4-laboratoriya ishi. Antivirus dasturlaridan foydalanish

Laboratoriya ishi rejasi:

4.1.Asosiy tushunchalar:

4.2. Mavzu bo‘yicha laboratoriya topshiriqlari

Laboratoriya ishini maqsadi: talabalarda kompyuterlarda axborot xavfsizligini ta’minlashda antivirus dasturidan foydalanish ko‘nikmalarini hosil qilish.

Laboratoriya ishini texnik-dasturiy ta’minoti: Zamonaviy kompyuterlar; Internet tarmog‘i; Antivirus ilovalari

Laboratoriya ishiga oid adabiyotlar va Internet axborot resurslari:

1) https://translate.yandex.ru/?utm_source=wizard&lang=ru-uzbcyr – Яндекс Переводчик

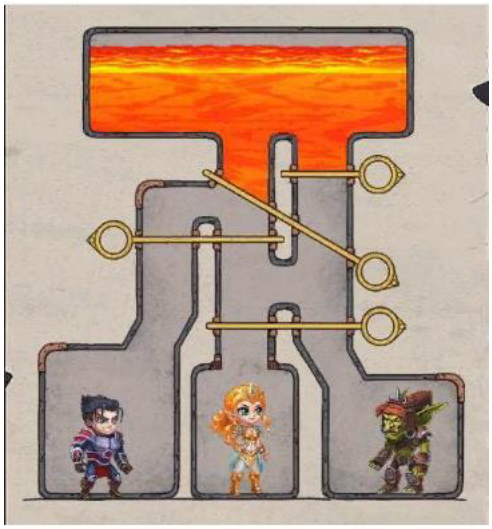
2) https://camafon.ru/informatsionnaya-bezopasnost - Информационная безобастность: защиты компьютера и данных

3) https://camafon.ru/informatsionnaya-bezopasnost/programmnoe-obespechenie-sistem - Программное обеспечение информационных систем: цель его использования

4) https://camafon.ru/informatsionnaya-bezopasnost/kompyuternaya - Компьютерная беопастность: Как защитить сети

5) http://bdstudy.ru/?p=514 - Основы информационной и компьютерной безопасности

6) https://lektsii.net/3-182823.html - Основы информационной и компьютерной безопасности



7) https://www.bsmu.by/downloads/kafedri/k_fiziki/2015-1/komp_bez.pdf - Классификация вирусов. Защита информации

8) https://support.microsoft.com/ru-ru/windows/обеспечение-безопасности-вашего-компьютера-дома-c348f24f-a4f0-de5d-9e4a-e0fc156ab221 - Обеспечение безопасности вашего компьютера дома

9) https://coderlessons.com/tutorials/kachestvo-programmnogo-obespecheniia/izuchite-kompiuternuiu-bezopasnost/kompiuternaia-bezopasnost-kratkoe-rukovodstvo- Компьютерная безопасность — Краткое руководство

10) https://www.tami.uz/matnga_qarang.php?id=1161 Axborot xavfsizligini ta’minlashning apparat-dasturiy vositalari

1.Laboratoriya ishini bajarish tartibi

Asosiy tushunchalar:

Kompyuter tarmoqlarining xavfsizligi tarmoq va unda mavjud resurslarga ruxsatsiz kirish, noto‘g‘ri foydalanish, o‘zgartirish yoki uzib qo‘yishning oldini olish va nazorat qilish uchun qabul qilingan siyosat va amaliyotlar orqali ta'minlanadi.

U tarmoq ma'muri tomonidan boshqariladigan ma'lumotlarga kirish avtorizatsiyasini o‘z ichiga oladi. Foydalanuvchilar o‘z vakolatlari doirasida ma'lumotlar va dasturlarga kirish imkonini beruvchi ID va parol yoki boshqa autentifikatsiya ma'lumotlarini tanlaydilar yoki tayinlaydilar.

Tarmoq xavfsizligi kundalik ishlarda foydalaniladigan, korxonalar, davlat idoralari va jismoniy shaxslar o‘rtasida tranzaktsiyalar va aloqalarni amalga oshiradigan ko‘plab davlat va xususiy kompyuter tarmoqlarini o‘z ichiga oladi.

Tarmoqlar shaxsiy (masalan, kompaniya ichida) yoki boshqa (omma uchun ochiq) bo‘lishi mumkin.

Kompyuter tarmog‘ining xavfsizligi tashkilotlar, korxonalar va boshqa turdagi muassasalar bilan bog‘liq. Bu tarmoqni himoya qiladi, shuningdek, himoya va nazorat operatsiyalarini bajaradi.

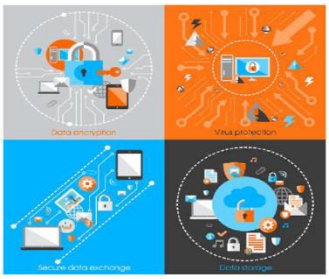
Tarmoq resursini himoya qilishning eng keng tarqalgan va eng oddiy usuli unga noyob nom va mos keladigan parolni belgilashdir.

Манба: https://uz.drunkentengu.com/obespechenie-bezopasnosti-2406 Kompyuter tarmoqlarining xavfsizligini ta'minlash - Turmush Tarzi – 2023

2.Laboratoriya ishi topshiriqlarini bajarish

1-topshiriq: Axborotni muhofaza qilishning apparat-dasturiy vositalarini tasniflang

Axborotni muhofaza qilishning apparat-dasturiy vositalari – axborotni muhofaza qilish funksiyalarini (foydalanuvchilarni identifikatsiyalash va autentifikatsiya qilish, resurslardan foydalana olishni cheklash, voqealarni qayd qilish, axborotni kriptografik himoyalash va shu kabilar) bajaradigan (mustaqil yoki boshqa vositalar bilan birgalikda) turli elektron qurilmalar va maxsus dasturlardir.



Axborotlarni muhofaza qilishning dasturiy vositalari axborotlar xavfsizligini ta’minlashga mo‘ljallangan va kompyuter vositalarining dasturiy ta’minoti tarkibiga kiritilgan maxsus dasturlardir.

Kompyuter viruslaridan va boshqa dasturlar ta’siridan va o‘zgartirishlardan himoyalanish, kompyuter tizimlarida axborotlarni qayta ishlash jarayonini himoyalashning mustaqil yo‘nalishlaridan hisoblanadi.

Ushbu xavfga yetarlicha baho bermaslik foydalanuvchilarning axborotlari uchun jiddiy salbiy oqibatlarni keltirib chiqarishi mumkin. Tarmoqning xavfsizligi undagi barcha kompyuterlarning va tarmoq qurilmalarining

xavfsizligi bilan aniqlanadi. Buzg‘unchi tarmoqning biror-bir tashkil etuvchisining ishini buzish orqali butun tarmoqni obro‘sizlantirishi mumkin.

Hamma foydalanayotgan tarmoqdan kelib chiqayotgan tahdidlarni blokirovkalash uchun “tarmoqlararo ekran” (**Firewall**) deb nomlanuvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi.

Axborotlarni muhofaza qilishning dasturiy vositalari deganda, faqatgina axborotlar xavfsizligini ta’minlashga mo‘ljallangan va kompyuter vositalarining dasturiy ta’minoti tarkibiga kiritilgan maxsus dasturlar tushuniladi.

Axborotlarni muhofaza qilishning asosiy dasturiy vositalariga quyidagilarni kiritish mumkin:

- kompyuter tizimlarida foydalanuvchilarni identifikatsiyalovchi va autentifikatsiyalovchi dasturlar;
- kompyuter tizimlari resurslaridan foydalanuvchilarning huquqlarini cheklovchi dasturlar;
- axborotlarni shifrlovchi dasturlar;
- axborot resurslarini (tizimli va amaliy dasturiy ta’minotni, ma’lumotlar bazalarini, ta’limning kompyuter tizimlarini va hokazo) noqonuniy o‘zgartirishlardan, foydalanishlardan va ko‘paytirishlardan himoyalovchi dasturlar.

Kompyuter tizimlarida axborot xavfsizligini ta’minlashga taalluqli ma’noda **identifikatsiyalash** atamasi kompyuter tizimlari sub’ektining unikal nomini bir qiymatli tanib olishni bildiradi. **Autentifikatsiyalash** esa taqdim etilgan nomni ushbu sub’ektga mosligini tasdiqlashni anglatadi (sub’ektning aslligini tasdiqlash).

Axborotlarni muhofaza qilishning yordamchi dasturiy vositalariga misol qilib quyidagilarni keltirish mumkin:

- qoldiq axborotlarni (tezkor xotira blokidagi, vaqtinchalik fayllardagi va hokazo) yo‘q qiluvchi dasturlar;
- kompyuter tizimlarining xavfsizligi tizimiga bog‘liq bo‘lgan turli voqea va hodisalarni tiklash hamda shunday voqea va hodisalar ro‘y berganini isbotlash uchun foydalaniladigan audit dasturlari (qayd qilish jurnallarini yuritish);
- qoidabuzar bilan ishlashni imitatsiyalovchi dasturlar (qoidabuzarni go‘yoki yopiq axborotlarni olgan deb chalg‘itish);
- kompyuter tizimlarining himoyalanganligini sinovdan o‘tkazuvchi nazorat dasturlar va boshqalar.

2-topshiriq: Axborotlarni muhofaza qilishning dasturiy vositalarining afzalliklarini tasniflang

Axborotlarni muhofaza qilishning dasturiy vositalarining afzalliklariga quyidagilar kiradi:

- ko‘paytirishning osonligi;
- moslanuvchanlik (turli sharoitlarda qo‘llaniladigan muayyan kompyuter tizimlarini, axborot xavfsizligiga tahdidning o‘ziga xosligini hisobga olib, sozlash imkoniyati);

•qo‘llashning qulayligi – bir xil dasturlar, masalan shifrlovchi dasturlar “shaffof” (foydalanuvchiga ko‘rinmaydigan) rejimda ishlaydi, boshqalari foydalanuvchidan hech qanday qo‘shimcha yangi (boshqa dasturlari bilan taqqoslaganda) ko‘nikmalar talab qilmaydi;

•ularni axborot xavfsizligiga yangi tahdidlar hisobini yuritish uchun o‘zgartirishlar kiritish yo‘li bilan takomillashuvining amaldagi chek-chegarasiz imkoniyatlari mavjudligi.

Axborotlarni muhofaza qilishning dasturiy vositalarining kamchiliklariga quyidagilar kiradi:

- himoyalovchi dasturlarning faoliyati kompyuter tizimlari resurslaridan foydalanish hisobiga bo‘lgani uchun bu tizimlar samaradorligining susayishi;
- juda past unumdorlik (xuddi shunday vazifani bajarayotgan apparat vositalar bilan taqqoslaganda, masalan shifrlovchi qurilma);
- axborotlarni himoyalovchi ko‘pgina dasturiy vositalarning kompyuter dasturiy ta’minotiga bevosita o‘rnatilmagani (quyidagi rasmlar), bu holat qoidabuzarning ushbu dasturlarni chetlab o‘tishiga prinsipial imkoniyatlar yaratadi;
- kompyuter tizimlaridan foydalanish jarayonida axborotlarni himoyalashning dasturiy vositalarini qasddan o‘zgartirish imkoniyati.

Kompyuter viruslaridan va boshqa dasturlar ta’siridan va o‘zgartirishlardan himoyalanish, kompyuter tizimlarida axborotlarni qayta ishlash jarayonini himoyalashning mustaqil yo‘nalishlaridan hisoblanadi. Ushbu xavfga yetarlicha baho bermaslik foydalanuvchilarning axborotlari uchun jiddiy salbiy oqibatlarni keltirib chiqarishi mumkin. Viruslarning ta’sir mexanizmlarini, ularga qarshi kurash usullari va vositalarini bilish viruslanishga qarshi harakatlarni samarali tashkil etish, ularning ta’siridan zararlanish ehtimolligini va talofatlarni minimumga keltirish imkonini beradi.

Kompyuter viruslari – bu kompyuter tizimlarida tarqalish va o‘zini o‘zi ishlab chiqish xususiyatiga ega bo‘lgan kichik hajmdagi bajariluvchi dasturlar. Viruslar kompyuter tizimlarida saqlanayotgan dasturiy vositalar yoki ma’lumotlarni yo‘q qilishi yoki o‘chirib yuborishi mumkin. Tarqalish jarayonida viruslar o‘zini modifikatsiyalashi mumkin.

Viruslarning ommaviy tarqalib ketishi va ularning kompyuter tizimlari resurslariga ta’siri oqibatlarining jiddiyligi, maxsus antivirus vositalarini va ularni qo‘llash usullarini yaratish va foydalanish zaruriyatini keltirib chiqardi.

3-topshiriq: Antivirus vositalari tushunchasini tasniflang

Antivirus vositalari quyidagi masalalarni hal etish uchun qo‘llaniladi:

- kompyuter tizimlarida viruslarni topish;
- virus – dasturlar ishini blokirovka qilish;
- viruslar ta’sirining oqibatlarini bartaraf qilish.

Viruslarni topishni, ularni joylashib olish bosqichida yoki hech bo‘lmaganda virusning buzg‘unchilik funksiyalarini boshlagunga qadar amalga oshirish maqsadga

muvofiq. Shuni ta’kidlash joizki, barcha turdagi viruslarni topishni kafolatlovchi antivirus vositalar mavjud emas.

Virus topilgan holatda, uning tizimga keltirishi mumkin bo‘lgan zararli ta’sirini minimallashtirish maqsadida darhol virus-dasturning ishini to‘xtatilish lozim.

Virusning ta’sir oqibatlarini bartaraf qilish ikki yo‘nalishda olib boriladi:

- virusni o‘chirish;
- fayllarni, xotira sohalarini tiklash.

Tizimni qayta tiklash virus turiga, uni aniqlangan hamda zararlovchi ta’sirini boshlagan vaqtiga bog‘liq. Viruslar tizimga kirish jarayonida, o‘zini saqlaydigan joydagi ma’lumotlarni o‘chirib yuborsa hamda zararlovchi ta’siri natijasida ma’lumotlarni o‘zgartirish nazarda tutilgan bo‘lsa, zaxiraga olingan ma’lumotlarsiz yo‘qolgan ma’lumotlarni tiklab bo‘lmaydi.

Viruslarga qarshi kurashda aniq bir ketma-ketlik va kombinatsiyada qo‘llaniluvchi, viruslarga qarshi kurashish usullarini hosil qiluvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi.

Kompyuter tizimining xavfsiz ishlashining asosiy shartlaridan biri, amalda sinovdan o‘tkazilgan va o‘zining yuqori samara berishini ko‘rsatgan bir qator qoidalarga rioya qilish hisoblanadi.

Birinchi qoida – qonuniy rasmiy yo‘l bilan olingan dasturiy mahsulotlardan foydalanish. Dasturiy ta’minotning qaroqchilik yo‘li bilan ko‘paytirilgan nusxalarida, rasmiy yo‘l bilan olinganlariga nisbatan viruslarning mavjudlik ehtimoli juda yuqori.

Ikkinchi qoida – axborotlar zaxirasini hosil qilish. Avvalo dasturiy ta’minotning distributivlari yozilgan tashuvchilarni saqlash zarur. Bunda tashuvchilarga ma’lumotlarni yozish imkoni berilgan bo‘lsa, imkon qadar uni blokirovka qilish zarur. Ishga taalluqli ma’lumotlarni saqlanishiga jiddiy yondashishi zarur. Muntazam ishga taalluqli fayllarning zaxira nusxalarini yaratib borish va ularni yozishdan himoyalangan yechib olinuvchi tashuvchilarda saqlash kerak. Agar bunday nusxalar yechib olinmaydigan tashuvchilarda yaratilayotgan bo‘lsa, ularni butunlay boshqa kompyuterning doimiy xotirasida yaratish maqsadga muvofiq. Bunda yoki faylning to‘liq nusxasi yoki kiritilayotgan o‘zgarishlarning nusxalari saqlanadi.

Uchinchi qoida – antivirus vositalaridan muntazam foydalanish.

Antivirus vositalari muntazam yangilanib turilishi lozim.

To‘rtinchi qoida – yangi yechib olinadigan axborot tashuvchilardan va yangi fayllardan foydalanilganda ehtiyotkorlikka rioya qilish. Yangi yechib olinadigan tashuvchilar olinganda, albatta, yuklanuvchi va fayl viruslari mavjudligiga, olingan fayllar esa fayl viruslari mavjudligiga tekshirilishi lozim. Tekshiruv, skanerlovchi – dasturlar va evristik tahlilni amalga oshiruvchi dasturlar yordamida amalga oshirilishi kerak. Olingan hujjatlar va jadvallar bilan ishlashda, ushbu fayllar to‘liq tekshirilgunga qadar, matn va jadval muharrirlariga o‘rnatilgan makrokomandalarning bajarilishini taqiqlash zarur.

Beshinchi qoida – tizimga, ayniqsa taqsimlangan tizimlarga yoki jamoa bo‘lib foydalaniladigan tizimlarga, kiritilayotgan fayllarni va yechiladigan axborot tashuvchilarni maxsus ajratilgan kompyuterlarda tekshirish. Uni tizim administratori yoki ma’lumotlar xavfsizligiga mas’ul bo‘lgan shaxsning avtomatlashtirilgan ish

joyidan amalga oshirilishi maqsadga muvofiq. Disk va fayllarni har tomonlama antivirus tekshiruvidan o‘tkaziluvidan so‘ng ularni tizimdan foydalanuvchilarga taqdim etish mumkin.

Oltinchi qoida – agar axborotlarni tashuvchilarga yozish nazarda tutilmagan bo‘lsa, bunday amallarni bajarilishini blokirovka qilish.

Yuqorida keltirilgan tavsiyalarga doimiy rioya qilinishi virus dasturlar bilan zararlanish ehtimolini ancha kamaytiradi va foydalanuvchini axborotlarni qaytib tiklab bo‘lmaydigan yo‘qotishlardan saqlaydi.

4-topshiriq: Axborot butunligi tushunchasini tasniflang

Kompyuter tarmog‘idan foydalanish bosqichlarida tizimdagi axborotlarning butunligi va ulardan foydalanish huquqi quyidagilar orqali ta’minlanadi:

- kompyuter tizimlarida mavjud axborotlarning butunligi;
- kompyuter tizimlarining rad etishga barqarorligini oshirish;
- tizimning qayta yuklanishi va «osilib qolishi»ni bartaraf etish;
- axborot zaxiralarini yaratish;
- qat’iy belgilangan dasturlar majmuidan foydalanish;
- texnik xizmat ko‘rsatish va kam-ko‘stini to‘ldirish jarayonlarining o‘ziga xos tartibiga rioya qilish;
- antivirus tadbirlari kompleksini o‘tkazish.

Axborotning butunligi va foydalanishga qulayligi apparat vositalar zaxirasini yaratish, foydalanuvchilarning xato harakatlarini blokirovka qilish, kompyuter tizimlarining ishonchli elementlaridan va barqaror ishlovchi tizimlardan foydalanish yo‘li bilan amalga oshiriladi.

Kompyuter tarmog‘ida axborotlarning butunligi va foydalanishga qulayligini ta’minlashning asosiy shartlaridan biri ularning zaxiralarini hosil qilishdan iborat. Axborotlar zaxirasini yaratish strategiyasi axborotning muhimligini, kompyuter tizimlarining uzluksiz ishlashiga bo‘lgan talablarni, ma’lumotlarni tiklashdagi qiyinchiliklarni hisobga olgan holda tanlanadi. Himoyalangan kompyuter tizimlarida faqatgina ruxsat etilgan dasturiy ta’minotdan foydalanilishi lozim.

Foydalanishiga rasman ruxsat etilgan dasturlarning ro‘yxati, ularning butunligini nazorat qilishning usullari va davriyligi kompyuter tizimlarini ekspluatatsiya qilinishidan oldin aniqlanishi kerak.

Dasturlar butunligini nazorat qilishning sodda usullaridan biri nazorat yig‘indilari usuli hisoblanadi. Nazorat yig‘indisi – ma’lumotlar blokining oxiriga yoziladigan bitlar ketma-ketligi. Nazoratdagi faylga kiritilgan o‘zgartirishni, nazorat yig‘indini tuzatib qo‘yish bilan, berkitishni istisno qilish maqsadida nazorat yig‘indini shifrlangan holda saqlash yoki nazorat yig‘indini hisoblashning maxfiy algoritmidan foydalanish zarur.

5-topshiriq. ESET NOD32 antivirus dasturini tasniflang

Ko‘rsatma.

Tasniflarda Internet qidiruv tizimlaridan foydalang. Masalan, “ESET NOD32 - характеристики антивирусов”, “Краткая характеристика антивирусов ESET»

“ESET NOD32 –характеристики и описание антивирусов” nomda qidiruvlarni amalga oshiring:

https://www.softmagazin.ru/blog/eset_nod32_antivirus/ - ESET NOD32 - характеристики антивирусов ;

«ESET NOD32 - характеристики и описание антивирусов» каби қидирувларни амалга оширинг

6-topshiriq. Dr Web antivirus dasturini tasniflang

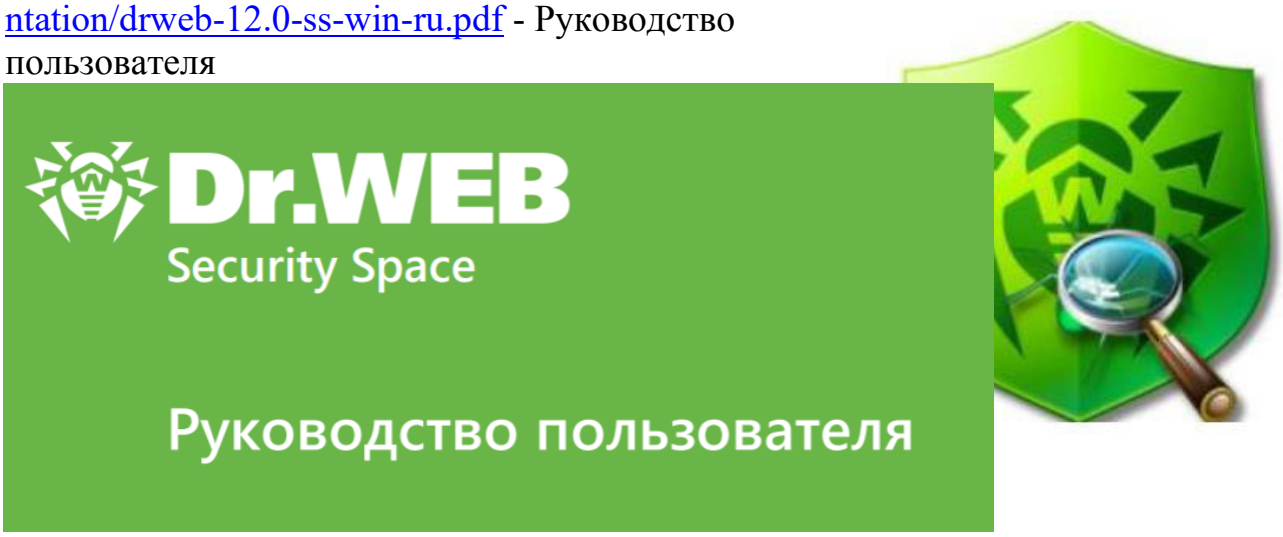
Ko‘rsatma. Antivirus imkoniyatlarini o‘rganishda quyidagi Internet manbalari tavsiya etiladi:

http://sd-company.su/article/antivirus/drweb **-Dr Web (Doctor Web) - описание антивируса**

https://club.dns-shop.ru/review/t-57-tehnologii/21721-obzor-antivirusa-dr-web-traditsionnoe-reshenie-slojnyih-problem/ - Обзор антивируса Dr.Web - традиционное решение сложных проблем

https://1comp.spb.ru/dr-web.html - Антивирус Dr.Web

https://download.geo.drweb.com/pub/drweb/windows/workstation/12.0/documentation/drweb-12.0-ss-win-ru.pdf - Руководство пользователя



http://www.paygid.ru/articles/antivirus-dr-web-svoystva-i-harakteristika/?q=726&n=1721 - Антивирус Dr Web: свойства и характеристика

7-topshiriq: Antivirus dasturlarini tasniflang.

Ko‘rsatma. Antivirus imkoniyatlarini o‘rganishda quyidagi Internet manbalari tavsiya etiladi:

http://www.univer.omsk.su/omsk-old/Edu/infpro/1/13/virys2.html - Характеристика антивирусных программ

https://sites.google.com/site/komputernyevirusykulikov/4-antivirusnye-programmy/klassifikacia-harakteristiki-primery - Компьютерные вирусы. Антивирусные программы

Антивирус Касперского
Dr. Web
Eset NOD32
Norton AntiVirus
Антивирус Avast!
Avira Antivir

https://infourok.ru/obzor-sovremennih-antivirusnih-programm-i-ih-harakteristiki-3876310.html - Обзор современных антивирусных программ и их характеристики

https://studbooks.net/2025607/informatika/antivirusnye_programmy - АНТИВИРУСНЫЕ ПРОГРАММЫ

https://compress.ru/article.aspx?id=10112 – Обзор антивирусных программ для персональных пользователей

Основные методы определения вирусов
Классификация антивирусных программ
Обзор наиболее популярных персональных антивирусов
Антивирус Касперского
Personal Pro v. 4.0
Doctor Web для Windows 95-XP
Norton AntiVirus 2003 Professional Edition
McAfee VirusScan Professional 6.0
Panda Antivirus Titanium

https://www.kaspersky.ru/home-security -

http://security.bezmani.ru/kaspersky-antivirus/ -Антивирус Касперского (Kaspersky antivirus)

- **Антивирусы**

Антивирус Касперского
Антивирус Norton AntiVirus
Антивирус Dr. Web
Антивирус NOD32
Антивирус Panda
Файерволл Outpost Firewall
Бесплатные антивирусы
Антивирусы для мобильного
Антивирусы для андроид
Другие антивирусы

- **Материалы**

Как защитить компьютер
Как установить антивирус
Как удалить антивирус
Скачать бесплатно антивирус

Kompyuter viruslari haqida va ularning turlari

- Hozirgi kunda hamma kompyuter foydalanuvchilari virus degan tushunchani yaxshi bilishadi. Bu kichik dastur bilan bir necha bor uchrashishgan. Koʻp hollarda magʻlub ham boʻlishgan. Bilib olgan boʻlsangiz bu maqolamiz viruslarga bagʻishlanadi.
- **Virus** – bu dasturchi tomonidan tuzilgan, kompyuter ish faoliyatini tekis ishlashiga halaqit beradigan, oqibatda kompyuterni yoqilishini ham taqiqlab qoʻyadigan dasturdir. Bu dasturlar asosan internet tarmogʻi orqali foydalanuvchi kompyuteriga tushadi.
- Albatta, bu dastur, internet foydalanuvchisi bilmagan holda oʻz kompyuterida paydo boʻladi. Ularga qarshi kurashadigan dastur antivirus deyiladi (bu toʻgʻrisida keyingi maqolalarda).
- **Viruslar kompyuterlarda oʻzini har hil tutadi**. Ba'zi birlari kompyuteringizni kerakmas fayllar bilan toʻldirsa, yana ba'zilari operativ xotirani koʻp qismini ishlatib, kompyuteringizni qotirib qoʻyadi, viruslarning bir qismi esa, kerakli fayllaringizni yoki tizim fayllarini oʻchirib sizga zarar yetkazadi. Shulardan saqlanish uchun viruslarning turini bilib olish lozim, ya'ni qaysi virus nima ish qiladi va bundan saqlanish oʻz oʻzidan kelib chiqadi. Quyida ularning turlari keltirilgan(turlari ref.uz dan olindi):
- **Troyanlar** (Trojan Horses) – Qadimgi yunonlarning Troyaga yurishlari davrida qoʻllagan hiylasi, ya'ni troyaliklarni otga ishqiboz ekanligidan foydalanib, ularga katta yogʻoch ot sovgʻa qilishlari va bu otning troyaliklar magʻlubiyatiga olib kelishi voqeasidan olingan nom. Hozirda troya oti iborasi «hosiyatsiz sovgʻa" degan ma'noni bildiradi. Kompyuter va internet dunyosida troyanlar «hosiyatsiz programma" deb nomlanishi maqsadga muvofiq. Troyanlar odatda internet orqali tarqaladi. Troyanlar kompyuteringizga oʻrnashib olib, dastlab foydali programma sifatida oʻzlarini tanishtiradilar, lekin ularning asl vazifasi foydalanuvchiga noma'lumligicha qoladi. Yashirin ravishda ular oʻzlarining yaratuvchisi (cracker – yovuz haker) tomonidan belgilangan harakatlarni amalga oshiradilar. Troyanlar oʻz-oʻzidan koʻpaymaydi, lekin kompyuteringiz xavfsizligini ishdan chiqaradi: troyanlar kerakli ma'lumotlaringizni oʻchirib yuborishi, kompyuterdagi ma'lumotlarni kerakli manzilga joʻnatishi, kompyuteringizga internetdan ruxsatsiz ulanishlarni amalga oshirishi mumkin.
- **Chuvalchang viruslar** (Worms) – Chuvalchang viruslar oʻz nomiga mos ravishda juda tez oʻz-oʻzidan koʻpayadigan viruslardir. Odatda bu viruslar internet yoʻli intranet tarmoqlari orasida tarqaladi. Tarqalish usuli sifatida elektron xatlar yoki boshqa tez tarqaluvchi mexanizmlardan foydalanadi. Ular haqiqatdan ham kompyuteringizdagi ma'lumotlar va kompyuter xavfsizligiga katta ziyon yetkazadi. Chuvalchang viruslar operatsion tizimning nozik joylaridan foydalanish yoki zararlangan elektron xatlarni ochish yoʻli bilan kompyuteringizga oʻrnashib olishi mumkin.
- **Boot sektor viruslari** (Bootsector viruses) – Bu viruslar kompyuterning ishlay boshlashi (zagruzka) uchun foydalaniladigan qattiq diskning maxsus qismini ishdan

chiqaradi. Bu virus kompyuteringizni zararlaganidan keyin, kompyuter ishlamay qolishi mumkin. Odatda floppy disklar orqali tarqaladi.

- **Makro viruslar** (Macro viruses) – **Macro** viruslar bu – o‘zlarining tarqalishi uchun boshqa bir programmaning makro dasturlash tilidan foydalanadigan viruslardir. Ular odatda **Microsoft Word** yoki **Excel** hujjatlarini zararlaydi.
- **Operativ xotirada yashovchi viruslar** (Memory Resident Viruses) — Bu viruslar kompyuteringizning operativ xotirasida (RAM) yashaydi va zararli harakatini amalga oshiradi. Odatda ularni ishga tushirish uchun boshqa virusdan foydalaniladi. Ular o‘zlarining ishga tushishga yordam bergan virus yopilgan bo‘lsa ham kompyuter xotirasida qoladi, shuning uchun ham ularga yuqoridagi nom berilgan.
- **Rootkit viruslari** (Rootkit viruses) – **Rootkit’lar viruslar** orasida o‘zlarining eng xavfliligi va yashirinishga ustaligi bilan alohida ajralib turadi. **Rootkit**lar kompyuteringizni yovuz hakerlar tomonidan qo‘lga olinishi uchun foydalaniladi. Ba’zi **Rootkit**larni antivirus programmalari ham aniqlay olmaydi, chunki ular o‘zlarini operativ tizim fayllari sifatida ko‘rsatishadi. **Rootkit**lar odatda troyanlar tomonidan kompyuteringizga o‘rnatiladi.
- **O‘zgaruvchan viruslar** (Polymorphic viruses) – Bu viruslar nafaqat o‘z-o‘zidan ko‘payadi, balki ko‘paygan paytda o‘zlarining kodlarini ham o‘zgartirib turishadi. O‘zgaruvchan viruslarni aniqlash ham ba’zi antiviruslar uchun qiyin kechishi mumkin.
- **Vaqt bombasi viruslari** (Time or Logic Bombs) – Bu viruslar muayyan sana yohud payt kelganida yoki foydalanuvchi tomonidan muayyan harakat amalga oshirilganida ishga tushadigan viruslardir. Misol uchun Kulgi kunida (1 aprel) yoki Yangi yilda kompyuteringizdagi ma’lumotlarni o‘chirib tashlab sizga “sovg‘a” taqdim etishi mumkin.

https://www.texnoman.uz/post/kompyuter-viruslari-haqida-va-ularning-turlari.html - Kompyuter viruslari haqida va ularning turlari

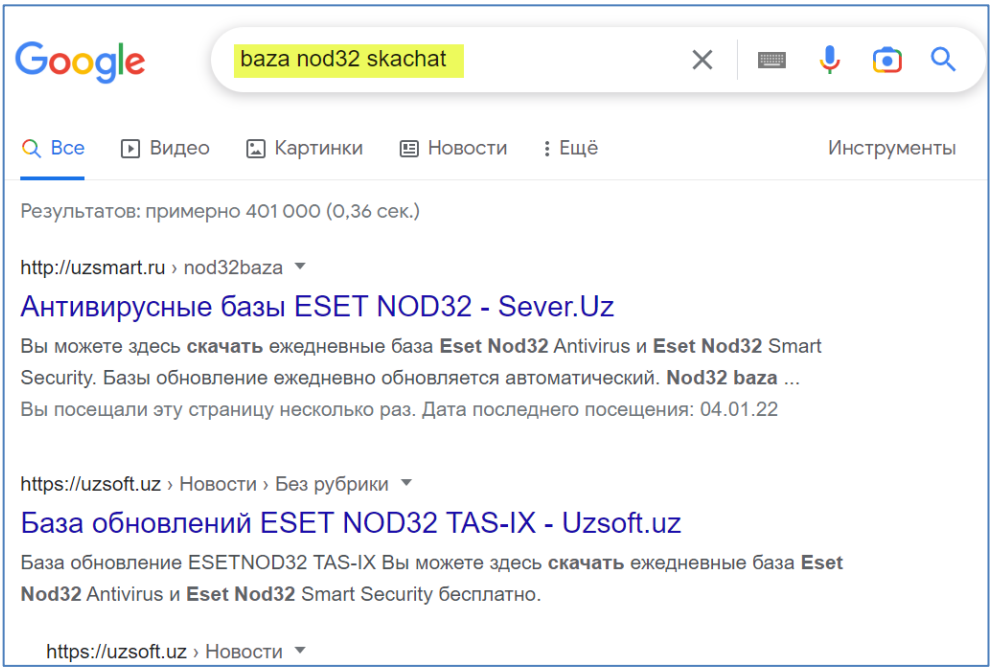
8-topshiriq. ESET NOD32 antivirus dasturi bazasini yangilash

Ko‘rsatma.

ESET NOD32 antivirus dasturi kompyuteringizga o‘rnatilgan bo‘lishi lozim. Ushbu antivirus kompyuterda samarali ishlashi uchun viruslar bazasini muntazam yangilab turish lozim.

ESET NOD32 antivirus bazasini ikki xil yo‘l bilan yangilash mumkin: on-line va off-line. Quyida antivirus bazasini off-line yangilashni ko‘rib chiqamiz.

1-qadam. Qidiruv oynasiga “**baza nod32 скачать**” jumlasini kiritib Enter tugmasini bosing.

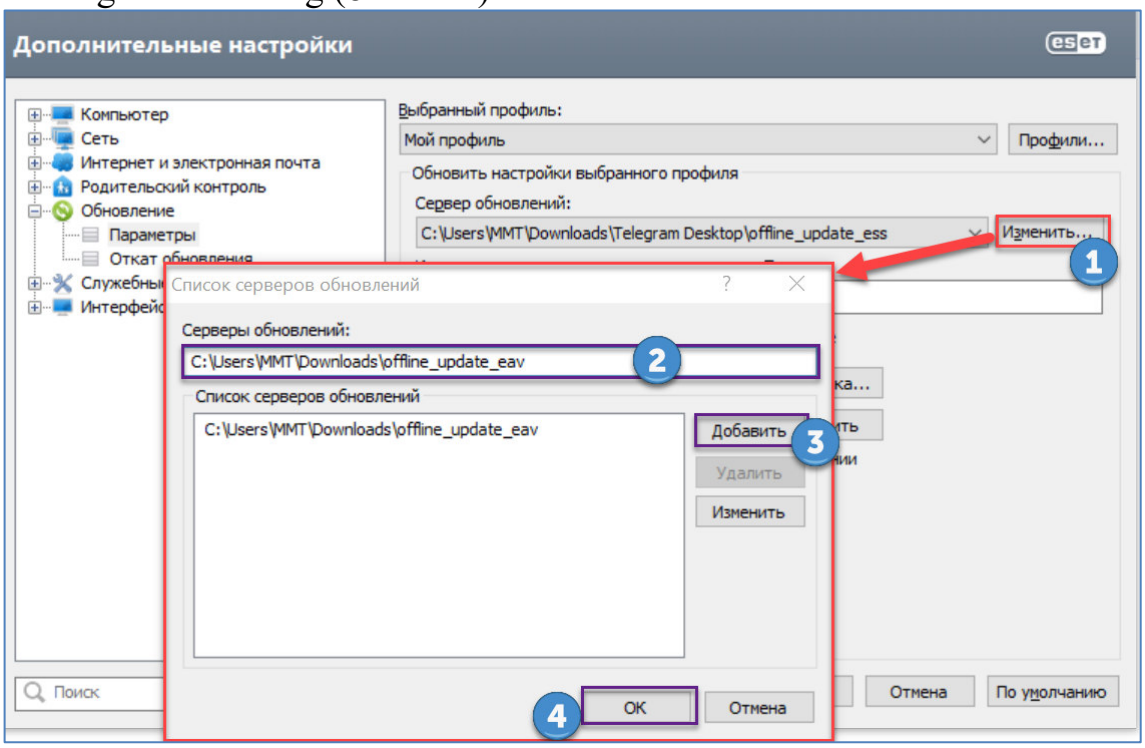


8.1-rasm.

2-qadam. Topilgan natijalardan birini oching (bizning misolda 1-natija). Ochilgan veb-sahifadan **ESET NOD32 (EAV)** ni yuklab oling (http://uzsmart.ru/nod32baza/) .

3-qadam. Yuklab olingan arxiv faylni shu nomdagi papkaga arxivdan chiqaring.

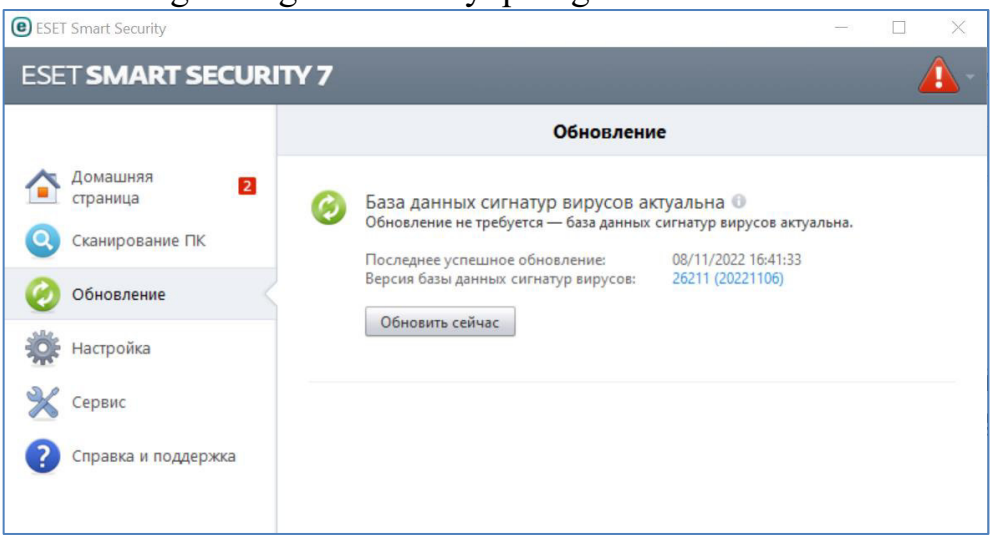
4-qadam. ESET NOD32 dasturini yuklang. Klaviaturadan **F5** tugmasini bosing. Natijada **Дополнительные настройки** (Qo‘shimcha sozlamalar) oynasi ochiladi. Bu oynadan **Обновленые ▹ Параметры** ni tanlang. **Сервер обновлений** qismidagi **Изменить** tugmasini bosing (8.2-rasm).



8.2-rasm.

5-qadam. Arxivdan chiqarilgan papkaning manzilini **Сервер обновлений** darchasiga kiriting va **Добавить** tugmasini bosing. So‘ngra **OK** tugmasini bosing (8.2-rasm). **Дополнительные настройки** oynasini yoping.

6-qadam. **ESET NOD32 dasturi** asosiy oynasidan **Обновление** bo‘limini tanlang va o‘ng oynadan **Обновить сейчас** tugmasini bosing (8.3-rasm). Yangilanish oxiriga yetguncha kuting. So‘ngra dasturni yopsangiz ham bo‘ladi.



8.3-rasm.