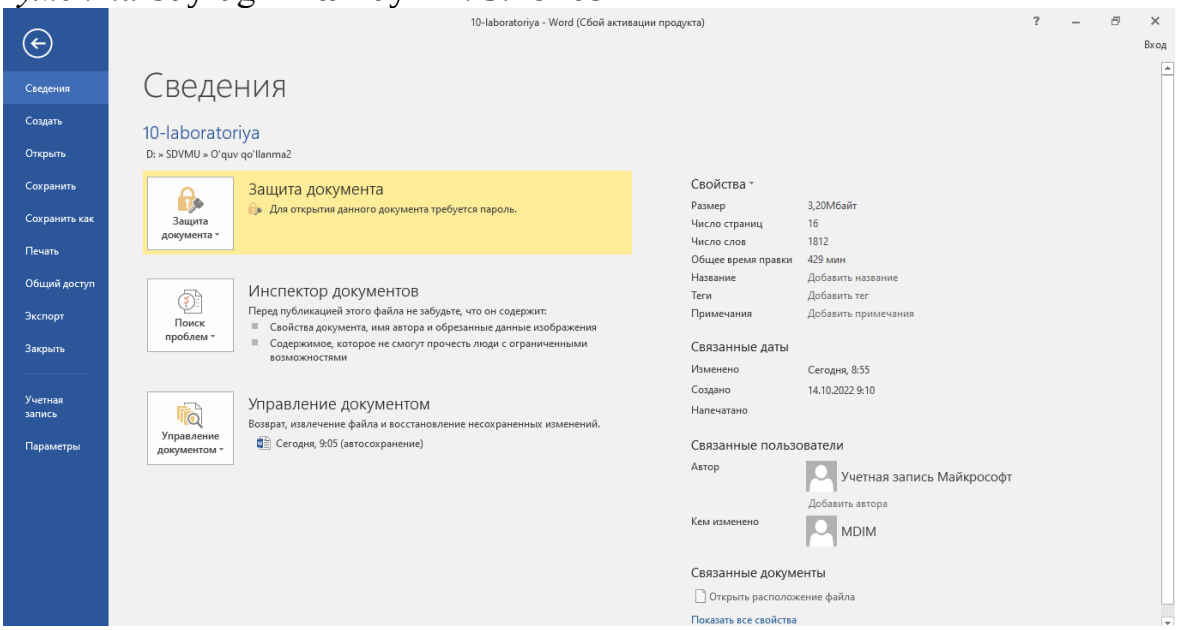
5.15-rasm

2- laboratoriya ish.

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

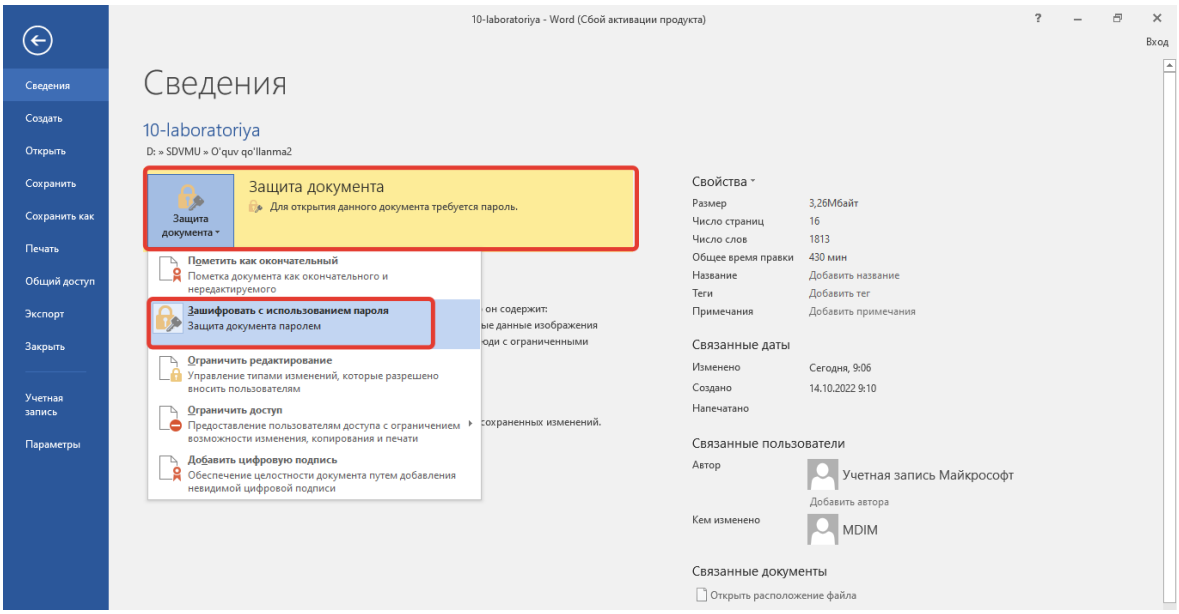
1-qadam.

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



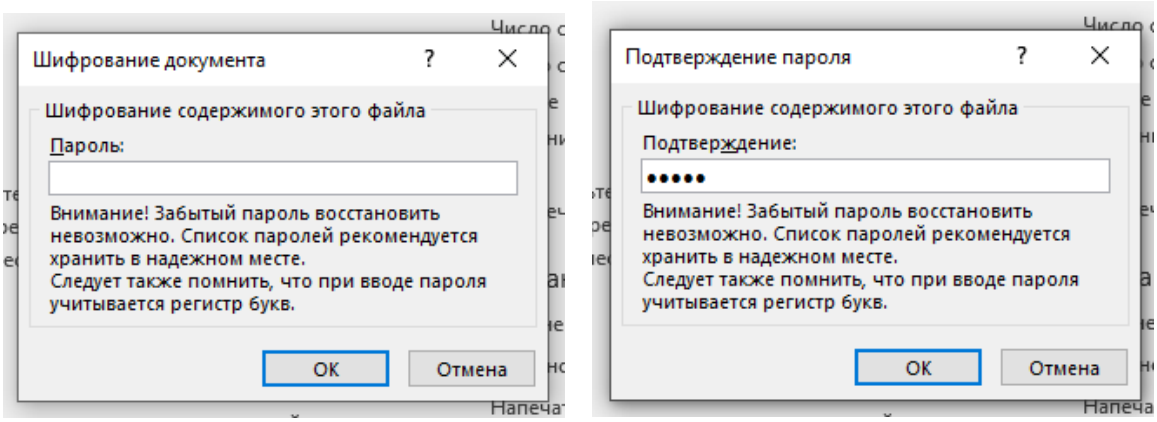
5.16-rasm.

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



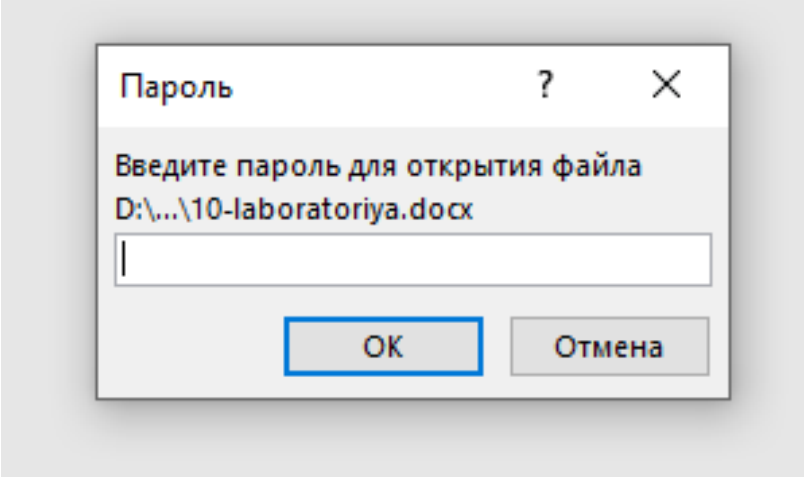
5.17-rasm.

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. 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 _____

7. Mavzuni mustahkamlash uchun testlar.

1. Kompyuter viruslari va zararli dasturlarni aniqlash, zararlangan fayllarni tiklash, shuningdek fayllarni yoki operasion tizimni profilaktik nazorat qilib borish uchun mo‘ljallangan dastur qanday ataladi?
   a) antivirus
   b) brauzer
   c) boshqarish paneli
   d) disklarni tozalash

2. «SPAM» - bu ...
   a) Barcha javoblar to‘g‘ri
   b) Taqiqlanmagan reklamali tarqatmalar
   c) Reklama yoki boshqa turdagi xabarlar va ma'lumotlarning ommaviy ravishda tarqatilishi
   d) Talab qilinmagan har xil xabarlarning ommaviy ravishda, anonim tarzda tarqatilishi

3. O‘z o‘zidan ko‘payadigan va foydalanuvchilarga hamda/yoki kompyuterlarga zarar yetkazadigan kompyuter dasturlarining turi qanday ataladi?
   a) virus
   b) spam
   c) antivirus
   d) tarqatish

4. WinRAR dasturi yordamida fayl va papkalarni arxivlash jarayonida parol qo‘ysa bo‘ladimi?
   a) Ha, bo‘ladi
   b) Yo‘q, bo‘lmaydi
   c) WinRAR dasturida bunday amal nazarda tutilmagan
   d) Arxivlash jarayonida ob'ektlarga parol qo‘yib bo‘lmaydi

5. Foydalanuvchilarning konfidensial ma’lumotlari bo‘lgan “login” va “parol”larni bilib olish maqsadida internetda amalga oshirilgan firibgarlik xarakati qanday nomlanadi?
   a) Fishing
   b) Ma'lumotlarni utilizatsiya qilish
   c) Viruslarni tarqatish
   d) Xaker xujumi

6. AVP «Kasperskiy Laboratoriyasi», NOD 32, Doctor Web, McAfee dasturlari dasturiy vositalarning qaysi turiga kiradi?
   a) Antivirus dasturlari
   b) Office uchun dasturiy ilovalar
   c) Internetga bog‘lanish uchun dasturlar
   d) Administrator nomidan ishga tushiriladigan dasturlar

7. Viruslar va/yoki zararlangan fayllarni sizning kompyuteringizga qaysi yo‘llar bilan o‘tishi mumkin?

a) Barcha javoblar to‘g‘ri
b) Internet tarmog‘idan foydalanganda
c) Tarmoq orqali tashkilotdagi boshqa bir xodimning komp'yuteridan
d) USB flesh, CD/DVD disk yoki boshqa axborot tashuvchi vositalardan foydalanganda

8. Eng optimal bo‘lgan parol ko‘rinishini ko‘rsating

a) p@r0L
b) pARoL
c) parolparol
d) prola

9. Kodlashtirish

a) Axborotni bir tizimdan boshqa tizimga ma’lum bir belgilar yordamida belgilangan tartib bo‘yicha o‘tkazish jarayoni
b) O‘z ichiga —boshlang‘ich matn belgilarini anglab olish mumkin bo‘lmagan shaklga o‘zgartirish altoritmlari
c) Konfidyentsial axborotlarni ruxsatsiz kirishdan himoyalash
d) Ruxsat etilmagan kirishdan axborotni ishonchli himoyalash

10. Kriptografiya nima?

a) Maxfiy xabar mazmunini shifrlash
b) Maxfiy xabarlarni yashirish usullari
c) Axborotlarni autentifikatsiyalash
d) Axborotlarni identifikatsiyalash

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 texnologiялari. 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. Informaциoнные texnologii. Uchebnik. M.: Oniks, 2012 god.

Qo‘shimcha adabiyotlar

1. Mirziyoyev SH.M. Erkin va farovon demokratik O‘zbekiston davlatini birgalikda barpo etamiz. Toshkent, “O‘zbekiston” NMIU, 2017 yil.
2. Mirziyoyev SH.M. Qonun ustuvorligi va inson manfaatlarini ta’minlash yurt taraqqiyoti va xalq farovonligining garovi.“O‘zbekiston” NMIU, 2017 yil.
3. Mirziyoyev SH.M. Buyuk kelajagimizni mard va olijanob xalqimiz bilan birga quramiz. “O‘zbekiston” NMIU, 2017 yil.
4. Vasilev A.N. Excel 2010 na primerax. – SPb.:SXB-Peterburg, 2010 god.
5. Garnaev A.Ю., Rudikova L.V. Microsoft Excel 2010: razrabotka prilojeniy. -SXB-Peterburg, 2011 god.
6. Leonov V. PowerPoint 2010 s nulя. – M.: Эksimo, 2010 god.
7. Karchevskiy E.M., Filippov I.E., Fillipova I.A. Word 2010 v primerax. Uchebnoe posobie. Kazan: Kazanskiy universitet, 2012 god.

Axborot manbalari:

1. https://ziyonet.uz
2. https://samvmi.uz
3. https://matworld.ru
4. https://math-pr.com