**O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

**Tahdid razvedkasi** fanidan

**Amaliy ishi**

Bajardi:712-19 guruh talabasi

No’monov Murodjon

Toshkent 2022

**3-Amaliy ish.**

**Elektron pochtaga kiruvchi kutilmagan xatlardan himoya**

***Ishdan maqsad:***

"The Bat!" elektron pochta dasturi misolida elektron pochtaga kiruvchi kutilmagan xatlardan himoya qilishning o'ziga xos xususiyatlarini o'rganish.

**Qisqacha nazariy ma’lumotlar.**

"The Bat!" - bu tijoriy dastur bo’lib, ikkita versiyada mavjud - Professional va Home, ular qo'llab-quvvatlanadigan funksiyalar sonidan farq qiladi. Mahsulotning professional nashri ko'p tilli interfeys bilan jihozlangan, axborotni shifrlashdan foydalanish imkoniyatini o'z ichiga oladi, shuningdek, dasturning ko'chma himoyalangan versiyasi - The Bat! Voyagerdan foydalanish imkonini beradi. Mobil versiyasi har qanday ko'chma xotira qurilmasidan ishlaydi (flesh-disk, USB-disk va boshqalar) va ko'pincha ofisdan tashqarida ishlaydigan va korporativ aloqa manbalariga xavfsiz masofadan kirishni talab qiladigan kompaniyalarning ishchilariga katta yordam berishi mumkin.

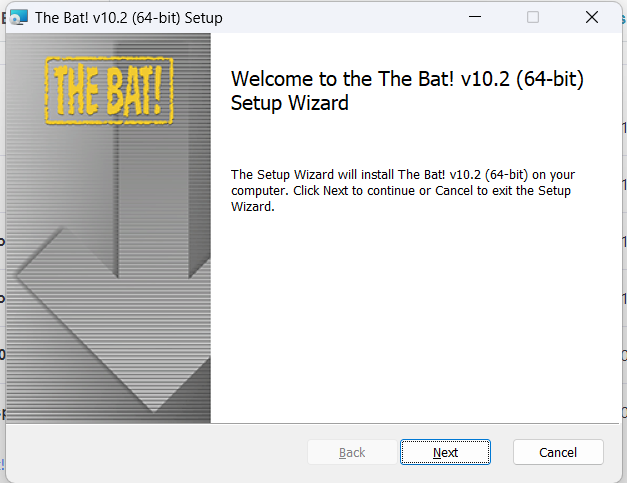
***Ishni bajarish tartibi:***

1. Dasturni o'rnatish

2. Dasturning qo'shimcha funksiyalarini o'rganish

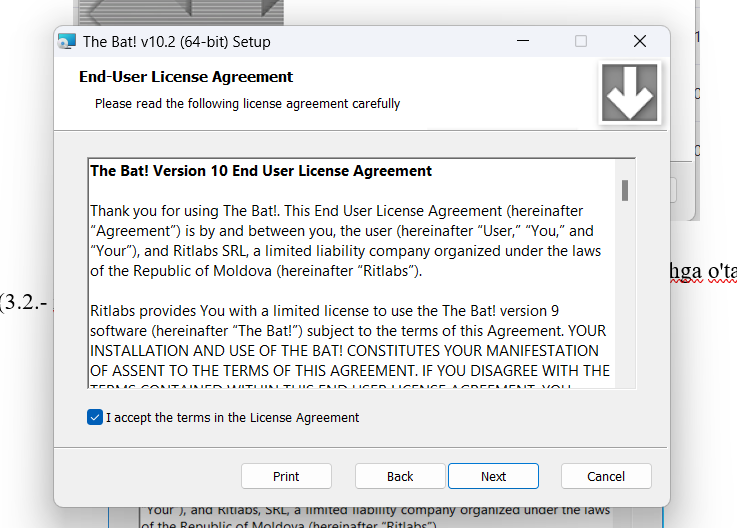
***1. Bat dasturini o'rnatish***

Dasturni o'rnatish uchun The Bat dastur paketi ishga tushiring, o'rnatishni davom ettirish uchun «Next» tugmasini bosing (3.1.- rasm).



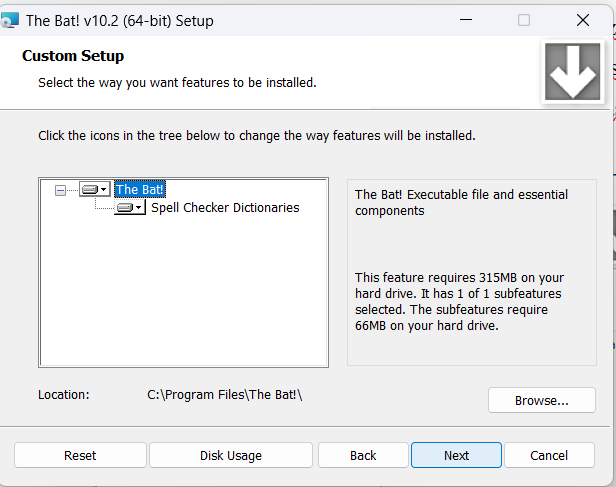
3.1.- rasm. O'rnatish jarayoni

Biz foydalanuvchi shartnomasini qabul qilamiz va keyingi bosqichga o'tamiz (3.2.- rasm).



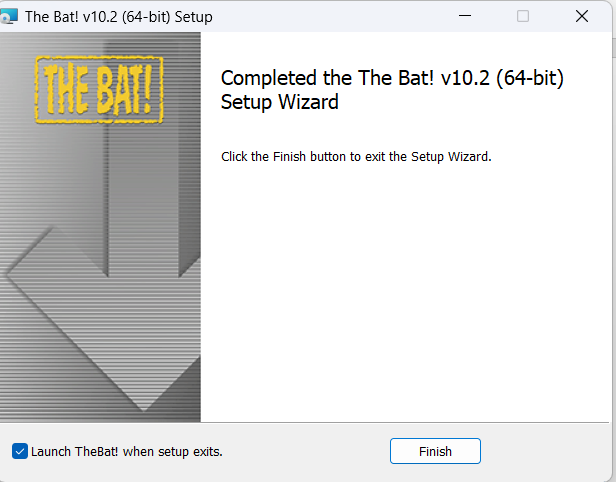
3.2.- rasm. Foydalanuvchi shartnomasi

Keyin o'rnatish ustasi sizni o'rnatish komponentlarini tanlashingizni so'raydi. Bu yerda siz hech narsani o'zgartirmasligingiz kerak va "Next" tugmasini bosing. Agar sizga ma'lum bir komponentni o'rnatish kerak bo'lsa, belgini olib tashlashingiz kerak (3.3.- rasm).



3.3.- rasm. O'rnatish yo'lini tanlash

Ushbu bosqichlarni bajargandan so'ng, o'rnatish ustasi ma'lumot to'plashni yakunlaydi va o'rnatish jarayoniga tayyorlanadi, davom etish uchun «Next» tugmasini bosing. Dasturni o'rnatish jarayoni boshlanadi, bu «Completed The Bat! Setup Wizard» dialog oynasining paydo bo'lishi bilan yakunlanadi va Bat dasturini muvaffaqiyatli o'rnatilganligi haqida xabar paydo bo’ladi. O'rnatishni yakunlash uchun "Finish" tugmasini bosing (3.4.- rasm).

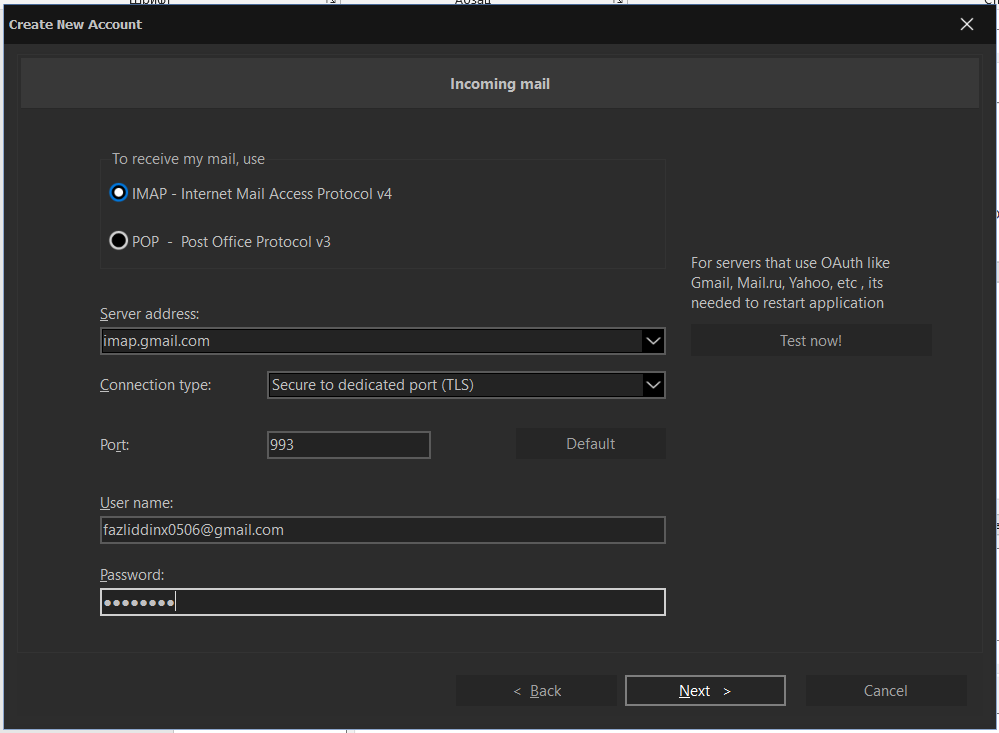


3.4.- rasm. O'rnatishni tugatish.

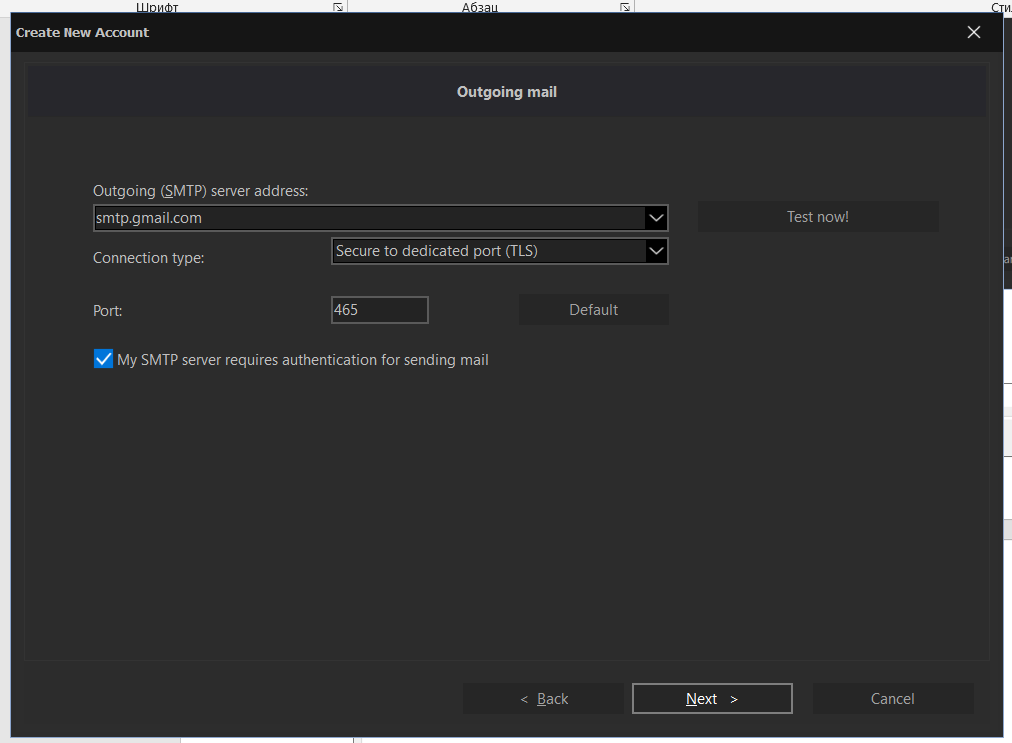
Autentifikatsiya qilingan foydalanuvchidan boshqa hech kim kompyuterda pochta xabarlarini o'qiy olmaydi, yangi pochta qutisini yaratishda ma'lumotlarni himoya qilish parametrlarini sozlashingiz kerak, ya'ni parolni o'rnatishingiz kerak. Pochta o'rnatilganda, oldindan ro'yxatdan o'tgan pochta qutisidagi ma'lumotlarni kiriting va «Далее» tugmasini bosing (3.5.- rasm).

«Исходящая почта» oynasida mavjud bo'lgan pochta qutisidan ma'lumotlarni kiritishingiz kerak, agar bilmasangiz, keyin hamma narsani standart holat bo'yicha qoldiring va davom etish uchun «Далее» tugmasini bosing   
(3.6.- rasm).

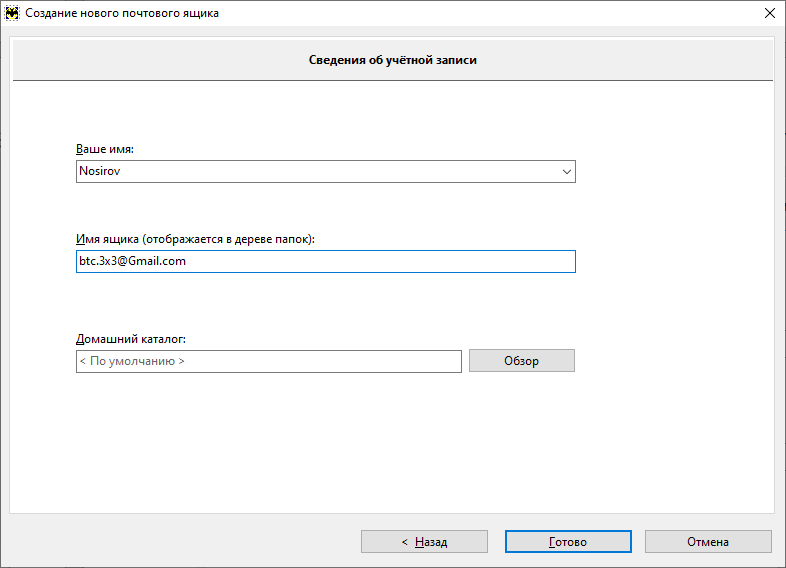
Oxirgi bosqichda siz pochta qutisi nomini va elektron pochta manzilini kiritishingiz va «Готово» tugmasini bosishingiz kerak (3.7.-rasm).



3.5.- rasm. Kiruvchi pochtani sozlash

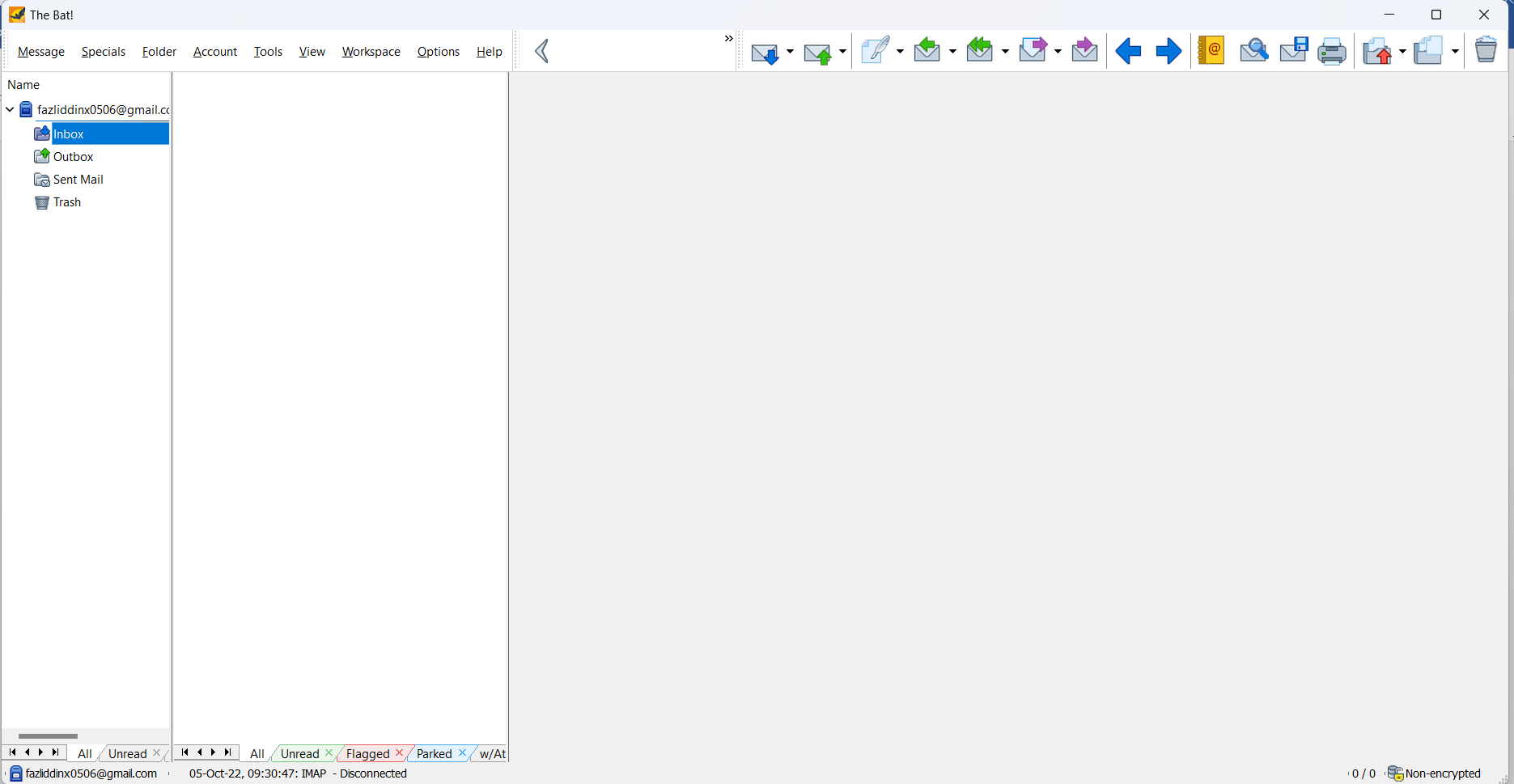


3.6.- rasm. «Исходящей почты» ni sozlash



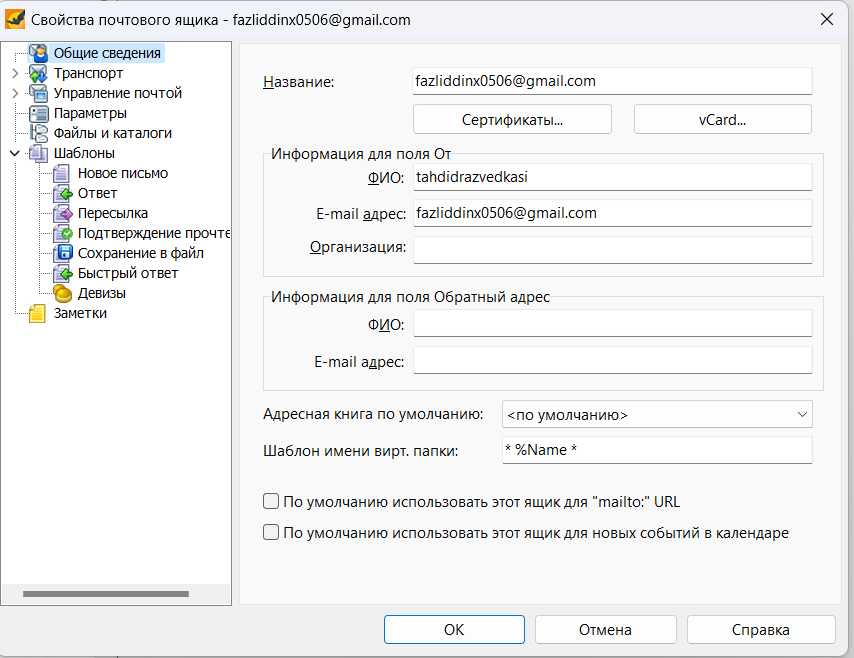
3.7.- rasm. Sozlashni tugatish

«Готово» tugmasini bosgandan so'ng, o'rnatish paytida ko'rsatilgan ulangan pochta qutisi bilan dasturning asosiy oynasi ochiladi (3.8.- rasm).



3.8.- rasm Dasturning asosiy oynasi

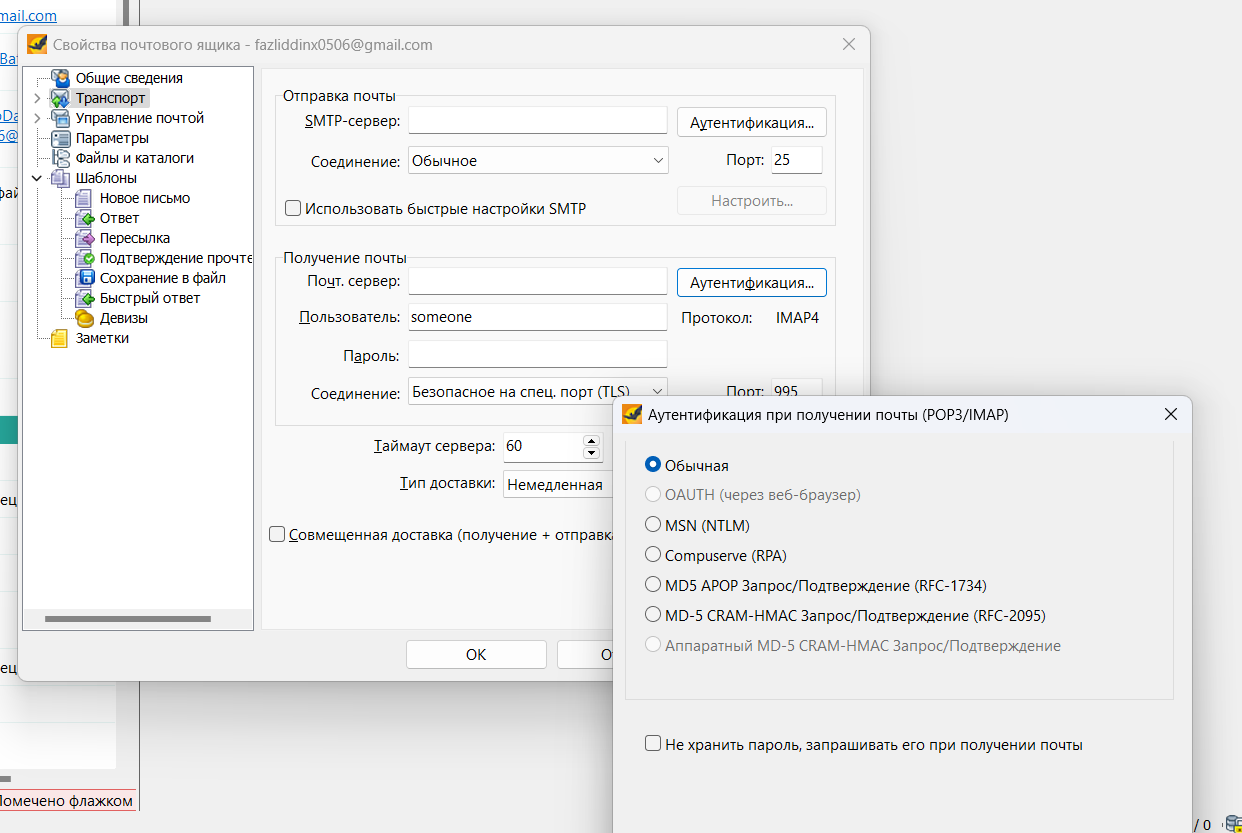
Barcha ma'lumotlar va sozlamalarni tahrirlash uchun siz pochta manzilini tanlashingiz kerak, keyin «Ящик» menyusini, so'ngra «Свойства почтового ящика» bandini tanlang (23-rasm).



3.9.- rasm Pochta qutisi xususiyatlari

***2. Dasturning qo'shimcha funksiyalarini o'rganish***

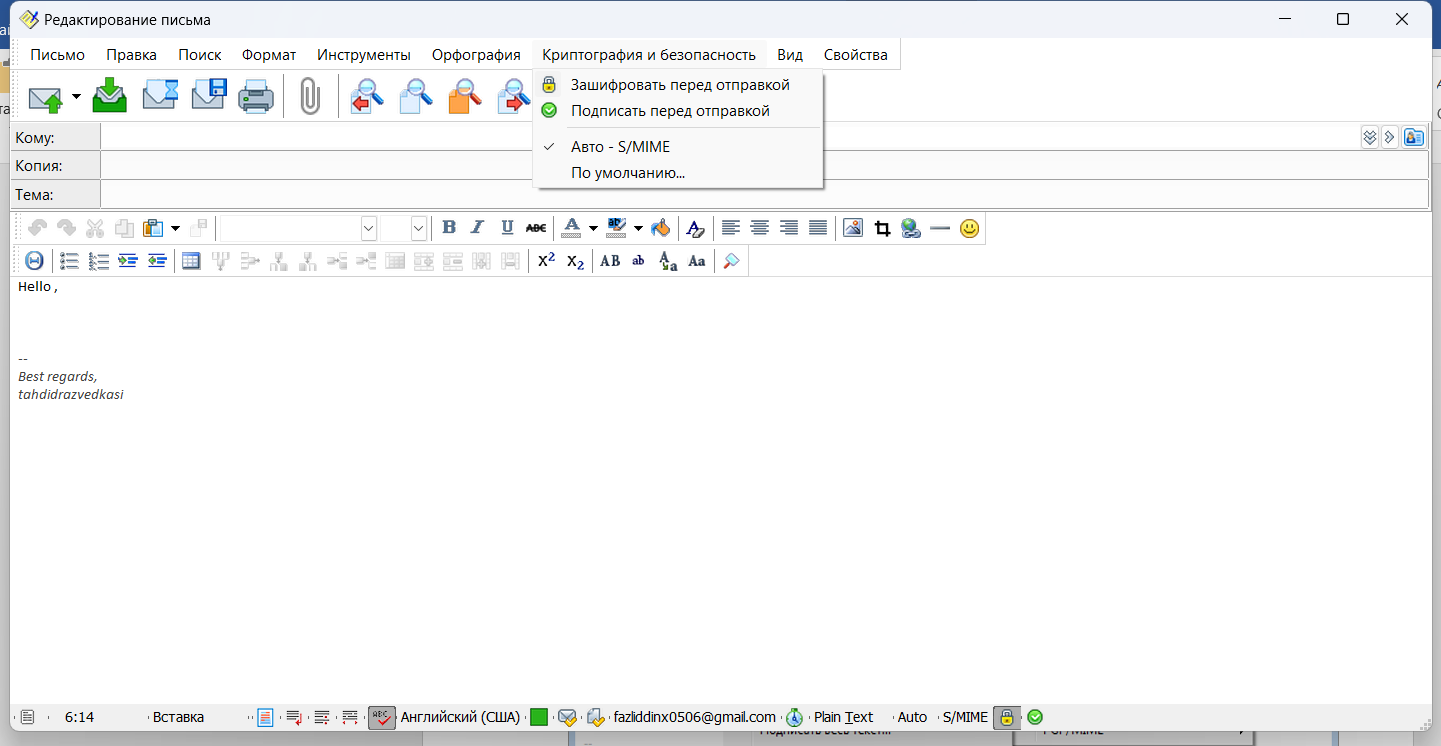
The Bat! dasturi pochta serverlari bilan aloqa o'rnatish uchun autentifikatsiya qilishning turli xil xavfsiz aloqa usullari bilan IMAP4, POP3 va SMTP protokollaridan foydalanadi. Ilova turli xil versiyalardagi SSL va TLS kriptografik protokollarini qo'llab-quvvatlaydi, bu esa mijozga tarmoq trafigini shifrlashdan foydalanadigan barcha pochta xizmatlari bilan o'zaro aloqada bo'lish imkonini beradi. The Bat dasturida ishonchli himoya qilish uchun pochta mijozining Professional nashrida mavjud bo'lgan va ruxsatsiz foydalanuvchilarning pochta serveridagi foydalanuvchi qayd yozuviga kirishini istisno qiladigan USB token qurilmasi bilan CRAM-MD5 autentifikatsiyasini qo'llab-quvvatlashni amalga oshiradi (3.10.- rasm).



3.10.- rasm. Pochta serverlari bilan ishlashda autentifikatsiya va shifrlash protokollarini qo'llab-quvvatlash

The Bat! dasturida nafaqat xavfsiz aloqa kanallaridan foydalanish, balki S/MIME, PGP va OpenPGP bilan shifrlangan elektron pochta xabarlarini yuborish va qabul qilish, shuningdek ularni elektron pochta orqali imzolash mumkin.

Dastlabki holatda, elektron pochta xabarlarining maxfiyligi va pochta serverida xabarlarning xavfsiz saqlanishi (agar u buzib tashlansa yoki xabarlar ushlab qolinsa, tajovuzkorlar xabarlarni o'qiy olmaydilar), ikkinchisida esa jo'natuvchini identifikatsiyalashdan tashqari, qabul qiluvchining yo'lida xatni o'zgartirishga bo'lgan har qanday urinish osongina aniqlanishi mumkin. Tegishli elementlar to'plami *«Криптография и безопасность»* menyusidagi elektron pochtalarni tahrirlash oynasida joylashgan. U bilan foydalanuvchi yordamida va avtomatik ravishda ham ishlashni amalga oshirish mumkin. Ushbu masala bo'yicha qo'shimcha ma'lumotlar pochta mijoziga biriktirilgan hujjatlarda taqdim etiladi (3.11.- rasm).



3.11.- rasm. Pochta jo'natishda kriptografiyadan foydalanish.

**5 – Amaliy ish.**

**Mavzu:** Razvedka hujumini amalga oshirishni o‘rganish

**Ishdan maqsad:** maxsus dasturiy vositalarni qo’llash orqali tarmoqda turli xil razvedka hujumlarini amalga oshirish, ularning imkoniyatlarini o’rganish va bu borada bilim va ko’nikmalarni shakllantirish.

**Nazariy qism:**

Tarmoq razvedkasi - mijozning axborot tizimi, axborot tizimining resurslari, foydalaniladigan qurilmalar va dasturiy ta'minot, ularning zaif tomonlari, himoya vositalari, shuningdek, axborot tizimiga kirish chegarasi to'g'risidagi ma'lumotlarni olish va qayta ishlash.

Tarmoq razvedkasi DNS so'rovlari, ping tekshiruvi va portni skanerlash shaklida bo'ladi. DNS so'rovlari ma'lum bir domenga kim egalik qilishini va ushbu domenga qanday manzillar tayinlanganligini tushunishga yordam beradi. DNS tomonidan topilgan manzillarga ping jo’natish sizga ma'lum bir muhitda qaysi xostlar ishlayotganligini ko'rish imkonini beradi. Xostlar ro'yxatini hisobga olgan holda, xaker ushbu xostlar tomonidan qo'llab-quvvatlanadigan xizmatlarning to'liq ro'yxatini tuzish uchun portni skanerlash vositalaridan foydalanadi. Va nihoyat, xaker xostlarda ishlaydigan ilovalarning xususiyatlarini tahlil qiladi. Natijada, xakerlik uchun ishlatilishi mumkin bo'lgan ma'lumotlar olinadi.

Zamonaviy tarmoq razvedkasi, faoliyatning maqsadlari, ko'lami va vazifalarni bajarish uchun qo'yilgan vazifalar xarakteriga qarab quyidagilarga bo'linadi:

* strategik.
* taktik;

Taktik razvedka hujumchilarning harakatlarini ta'minlaydi. Bularga tajovuzkorlar ham, axborot tizimini sinovdan o'tkazuvchi mutaxassislar ham kiradi. Taktik razvedka quyidagi ma'lumotlarni ochib beradi:

* texnik jihozlar,
* dasturiy ta'minot uskunalari,
* pochta serveridagi zaifliklar,
* xizmatlar va pochta mijozlari,
* tarmoq segmentlarining chegaralari,
* foydalanilgan aloqa kanallari (turi, tarmoqli kengligi),
* axborot tizimlariga hujumni rejalashtirish va amalga oshirish bo'yicha maqbul qarorlarni qabul qilishga yordam beradigan tarmoq va/yoki serverga davlat (geografik, tijorat) egalik qilish.

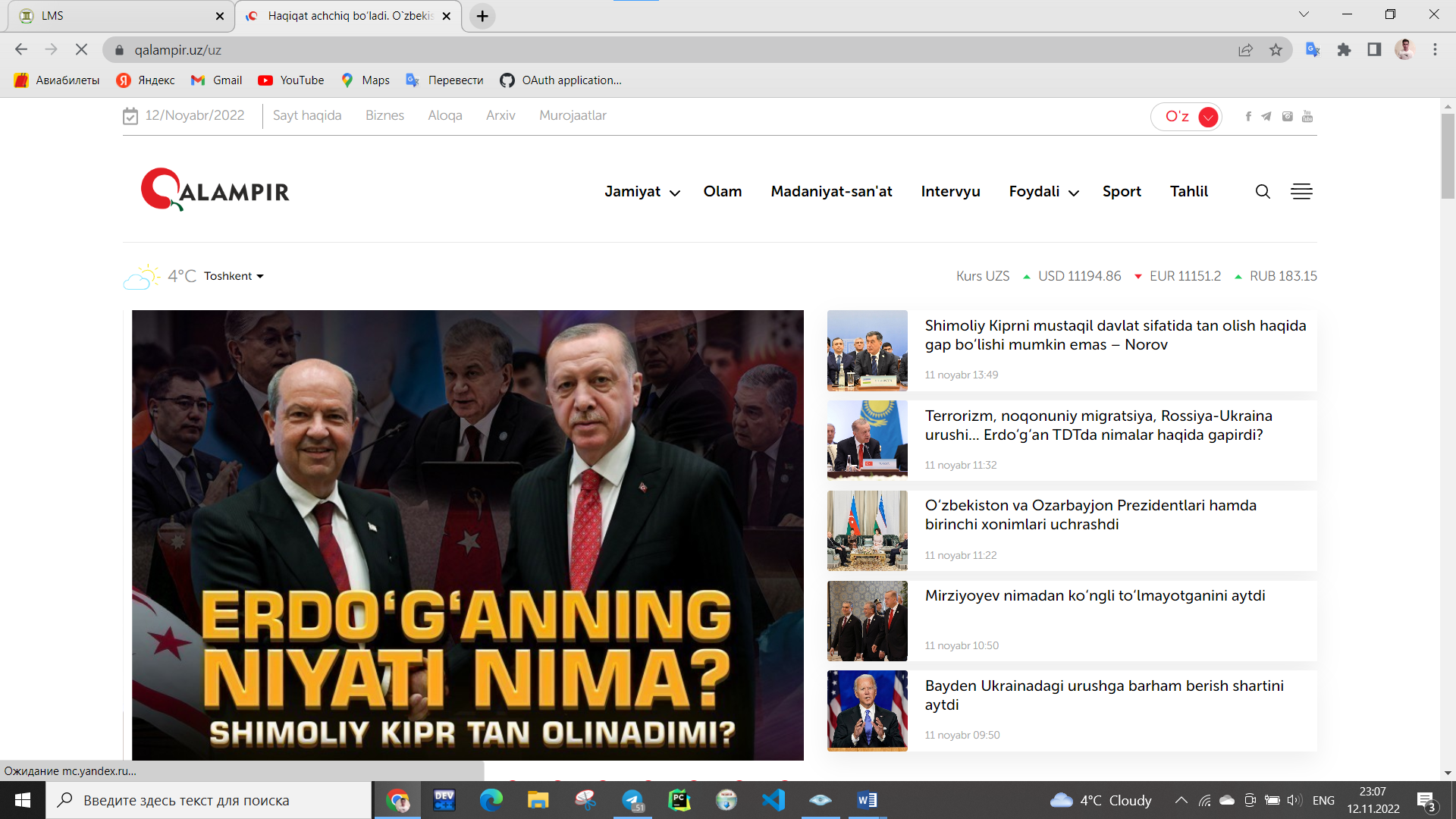
Ushbu ma'lumotlar elektron vositalar orqali uzatiladigan ma'lumotlarni ushlab turish orqali olinadi.

**Amaliy qism.**

**Nmap**

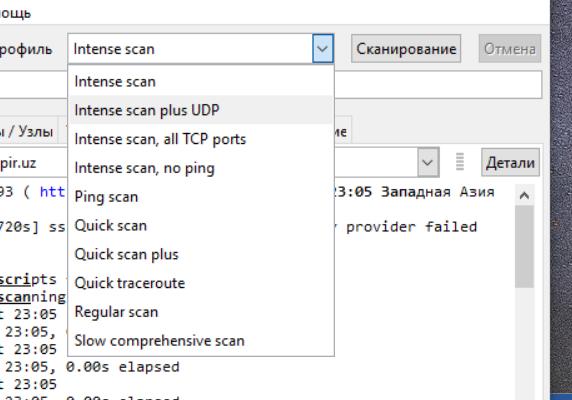
Nmap dasturiy vositasi tarmoqda mavjud domenning host tizimi, portlari, foydalanuvchi xizmatlari va ulardagi xavfsizlik vositalari haqida axborot yig’uvchi vosita hisoblanadi. Undan foydalanish interfeysning soddaligi tufayli qulaydir.

Dastlab bravzer orqali biz tekshirmoqchi bo’lgan saytimiz manzili aniqlab olinadi.



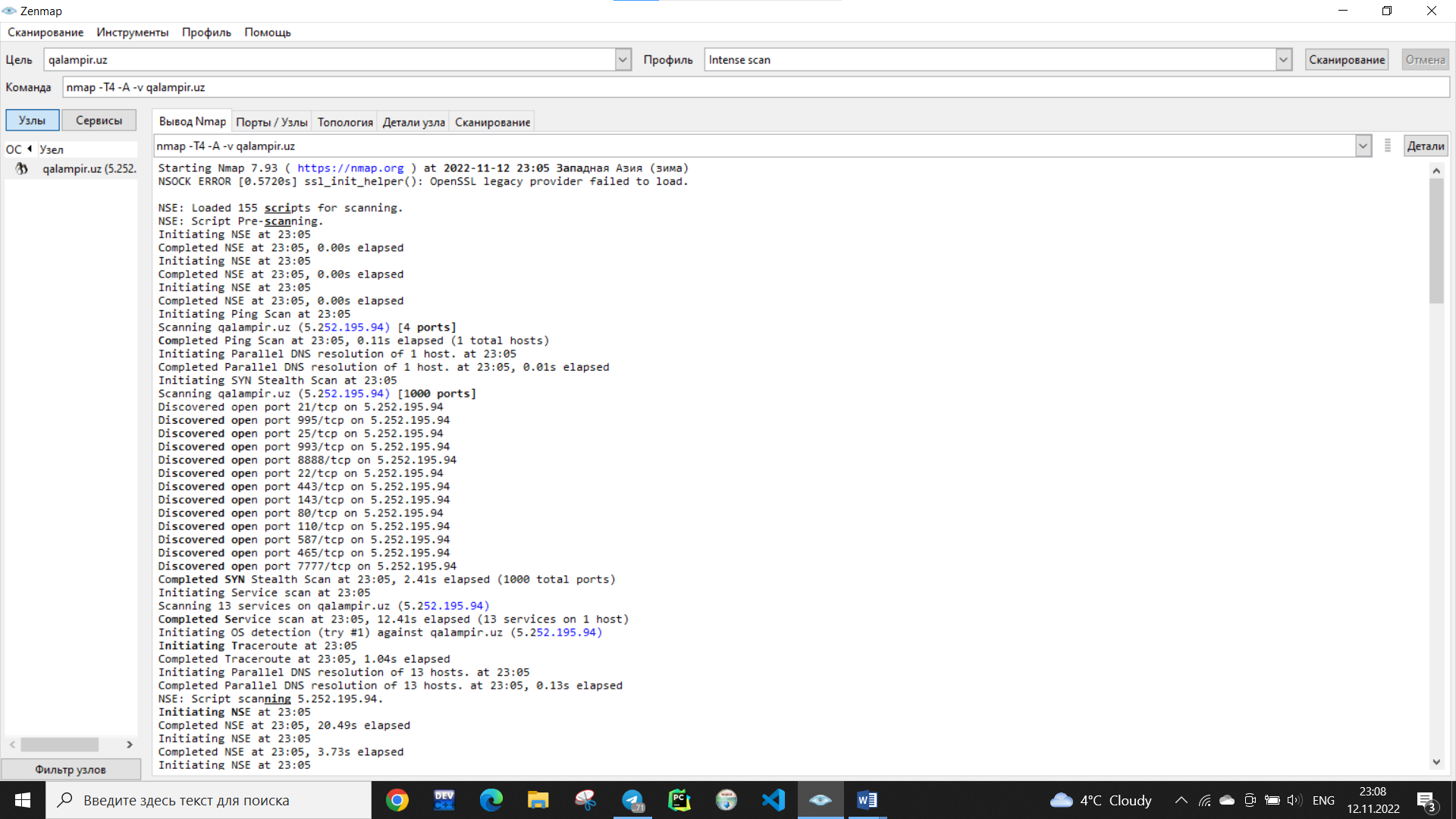
1-rasm. Sayt manzilini aniqlash

Aniqlangan manzil Nmap dasturiga qo’yiladi. Buning uchun dasturda “Nishon (Цель - Target)” qismi mavjud bo’lib, u tekshirilishi lozim bo’lgan sayt manzilini qabul qiladi. So’ngra “Skanerlash” tugmasi bosiladi. Bundan oldin “Profil” qismidan bizga kerakli bo’lgan skanerlash turi tanlanadi.



2-rasm. Skanerlash profillari

“Skanerlash” tugmasi bosilganidan so’ng, dastur biz kiritgan manzilni tekshirish boshlaydi. Tekshirish “Nmap Done” xabari chiqmagunigacha davom etadi.

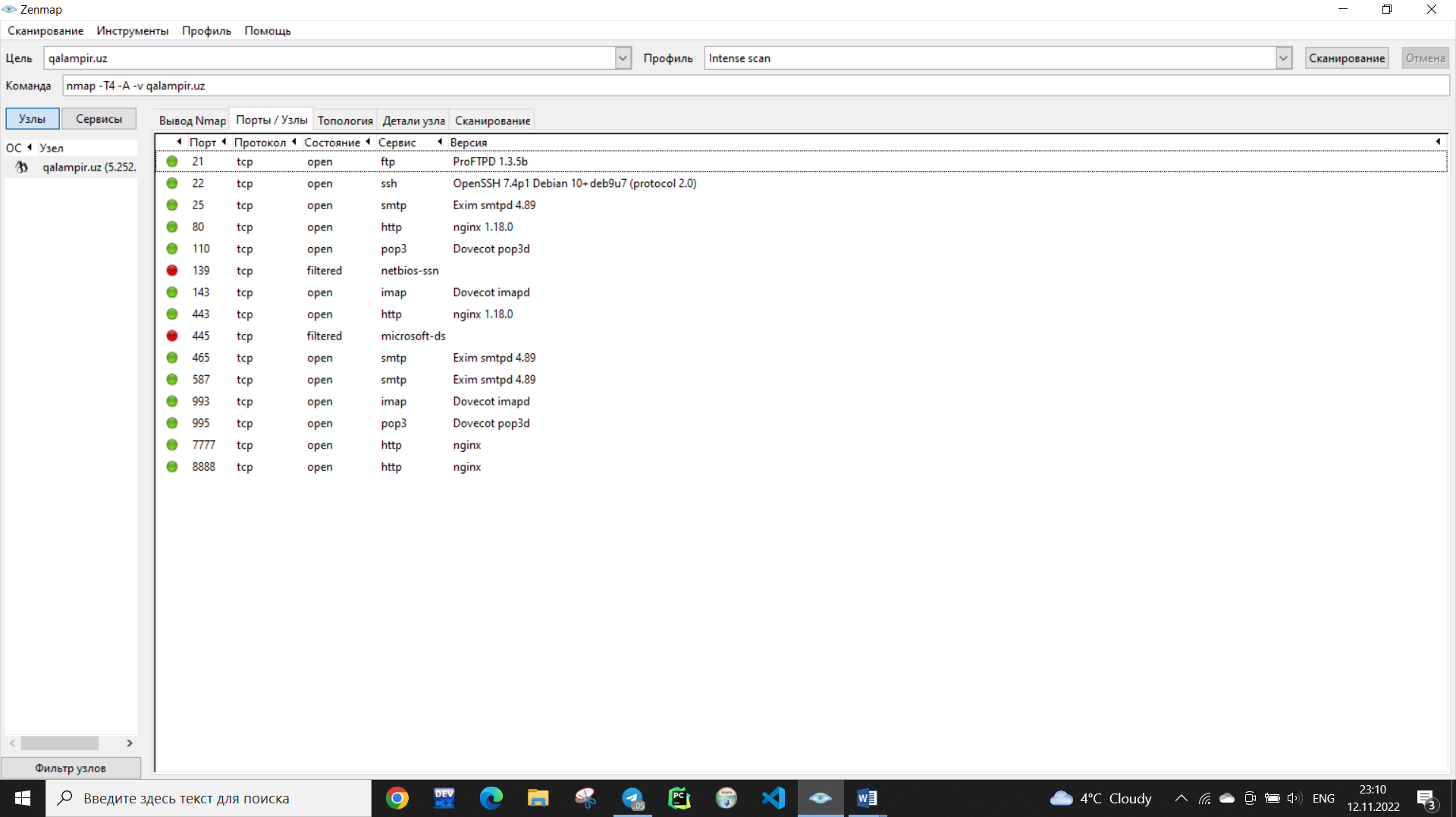


3-rasm. Skanerlash jarayoni

Dasturning asosiy oynasida skanerlash jarayoni tugaguniga qadar barcha xabarlar ketma-ketligi berib boriladi.

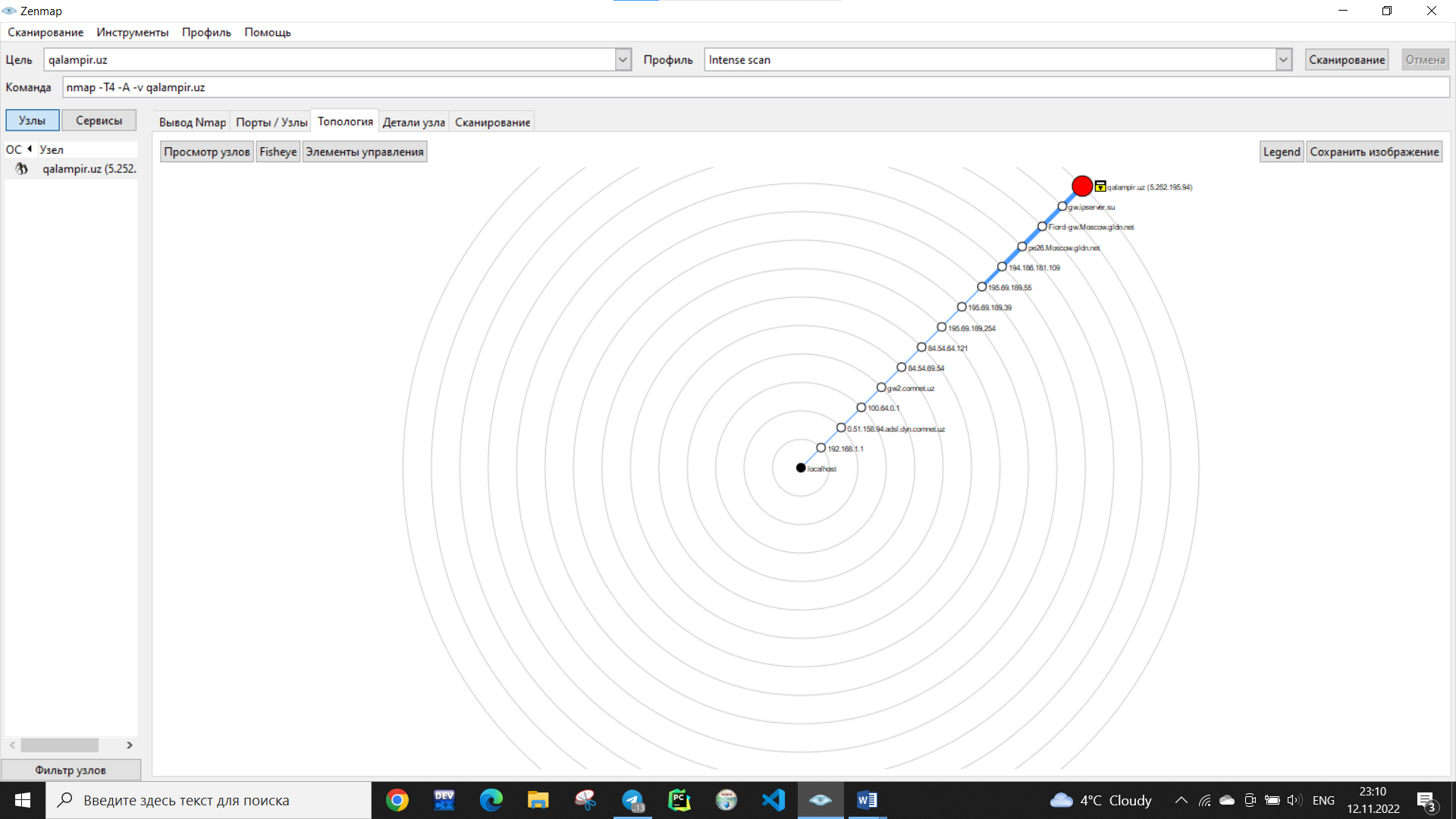
4-rasm. Skanerlash yakunlangan holati

Dasturning “Portlar (Ports - Порты)” bo’limida biz skanerlagan sayt o’rnatilgan hostdagi ochiq yoki firewall yordamida bloklangan portlar ro’yhati, ulardan foydalanuvchi xizmatlar, portlar holati, protokoli va versiyasi haqida ma’lumot olishimiz mumkin.



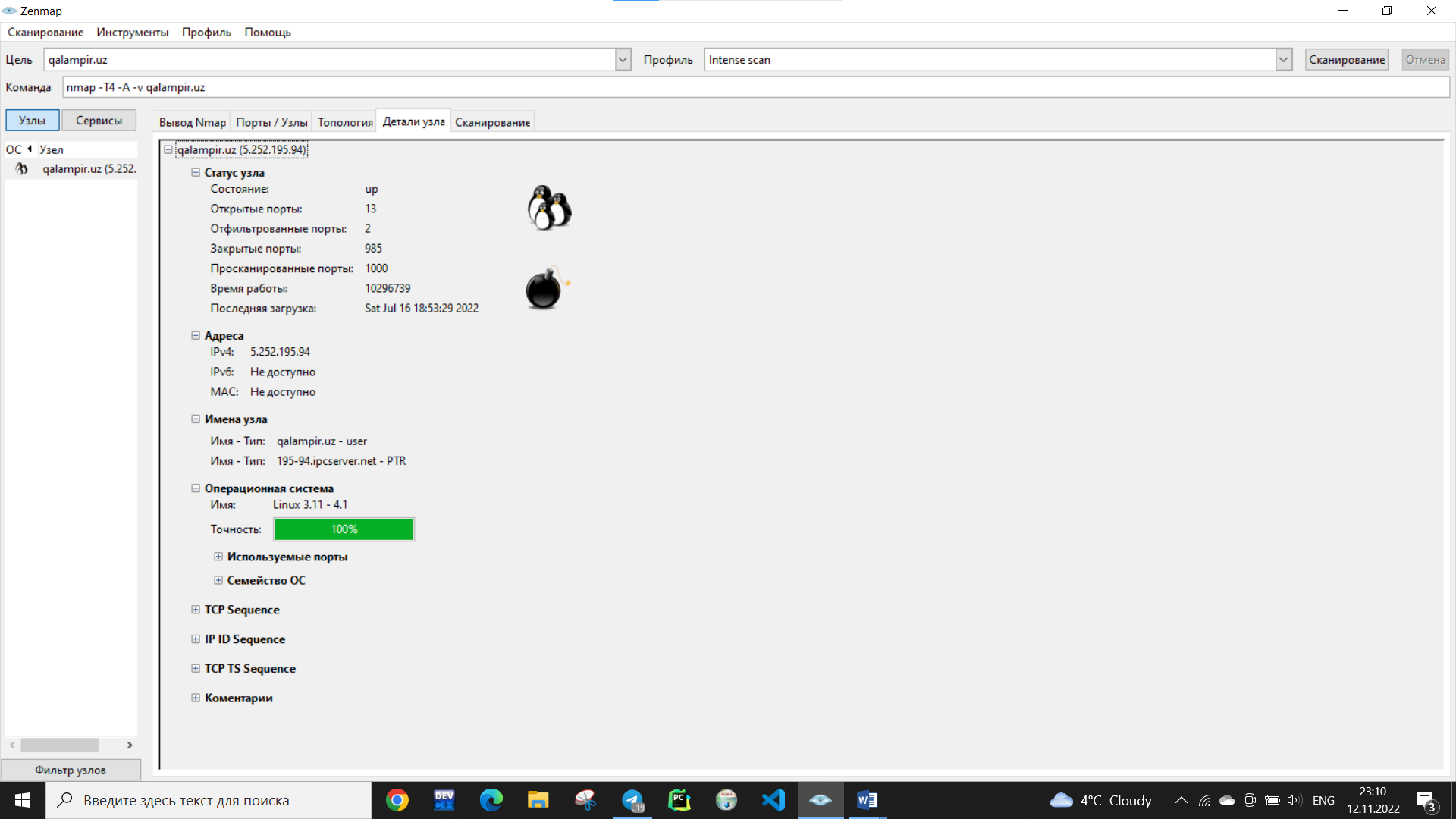
6-rasm. Portlar (Ports - Порты) bo’limi

Dasturning “Topologiya” bo’limida bizning tarmoq qurilmamizdan sayt faoliyat olib boruvchi hostgacha asosiy yo’nalishni ko’rishimiz mumkin.



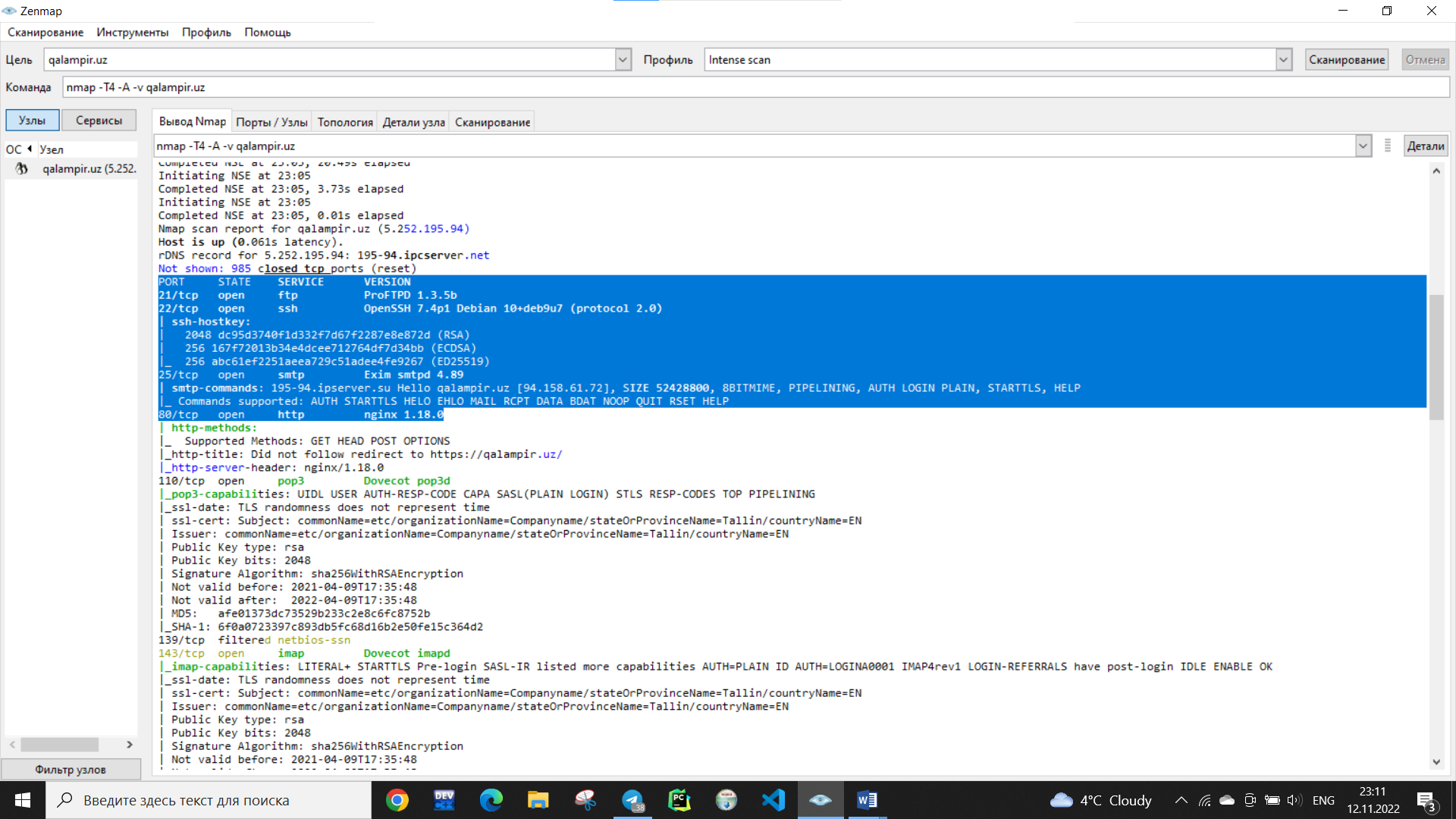
7-rasm. Topologiya oynasi

“Uzel parametrlari (Getaway detail – Детали узла)” bo’limida hostda o’rnatilgan OT va skanerlashning umumiy natijalarini ko’rish mumkin.

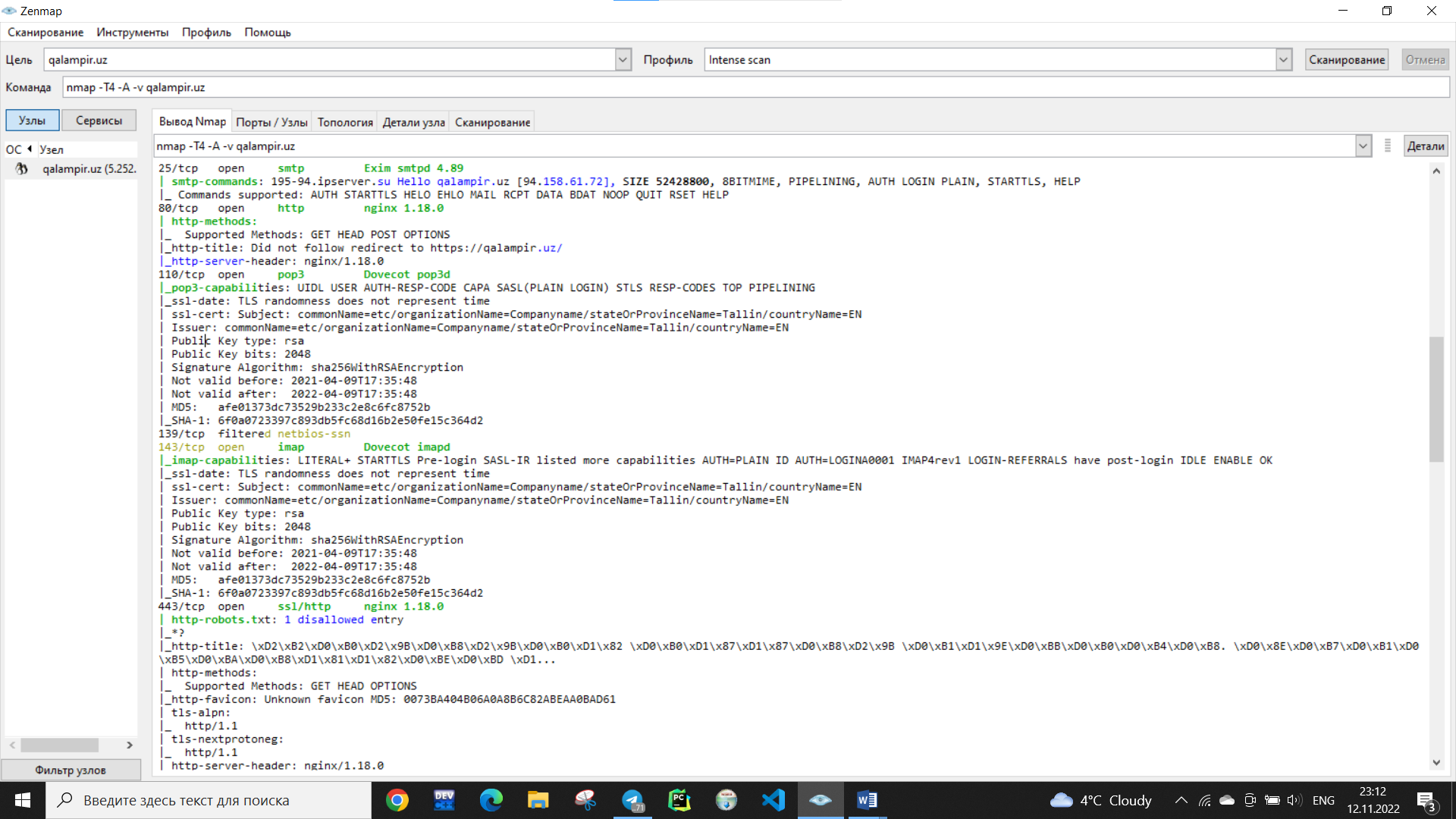


8-rasm. Uzel parametrlari bo’limi

Dasturning asosiy oynasida saytdagi xavfsizlik parametrlari haqida to’liqroq ma’lumot olish mumkin. Masalan, ssl sertifikati, kalitlar haqida ma’lumot, ssh protokoli va hokazo.



9-rasm. SSL sertifikati haqida ma’lumot



10-rasm. ftp va ssh haqida ma’lumot