DOI: https://doi.org/10.5281/zenodo.12542394

XAVFSIZ FILTRLASH VOSITALARINI AYLANIB O‘TISH VA BLOKLANGAN SAYTLARGA RUXSATSIZ KIRISH YO‘LLARI TAHLILI

Jumayev Sodiqjon Nuraliyevich
Denov tadbirkorlik va pedagogika instituti, Surxondaryo, O‘zbekiston
jumayev.sodiq9091@mail.ru

Anotatsiya. *Ushbu maqolada bloklangan saytlarga kirish usullari, yo‘llari va vositalari shuningdek, anonimlikni ta’minlash maqsadida qaysi vositadan foydalanish afzalligi haqida tahliliy ma’lumotlar keltirilgan.*

Kalit so‘zlar: *filtrlash, bloklangan sayt, anonimlik, ruxsatsiz kirish.*

Аннотация. *В данной статье представлена аналитическая информация о способах, пути и средствах доступа к заблокированным сайтам, а также о том, какой инструмент лучше всего использовать для обеспечения анонимности.*

Ключевые слова: *фильтрация, заблокированный сайт, анонимность, несанкционированный доступ.*

Annotation. *In this paper is given analytical information about the methods, ways and tools of accessing blocked sites, as well as which tool is best to use to ensure anonymity.*

Keywords: *filtering, blocked site, anonymity, unauthorized access.*

KIRISH

Internetning shiddat bilan rivojlanishi natijasida dunyoda axborotni tarqatish va undan foydalanishga talab ortib ketdi. Internetga bo‘lgan qiziqish va u orqali amalga oshiriladigan biznesning kengayishi Internet foydalanuvchilari uchun arzon va qulay

kommunikatsiya tarmog‘ining hosil bo‘lishiga olib keldi. Korxonalar Internet kanallaridan o‘zining tijorat va boshqaruv axborotlarini uzatish va qabul qilish imkoniyatlariga ega bo‘ldi.

Bundan tashqari, internet tarmog‘ining rivojlanishi natijasida turli insonlar ma’naviyati va madaniyatiga zid, yosh avlod tarbiyasini butunlay o‘zgartirib yuboradigan axborotlar, xizmatlar va kompyuter o‘yinlari kirib kelmoqda. Kompyuter va axborot texnologiyalarining yuqori darajada rivojlanishiga qaramay ushbu ma’lumotlarni kirib kelishini to‘sish yoki taqiqlash imkonsizligicha qolmoqda. Chunki, har soniyada millionlab sahifalarda yangi axborotlar hosil bo‘ladi. Ularni oldini olish uchun esa, ushbu maqsaddagi ma’lumotlar borligi aniqlansa, saytni to‘liqligicha bloklash amalga oshirilmoqda.

Internet tarmog‘ida axborot oqimining ortishi va uning salbiy ta’sirlarini kamaytirish maqsadida provayderlarda turli filtrlash vositalaridan foydalaniladi. 2018-yilda Xitoy Xalq Respublikasi hududida ko‘plab xorijiy saytlarga ulanish Buyuk Xitoy tarmoqlararoekran tizimi yoki internetdagi kontentlarni filtrlovchi tizim — «Oltin qalqon» loyihasi bilan bloklangan edi[1]. Uning asosiy sababi Xorijiy resurslarning “Aholi uchun halokatli” axborotlarning ehtimoliy tarqalishini oldini olish sifatida ko‘rsatilgan. Axborotga bo‘lgan ehtiyojning o‘rnini qoplash uchun esa, Xitoy kompaniyalari ularning milliy namunalarini yaratishgan.

ASOSIY QISM

F.M.Muxtarovning PHD dissertatsiyasida[2] davlatlararo munosabatlarda kritik axborot infratuzilmasida shaxs, jamiyat va davlat xavfsizligiga tahdidlarni hisoblash va kontentlarni filtrlash usullari va algoritmlari ishlab chiqilgan. Ular yordamida ayrim turdagi axborotlarni filtrlashga erishish mumkinligi ko‘rsatib o‘tilgan.

Shuningdek, T.N. Qori Niyoziy nomidagi O‘zbekiston pedagogika fanlari ilmiy tadqiqot instituti tomonidan “Telekommunikatsiya tizimining globallashuvi sharoitida bolalar axborot xavfsizligini ta’minlash bo‘yicha ota-onalar uchun tavsiya” deb nomlangan qo‘llanma[3] ishlab chiqilgan va unda Internet - Xorijiy ommaviy axborot vositalarining bola shaxsini destruktiv manipulyatsiya qilishini oldini olish yuzasidan hamda internet kontentlarini texnik jihatdan filtrlash imkoniyati mavjud bo‘lmagan yoki murakkablashgan hollarda tarbiyaviy usullar orqali farzandlarimizni ma’naviy immunitetini shakllantirish bo‘yicha tavsiyalar keltirilgan.

[1] https://vc.ru/future/37403-za-stenoy-kak-kitayskiy-internet-razvivaetsya-posle-blokirovok-inostrannyh-servisov.
[2] Muxtarov F.M. “Xavfsizlikni ta’minlash tizimi modellari va davlatlararo munosabatlar strategiyasini muvofiqlashtirish algoritmlari” falsafa doktori (PhD) dissertatsiyasi.
[3] https://lib.jspi.uz.

Bundan tashqari, “Kiberxavfsizlik markazi” DUK tomonidan 2016-yilda ishlab chiqilgan “Onlayn muhitda yoshlarni himoya qilish bo‘yicha qo‘llanma” bolalarni Internet tarmog‘idagi xavf-xatarlardan asrash va ularning axborot xavfsizligi me’yorlariga rioya qilishlari bo‘yicha tavsiyalar bayon etilgan.

Yuqorida keltirilgan manbaalarga tayanib shuni aytish mumkinki, ma’naviyat uchun xavfli bo‘lgan kontentlarni filtrlash maqsadida ishlab chiqilgan tavsiyaviy xarakterga ega qo‘llanmalar to‘laqonli himoyani ta‘minlay olmaydi. Buning uchun davlatning axborot xavfsizligini ta’minlash borasidagi siyosati darajasidagi choralarni ko‘rish tavsiya etiladi.

Hozirgi kunda quyidagi texnik filtrlash usullari mavjud:

- IP manzili bo‘yicha blokirovkalash;
- DNS yozuvlarini buzish;
- URL orqali blokirovkalash;
- paketli filtrlash;
- HTTP proksi-server orqali filtrlash;
- tarmoqni uzib qo‘yish;
- qidiruv natijalarini filtrlash.

Keltirilganlarning barchasi statik ma’lumotlarga tayanadi. Ya’ni filtrlanishi lozim bo‘lgan saytning manzili yoki u haqidagi kalit so‘zlar kiritiladi, natijada ushbu so‘z yoki manzilli sayt bloklanadi. Ammo, niqoblangan yoki dinamik DNS nomidan foydalanadigan saytlar uchun ushbu harakatlar besamara bo‘lishi mumkin.

Kontentlarni filtrlash quyidagi darajalarda bo‘ladi:

- xalqaro shlyuz;
- internet-provayderda;
- internet sayt yoki tashkilot tarmog‘ida;
- shaxsiy kompyuterlarda.

Bundan tashqari, odatiy ko‘rinishga ega sayt yoki ijtimoiy tarmoqlarda davlat siyosatiga qarshi qaratilgan, diniy ekstremizm, terrorizm, narkotik moddalar iste’moli, pornografik ruhdagi videokontentlarni ko‘plab uchratish mumkin. Mamlakatimizda mashxo‘r Instagram, Youtube, Telegram, Facebook va boshqa shu kabi ijtimoiy tarmoqlarda yuqorida keltirilgan mavzulardagi video kontentlar ko‘plab joylanmoqda. Ularning siyosatida kontentlarni filtrlash bo‘yicha qoidalar mavjud, ammo ular ham to‘laqonli natijani bermaydi. Bunga yaqqol misol sifatida yuqorida keltirilgan ijtimoiy tarmoqlardagi pornografik ko‘rinishdagi video kontentlarni keltirish mumkin. Ushbu tarmoqlarda ro‘yxatdan o‘tgan ixtiyoriy foydalanuvchi ushbu kontentlarni tomosha qilishi mumkin. Bu esa, yoshlarning ma’naviyatiga va vaqtini turli samarasiz maqsadlarda o‘tkazishiga olib keladi.

Shunday bo‘lsada, xorijiy saytlarda (bloklangan) nashr etilgan mamlakatimiz va uning mavqeyini tushirishga qaratilgan axborotlarni aniqlash hamda ularni bartaraf etishga qaratilgan chora-tadbirlarni ishlab chiqish maqsadida ushbu saytlarga aylanib kirish yo‘llaridan foydalaniladi.

Insoniyat har doim cheklangan narsalardan foydalanish, ko‘rish va uni buzishga harakat qiladi. Bunga yaqqol misof sifatida O‘zbekistonda “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonun asosida Twitter, TikTok, Skype va Vkontakte platformalari faoliyatiga cheklov qo‘yilgan edi[1]. Foydalanuvchilar tomonidan ushbu ijtimoiy tarmoq va taqiqlangan saytlarga kirish uchun turli anonimayzer, proksi server kabi vositalar qo‘llanilmoqdaki, natijada ushbu sahifalarga ulanish va undagi axborot va xizmatlardan foydalanish imkoniyati yuzaga kelmoqda.

Bloklangan saytlarga aylanib kirishning quyidagi yo‘llari va vositalar mavjud:

VPN (Virtual Private Newtwork) – virtual himoyalangan tarmoq.

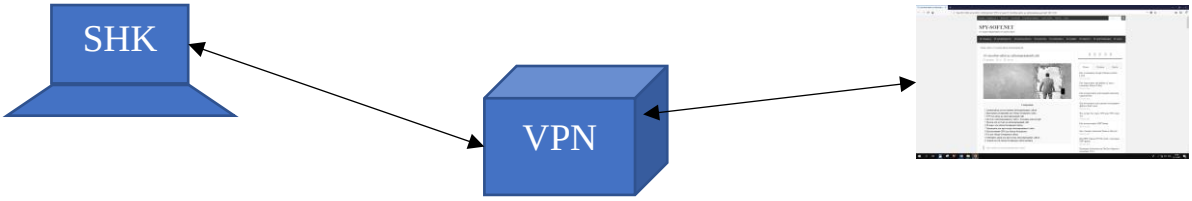
Virtual tarmoqlarni qurish konsepsiyasi asosida yetarlicha oddiy g‘oya yotadi: agal global tarmoqda axborot almashinuvchi ikkita kanal bo‘lsa, bu kanallar orasida ochiq tarmoq orqali uzatilayotgan axborotning konfidensialligini ta’minlovchi virtual himoyalangan tunnel qurish zarur. Bu virtual tunneldan uzatiladigan ma’lumotlar ruxsati mavjud bo‘lmagan shaxslar va tashqi kuzatuvchilardan himoyalangan.

Shunday qilib, VPN tunneli ochiq tarmoq orqali o‘tkazilgan ulanish bo‘lib, u orqali virtual tarmoqning kriptografik himoyalangan axborot paketlari uzatiladi. Axborotni VPN tunneli bo‘yicha uzatilishi jarayonidagi himoyalash quyidagi vazifalarni bajarishga asoslangan:

– o‘zaro aloqadagi taraflarni autentifikatsiyalash;
– uzatiluvchi ma’lumotlarni kriptografik berkitish (shifrlash);
– yetkaziladigan axborotning haqiqiyligi va yaxlitligini tekshirish.

VPNning asosiy xususiyati shundan iboratki, u jo‘natuvchi va qabul qiluvchining ma’lumotlari (IP manzillari)ni ham shifrlaydi. Shuning uchun so‘rov jo‘natuvchi va qabul qiluvchilar haqidagi ma’lumorlarni aniqlash murakkab.

Quyidagi rasmda shaxsiy kompyuter va veb saytni bog‘lashda VPNdan foydalanish sxemasi keltirilgan.



1-rasm. VPN shlyuz ulanishi

[1] https://kun.uz/uz/news/2021/07/07/

VPN texnologiyasi nafaqat axborot himoyasida, balki uning qabul qiluvchi va jo‘natuvchi manzillarini shifrlash xususiyatidan taqiqlangan saytlarga kirish maqsadida ham foydalaniladi. Buning uchun, oddiy foydalanuvchi sifatida mobil qurilma yoki kompyuterga VPN dasturi o‘rnatiladi va taqiqlangan saytlarga kirish imkoniyati yuzaga keladi.

Saytlar odatda IP manzili yoki DNS nomi orqali cheklov o‘rnatiladi. VPN esa, yuqorida ta’kidlanganidek, saytning manziliga tegishli ma’lumotlarni shifrlaydi.

2-rasmda taklif etilayotgan VPN manzillar va uning ma’lumotlari keltirilgan. Agar bitta VPN IP manzili faol holatda bo‘lmasa boshqasini tanlash mumkin.

	Proxy	Port	Version	Speed	Country	Region	City	Distance	Email	UDP
✓	50.149.118.201	43078	Socks5	medium	United States	Washington	Redmond	near	No	No
✓	179.210.48.15	44430	Socks5	slow	Brazil	Rio de Janeiro	Rio De Janeiro	medium	Yes	No
✓	218.24.88.85	1080	Socks4	fast	China	Liaoning	Shenyang	medium	No	No
✓	74.51.153.215	45554	Socks5	slow	United States	California	San Bruno	near	No	No
✓	78.22.96.71	44816	Socks5	fast	Belgium	Oost-Vlaanderen	Merelbeke	medium	No	Yes
✓	75.127.28.212	45554	Socks5	medium	United States	Wyoming	Rozet	near	No	Yes
✓	75.109.215.177	45554	Socks5	fast	United States	Texas	College Station	near	No	Yes
✓	24.192.17.82	45554	Socks5	slow	United States	Michigan	Southgate	near	No	No
✓	92.220.244.154	64272	Socks5	medium	Norway	Vestfold	Sandefjord	medium	No	No
✓	87.92.149.75	45554	Socks5	slow	Finland	Western Finland	Naantali	medium	No	Yes

2-rasm. VPN uchun taklif etilgan manzillar va ularning xususiyatlari.

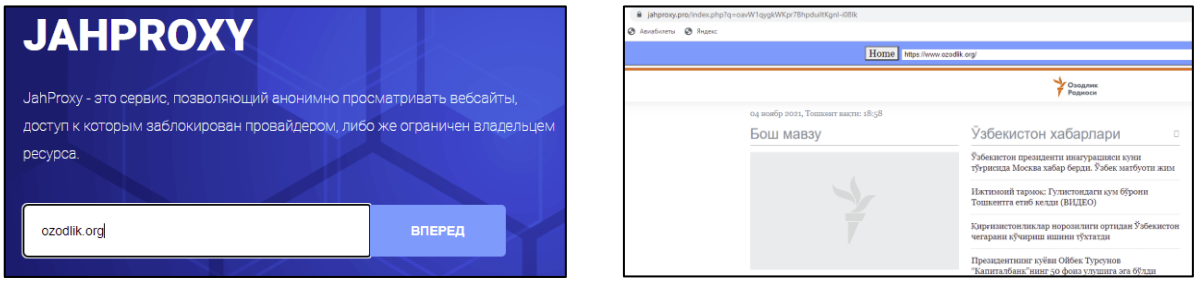
Hozirgi kunda Free VPN, Hola Unlimited Free VPN, Turbo VPN, ExpressVPN, Free VPN Tomato, NordVPN kabi dasturlar keng foydalanilmoqda. Ushbu dasturlardan cheklangan saytlarga kirish va konfidensiallikni ta’minlash maqsadida foydalanish mumkin. Shuningdek, ushbu dasturlarning brauzer kengaytmalari mavjud bo‘lib, uni ishga tushirish va o‘chirish bitta tugma orqali amalga oshiriladi.

ANONIMAYZERLAR.

Foydalanish va kirish cheklangan veb xizmatlar va saytlarga, ularning taqiqlarini chetlab kirishga imkon beradigan barcha vositalarni anonimayzerlar deb aytish mumkin. Shuningdek, mutaxasisslar tomonidan Anonimayzer vasifasini bajaruvchi saytlar ham mavjud bo‘lib, ushbu saytlarga tashrif buyurganimizda taqiqlangan saytning manzilini yozish qismi mavjud va shu orqali taqiqlangan saytga kirishga erishiladi.

Misol sifatida Jahproxy[1] anonimayzerida provayder tomonidan foydalanilishi cheklangan veb sayt nomi kiritiladi va u taqiqlangan saytga anonim holatda kirishni ta’minlab beradi. Ya’ni anonimayzer taqiqlangan saytga O‘zbekiston hududidan emas, boshqa davlatdan kirilmoqda deb ko‘rsatadi. 3-rasmda provayderlar tomonidan cheklangan *ozodlik.org* saytiga tashrif bo‘lganini ko‘rish mumkin.

[1] https://jahproxy.pro/



3-rasm. Jahproxy yordamida cheklangan saytga kirish

VPN va anonimayzerlarning bloklangan saytlarga kirishda vazifasi bir xil bo‘lsada, xususiyatlari turli. Quyidagi jadvalda uning ayrim xususiyatlari tahlili keltirilgan.

1-jadval. VPN VA ANONIMAYZER TAHLILI

Xususiyatlar	VPN	Anonimayzer
Internet trafigini tinglash va yozishdan himoyalangan	Yuqori	Past
Internet provayderni bloklash mumkin emas	+	-
O‘yin va ilovalar bilan ishlashi	+	-
Turli qurilmalarni qo‘llab-quvvatlaydi (telefon, router)	+	-
Deyarli barcha mamlakatlarni qamrab olgan	+	-
Yuqori tezlik	+	-
Foydalanish faktini berkitish	+	-
Shaxsiy ma’lumotlarni berkitish	+	+
Saytlar uchun foydalanuvchi IP manzilini berkitish	+	+

Anonimayzerlar saytlarni tez va barcha funksional imkoniyatlari bilan birgalikda ochish va foydalanishga imkon beradi. Undan faqat yangilik saytlariga tashrif maqsadida foydalanish lozim. Autentifikatsiya (login, parol), kredit kartalari va boshqa shunga o‘xshash bloklangan saytlarga bu usul orqali kirish tavsiya etilmaydi.

Proksi-server.

Uning asosiy maqsadi tashkilot yoki korporativ tarmoq foydalanuvchilarining yagona IP manzil orqali global tarmoqqa chiqishini ta’minlab beradi. Demak, taqiqlangan saytlarga mavjud IP manzil bilan emas, proksi-serverda ko‘rsatilgan manzil orqali kiradi. Shuning uchun provayderda cheklangan manzillar (O‘zbekiston yoki boshqa davlat) ro‘yxatida foydalanuvchining manzili aniqlanmaydi.

Quyidagi jadvalda ayrim Proksi server IPlarini taqdim etuvchi va server sifatida faoliyat yurituvchi saytlarning tahlili keltirilgan.

2-jadval. Proksi server saytlarining tahlili

Xususiyatlari	Cameleo.ru	Dostyp.ru	HideMe.ru	NinjaClaok.com	VTunnel.com
Davlat	Rossiya	Rossiya	Rossiya	AQSh	AQSh
Ishlash tezligi	A'lo	A'lo	Yaxshi	Qoniqarli	Qoniqarli
Sozlanmasi mavjudligi	-	-	+	+	+
Proksini tanlash imkoniyati	-	+/-	+	-	+
Reklama va boshqa bloklar	+	-	+	+	+
O'zining reklamasi	-	-	+	++	++
Flesh xotirani qo'llashi	+	+	+	Uzoq yuklaydi	+

Eng keng tarqalgan HTTP proksi server 3 ta darajada ishlaydi:

1-daraja. Yuqori darajali anonimlik.

2-daraja. Anonim holatda saytlardan foydalaniladi, ammo joriy IP manzilni aniqlash imkoniyati mavjud emas.

3-daraja. Shaffof proksi-server, joriy IP manzilni aniqlash imkoniyati mavjud.

Hozirgi kunda HTTPS va SOCKS proksilar keng tarqalgan.

Darknet.

Darknet (inglizcha DarkNet, "Yashirin tarmoq", "Qorong'u tarmoq", "Soya tarmog'i" kabi ma'nolarni anglatib, "Dark web" nomi bilan ham tanilgan) - yashirin tarmoq, faqat ishonchli va teng huquqli ishtirokchilar o'rtasida nostandart protokol va portlardan foydalangan holda hosil qilinadigan tarmoq.

Anonim tarmoq - bu shifrlangan ma'lumotlarni uzatishni ta'minlaydigan bog'lanmagan virtual tunnellar tizimi. Darknetning boshqa taqsimlangan nuqta-nuqta (P2P) tarmoqlaridan farqi shundaki, fayl almashish anonim tarzda amalga oshiriladi. Foydalanuvchilar tarmoqda yopiq IP manzil asosida hukumat aralashuvisiz muloqot qilishi mumkin. Shuning uchun ushbu tarmoq ko'pincha turli yer osti va noqonuniy faoliyatda aloqa vositasi sifatida qabul qilinadi.

"Darknet" atamasi 1970-yillarda xavfsizlik maqsadlarida ARPANETdan ajratilgan tarmoqlarga nisbatan ishlatilgan, keyinchalik u Internetning alohida tarmog'iga aylangan. Darknet ishtirokchilari ARPANETdan ma'lumot olishi mumkin,

ammo uning manzillari tarmoqlar ro‘yxatida ko‘rinmaydigan va tashqaridan kelgan so‘rovlarga javob bermaydigan texnologiyalar asosida qurilgan.

Darknetdan quyidagi maqsadlarda foydalanish mumkin:

– Maxfiylikni ta’minlash va siyosiy repressiyalardan himoya qilish.
– Axborot texnologiyalari sohasidagi jinoyatlar.
– Mualliflik huquqi bilan himoyalangan fayllarni tarqatish.
– Terrorizm.
– Kiberrazvedka.

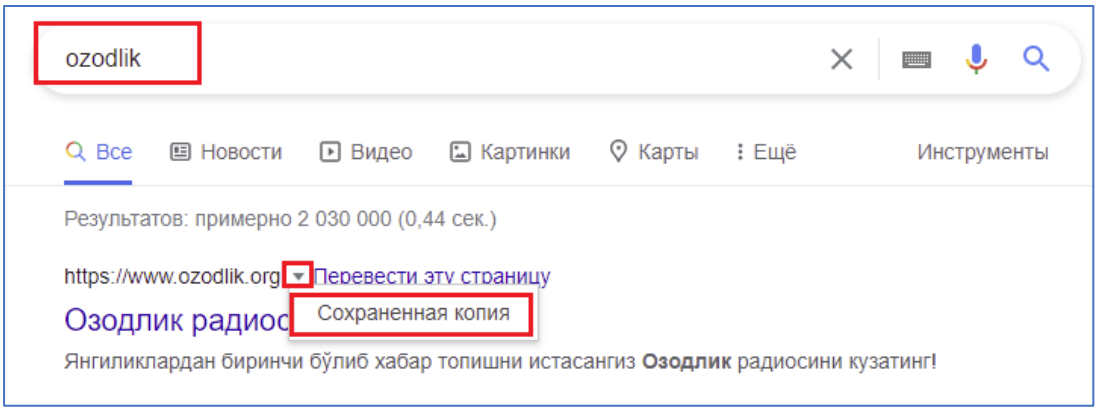
Ko‘pgina Darknet tarmoqlariga kirish uchun maxsus dasturlarni o‘rnatish talab etiladi. Quyida ayrim mashxo‘r Darknet tarmoqlari keltirilgan:

– Tor anonim tarmoqlar uchun eng mashxo‘r dasturlardan biri bo‘lib, u Darknetga kirish uchun ham qo‘llaniladi.
– I2P.
– RetroShare.
– Freenet.
– GNUnet.

Oxford universiteti tadqiqotlariga ko‘ra, Tor dasturidan eng ko‘p foydalanadigan davlatlarga Italiya, Moldova, Isroil tegishli. Ularda o‘rtacha bir kunda 100 mingta internet foydalanuvchidan 200 tadan ortig‘i ushbu anonim tarmoqdan foydalanadi. Ispaniya, Fransiya, Niderlandiya, Eron va Suriya kabi davlatlarda nisbatan kamroq, ya’ni 100-200 oralig‘ida.

Google keshi yordamida kirish.

Saytdagi ma’lumotlarni joriy holati bo‘yicha ko‘rish lozim hollarda saytning google qidiruv tizimi keshida saqlangan qismlarini ko‘rish mumkin. Buning uchun quyidagi rasmda tasvirlangan amallarni bajarish lozim.



4-rasm. Google kesh orqali bloklangan sahifaning dastlabki oynasini ko‘rish

Bloklangan saytga google orqali kirish quyidagi ketma-ketlikda amalga oshiriladi:

IP manzillardan foydalanish.

Bloklangan saytga kirishning keyingi usuli sifatida URL (sayt nomi) manzil o‘rniga uning IP-manzilidan foydalanishni keltirish mumkin. Ba’zan saytni blokirovka qilish sayt nomini qora ro‘yxatga qo‘shish orqali amalga oshiriladi. Bunday hollarda ushbu usul yordam beradi.

Bloklangan ozodlik.org saytining IP manzili 104.81.235.125 ko‘rinishga ega.

Ushbu bloklangan saytning IP manzilini *ping ozodlik.org* buyrug‘ini kiritish orqali oson aniqlash mumkin. Lekin ushbu yo‘l doim ham samara bermasligi mumkin. Chunki, ko‘pchilik blokatorlar IP manzilni ham o‘z ichiga oladi.

Tarjimondan foydalanish.

Online tarjimon saytlari yordamida bloklangan sayt manzili kiritiladi va tarjima qilingan varianti orqali ushbu saytga kirish mumkin. *Google tarjimonning* tarjima variantidagi manzil ustiga sichqonchaning chap tugmasini bosish orqali ushbu saytga kiriladi.

Yandex tarjimon saytida internet manzillarni tarjima qiladigan alohida funksiyasi mavjud. Uning yordamida sayt tarjimasini Yandex sahifasining o‘zida ko‘rish mumkin.

Shuningdek, bloklangan saytlarga kirishda Bing tarjimonining samaradorligi yuqori. U har qanday bloklangan saytni ochish imkoniyatiga ega.

DNS (Domain Name System) – Domen nomi tizimi.

DNS nafaqat taqiqlangan veb-saytlarga kirish imkonini beradi, balki internet tezligini ham oshiradi. Odatda, OpenDNS eng yaxshi DNS serverlardan. Shuningdek, GoogleDNSdan ham foydalanishi mumkin.

DNS shlyuz Internet-provayderning DNS-serverlarini chetlab o‘tib, OpenDNS orqali Internetga kirish imkonini beradi.

Ushbu manzillar bloklangan saytlar ro‘yxatiga kiritilishi mumkin. Shuning uchun, https://use.opendns.com/ kabi saytlar orqali ixtiyoriy biridan foydalanish mumkin.

Internet arxividan foydalanish.

Bu usul qidiruv tizimi tomonidan sahifalarni keshlashiga o‘xshaydi, lekin qidiruv tizimlaridan farqli o‘laroq, Wayback Machine (Internet arxivi sayti) sahifalarni bir oy yoki bir necha yil oldingi holatidagidek saqlaydi. Misol sifatida, archive.org saytini keltirish mumkin. Unda nafaqat veb saytlar, balki, video, ovoz, TV, rasm va boshqa shu kabi ma’lumotlar arxivini kuzatish mumkin.

Wayback Machine statik turdagi sahifalarni ko‘rish uchun eng yaxshi vosita sanaladi. Umuman olganda, sayt qanchalik mashxo‘r bo‘lsa, ushbu saytning veb-arxivi shunchalik tez yangilanadi.

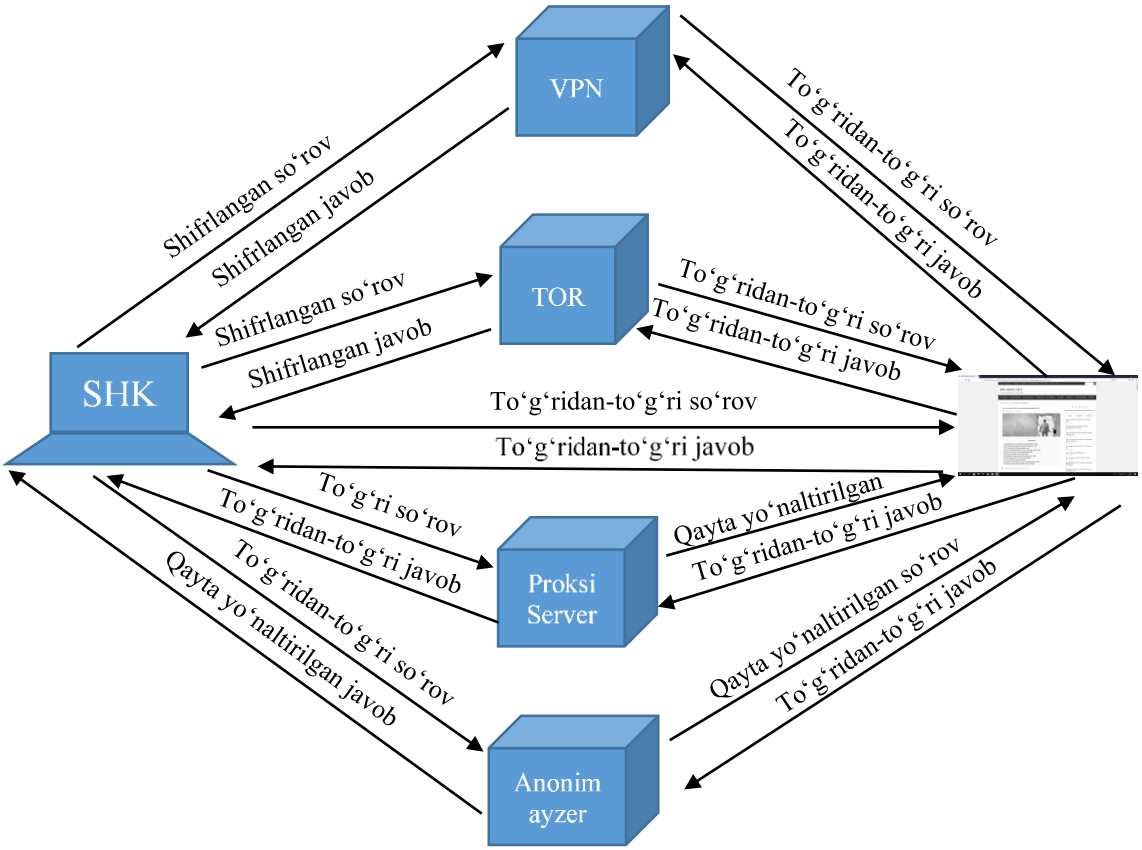
Quyidagi jadvalda VPN, Proksi server va Tor vositalarining tahlili keltirilgan bo‘lib, uning asosida maqsadga bog‘liq holda ulardan birini tanlash mumkin.

2-jadval. VPN, Proksi server va Tor vositalarining tahlili

	VPNnet	Oddiy VPN	Proksi server	Tor
Saytga anonim IP bilan kirish	+	+	+	+
Ixtiyoriy saytga tashrif	+	-	+	-
Ixtiyoriy sahifada ishlash	+	-	-	-
Provayderlar aniqlay omasligi	+	-	-	-
Statik IP	+	-	+	-
Trafikni shifrlash	+	+	-	+
Shifrlanganda tezlik	+	-	-	-
Sozlashda qo‘shimcha dastur talab etmaydi	+	-	+	-
Cheklanmagan qurilmalar soni	+	-	-	-
Qurilmalarning qo‘shimcha yuklanish olmasligi	+	-	+	+
Tekin	-	-	+	+
Log fayllar va boshqa izlar mavjud emas	-	-	+	+

VPNnet pullik ko‘rinishda xizmat ko‘rsatishga mo‘ljallangan xizmat hisoblansada, u boshqa vositalarda mavjud bo‘lmagan xususiyatlarni ham o‘zida mujassam etganligi bilan farqlanadi.

Quyidagi rasmda VPN, Tor, Proksi server va Anonimayzerlarning o‘zaro tahliliy sxemasi keltirilgan bo‘lib, foydalanuvchi kompyuteri va bloklangan saytlarga kirishga imkon beruvchi vosita hamda vosita va sayt o‘rtasidagi aloqalar keltirilgan.



5-rasm. VPN, Tor, Proksi server va Anonimayzerlarning o‘zaro tahlil sxemasi

Ushbu rasmdan ko‘rinib turibdiki, bloklangan saytlarga kirishga imkon beruvchi barcha dasturlarning imkoniyatlari turli bo‘lib, maqsadga bog‘liq holda foydalaniladi.

VPN internet-trafikni shifrlaydi, odatda uni faqat bitta server orqali yo‘naltiradi. Shuning uchun tezligi Tordan yuqori. Ulanish anonim emas, lekin VPN provayderi foydalanuvchi jurnallarini saqlamasa va ularni maxsus xizmatlarga o‘tkazmasa, tarmoqdagi harakatlar maxfiy hisoblanadi.

Proksi server va foydalanuvchi o‘rtasida to‘g‘ridan-to‘g‘ri aloqa hosil qiladi, ammo Proksi server va sayt o‘rtasida qayta yo‘naltirilgan (o‘zgartirilgan) manzil orqali bog‘lanadi.

Anonimayzer ulanishida esa, anonimayzer va foydalanuvchi o‘rtasida javob hamda anonimayzer va sayt o‘rtasida so‘rov qayta yo‘naltirilgan (o‘zgartirilgan) manzil orqali bog‘lanadi.

XULOSA

Keltirilgan usul va vositalar ichidan VPN va Torning imkoniyatlari keng. Ularning ishlash funksiyasi bir-biriga yaqin, agar ularni birgalikda qo‘llansa quyidagicha natija beradi. Ushbu holatda ikki xil ulanish yuzaga kelishi mumkin:

Foydalanuvchi→VPN→Tor→Internet (Torni VPN orqali qo‘llash).

Ushbu to‘plamdan foydalanish uchun tanlangan VPN serveriga ulanib Tor brauzeri ishga tushiriladi. Shifrlangan VPN trafigi Tor tarmog‘iga yo‘naltiriladi va u yakuniy manzilga yetguncha Tor tugunlari bo‘ylab o‘tadi. End-to-end VPN shifrlash va Tor anonimligi xavfsiz aloqa uchun yaxshi juftlik.

Afzalliklari:

– Sozlash oson.

– Yuqori tezlik va barqaror ishlashini ta’minlaydi.

– VPN provayderi kontent yoki trafik manbasini ko‘ra olmaydi, faqat Torga ulanish faktini ko‘radi.

– Internet provayderi Tordan foydalanilayotganini ko‘rmaydi, faqat VPN dan foydalanayotganini ko‘radi.

– Tor kirish tuguni haqiqiy IP manzilni emas, VPN IP manzilini ko‘radi.

Kamchiliklari:

– VPN provayderi hali ham haqiqiy IP manzilni ko‘rishi va bu ma’lumotni razvedka idoralariga taqdim etishi mumkin.

– Agar shifrlanmagan trafik yuborilsa, zararli Tor chiqish tugunlariga qarshi himoyasiz bo‘ladi.

– Agar VPN to‘satdan o‘chib qolsa, provayder tarmoqdagi harakatlar haqida bilib oladi.

Foydalanuvchi→Tor→VPN→Internet (VPNni Tor orqali qo‘llash).

Ushbu zanjirdan foydalanish uchun avval Torga ulanib, keyin VPN ishga tushiriladi. Tor tugunlariga ulanilgandan so‘ng trafik shifrlanadi.

Afzalliklari:

– VPN provayderi haqiqiy IP manzilni ko‘ra olmaydi.

– Internet provayderi VPNdan foydalanilayotganlikni ko‘ra olmaydi.

– Anonim xaridlar uchun ulanish qulay.

Kamchiliklari:

– Tezligi juda past.

– Faqat Tor saytlariga kirish mumkin.

– Barcha VPN provayderlari bu to‘plamdan foydalanishga ruxsat bermaydi.

Yuqoridagi mulohazalardan kelib chiqib, anonimlik uchun Tor brauzeri va maxfiylik uchun VPNdan foydalanish maqul degan xulosaga kelish mumkin. Chunki, Tor VPNga qaraganda yuqori anonimlikni ta’minlaydi. Ma’lumotlar tasodifiy tugunlar zanjiri orqali o‘tadi. Ulanish anonim, lekin provayder Tordan foydalanayotganlikni ko‘rishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Ijtimoiy tarmoqlar faoliyatiga chek qo‘yildi. Maqola. https://kun.uz/uz/news/2021/07/07/.

2. Xitoyda xorijiy xizmatlar bloklandi. Maqola. https://vc.ru/future/37403-za-stenoy-kak-kitayskiy-internet-razvivaetsya-posle-blokirovok-inostrannyh-servisov.

3. Muxtarov F.M. “Xavfsizlikni ta’minlash tizimi modellari va davlatlararo munosabatlar strategiyasini muvofiqlashtirish algoritmlari” falsafa doktori (PhD) dissertatsiyasi.

4. Bloklangan saytlarga aylanib o‘tish. Maqola. https://lib.jspi.uz.

5. Jahproxy proksi serveri. Maqola. https://jahproxy.pro/.

6. Bibhu Dash, Meraj Farheen Ansari, Pawankumar Sharma, Nikhitha Yathiraju. “Artificial Intelligence and Cybersecurity” 2021. Brussels.

7. Технологии информационного воздействия в социальных системах. Статья. www.evartist.narod.ru/text24/0028.