TARMOQ PROTOKOLLARIGA QILINADIGAN HUJUM TURLARI VA ULARNING XAVFSIZLIGINI TA’MINLOVCHI PROTOKOLLAR

Sultonmuratova Mashhura Quvonchbek qizi
TATU Urganch filiali talabasi
E-mail: sultonmuratovamashhura@gmail.com

Annotatsiya. Bu maqolada tarmoq protokollariga qilinadigan hujum turlari va ularning xavfsizligini ta’minlovchi protokollar va ularning qo‘llanilishi, ularning muhimligini va amaliyotga tatbiq etilishi mumkin bo‘lgan foydalarini o‘rganish mumkin. Tarmoq xavfsizligi sohasidagi asosiy standartlarni va tavsiyalarni identifikatsiya qilish, standartlarning amaliyotga tatbiq etish haqida ma’lumotlar berilgan.

Аннотация. В этой статье рассматриваются типы атак на сетевые протоколы и протоколы, которые их защищают, а также их использование, их важность и практические преимущества. Дана информация об определении основных стандартов и рекомендаций в области сетевой безопасности, а также о внедрении стандартов.

Annotation. This article explores the types of attacks on network protocols and the protocols that secure them and their uses, their importance, and their practical benefits. Information is given on the identification of the main standards and recommendations in the field of network security, and the implementation of the standards.

Kalit so‘zlar: kriptografik hujumlar, protokol, DarkNET, IP-adres, kommutatsiya texnologiyasi.

Ключевые слова: криптографические атаки, протокол, DarkNET, IP-адрес, технология коммутации.

Key words: cryptographic attacks, protocol, DarkNET, IP address, switching technology.

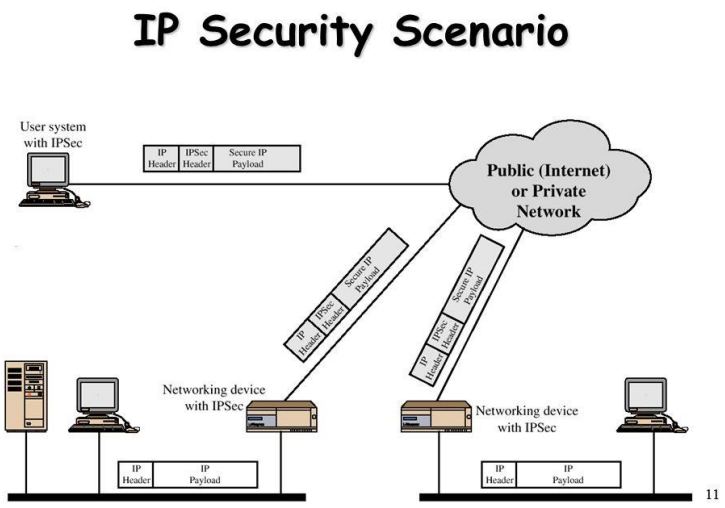
Kirish. Kriptografik hujumlar protokollarda ishlatiladigan kriptografik algoritmlarga, algoritm va protokollarni tadqiq qilishda ishlatiladigan kriptografik usullarga yoki protokollarning o‘ziga yo‘naltirilgan bo‘ladi.

Protokollarga qaratilgan hujumlarda odamlar ko‘pgina usullarni qo‘llashi mumkin, ba’zi jinoyatkorlar protokolda ishtirok etmay turib protokolni to‘liq yoki qisman “eshitishi” mumkin. Bu usul **passiv hujum** deb ataladi, chunki buzg‘unchi protokolga hech qanday ta’sir ko‘rsatmaydi, u faqat protokolni kuzatishi va axborot olishga urinishi mumkin. Bu turdagi hujumlar faqat shifrmatn asosidagi hujumlarga mos keladi, chunki passiv ochilishlarni aniqlash qiyin, protokollar ularni aniqlashga emas, balki qaytarishga urinishadi. Bizning protokollarda “Eshituvchi” rolini E bajaradi. Shu maqsadda u o‘zini boshqa odam sifatida ko‘rsatishi, protokolga yangi axborotlar kiritishi, bir axborotni boshqa axborotga almashtirishi, qaytadan eski axborotlarni jo‘natishi, aloqa liniyasini uzishi yoki kompyuterda saqlanadigan axborotni modifikatsiya qilishi (o‘zgartirishi) mumkin. Bunday harakatlar **aktiv hujum** deb ataladi. Bunday hujumlarning shakli tarmoq standartiga bog‘liq.

Passiv buzg‘unchilar protokol ishtirokchilari haqidagi ma’lumotni olishga urinishadi. Ular turli tomonlardan yuborilgan xabarlarni yig‘adilar va kriptotahlil qilishga urinadilar. Aktiv ta’sir qiluvchilarning urinishlari kengroq maqsadni ko‘zlaydi. Buzg‘unchi axborot olishdan, tizim tezligining pasayishidan yoki resurslardan ruxsatsiz foydalana olishdan manfaatdor bo‘lishi mumkin.

Aktiv hujumlar passivlarga nisbatan ancha xavfli. Ayniqsa bu tomonlar bir-biriga ishonishi shart bo‘lmagan protokollarga tegishli. Buzg‘unchi sifatida har doim ham mutlaqo begona odam ishtirok etmaydi. U tizimning registrasiya qilingan ishtirokchisi yoki tizim administratori yoki kelishgan holda ishlovchi jinoyatkorlar guruhi bo‘lishi mumkin. Buzg‘unchi sifatida protokol ishtirokchilaridan biri bo‘lishi mumkin. Protokolni bajarib u hamkasblarini aldashi yoki umuman protokolga rioya etmasligi mumkin. Bunday buzg‘unchi firibgar deb aytiladi. Passiv firibgarlar protokolni bajaradilar, ammo, protokolda mo‘ljallangan axborotdan tashqari yana ko‘proq axborot olishga urinishadi. Aktiv firibgarlar protokolning normal bajarilishini buzadilar. Agar protokol ishtirokchilarining ko‘pi aktiv firibgarlar bo‘lsa, u holda protokolning ishonchliligini ushlab turish qiyin, ba’zan qonuniy ishtirokchilar aktiv firibgarlarni aniqlashi mumkin va shu sababli protokollarni passiv firibgarlardan ham himoyalash kerak.

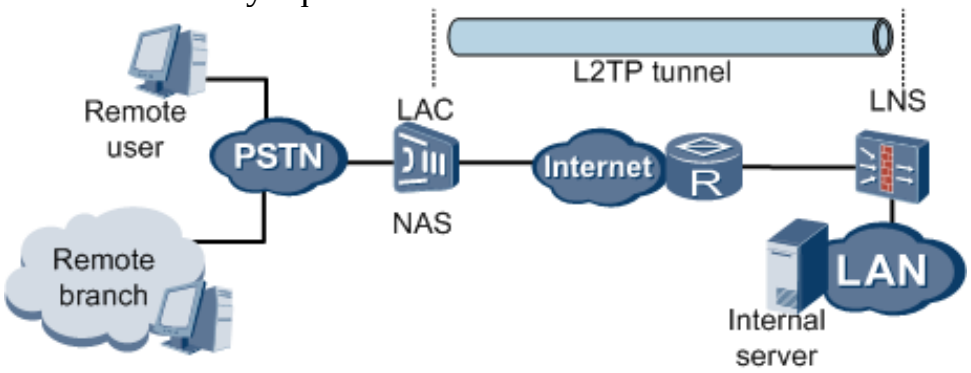
IPSec (IP Security) - bu Internet Protocol (IP) orqali uzatiladigan ma’lumotlarning himoyasini ta’minlash uchun protokollar to‘plami. Autentifikatsiya (autentifikatsiya), IP-paketlarning yaxlitligini tekshirish va shifrlash imkonini beradi. IPsec shuningdek, Internet orqali xavfsiz kalit almashinuvi uchun protokollarni ham o‘z ichiga oladi. U asosan VPN ulanishlarini tashkil qilish uchun ishlatiladi. IPSec (IP Security) protokoli ikkita rejimda – transport va tunnel rejimida ishlaydi. Transport rejimida (ushbu rejim hostlar orasidagi ulanishlarni o‘rnatishda ishlatiladi) IPSecdan qandaydir boshqa usul, xususan, shifrlash funksiyasi bo‘lmagan L2TP tomonidan tashkil etilgan “nuqta-nuqta” xilidagi tunnellarni himoyalashda foydalanish mumkin.



1-rasm. IP Security protokolining ishlash prinsipi

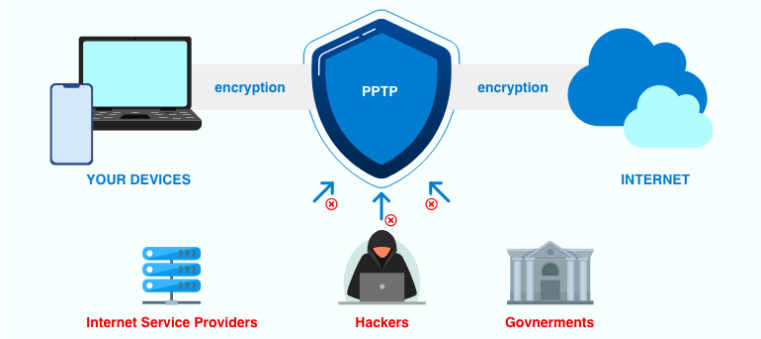
L2TP (Layer 2 Tunneling Protocol) - bu tarmoq protokoli, ma’lumotlarni

tarmoqning ikkinchi qatlamida (Layer 2) yuborish va qabul qilish uchun ishlatiladi. Uning asosiy maqsadi, eng yuqori darajadagi xavfsizlik va autentifikatsiya talablari bilan ma’lumotlarni boshqa tarmoqlar orasida "tunnel" yordamida yo‘lga qo‘yishdir. L2TP, IP protokoli ustida ishlaydigan tarmoq protokollari bilan birgalikda ishlatiladi va Virtual Private Network (VPN) tizimlarida keng tarqalgan. Ushbu protokol, bir tarmoqdan ikkinchisiga ma’lumotlarni o‘girish imkonini beradi, shuningdek, tarmoq tarkibidagi qurilmalar orasida eng muhimi, ma’lumotlarni shifrlash va tunnelni xavfsizlik bilan himoya qilishdir.



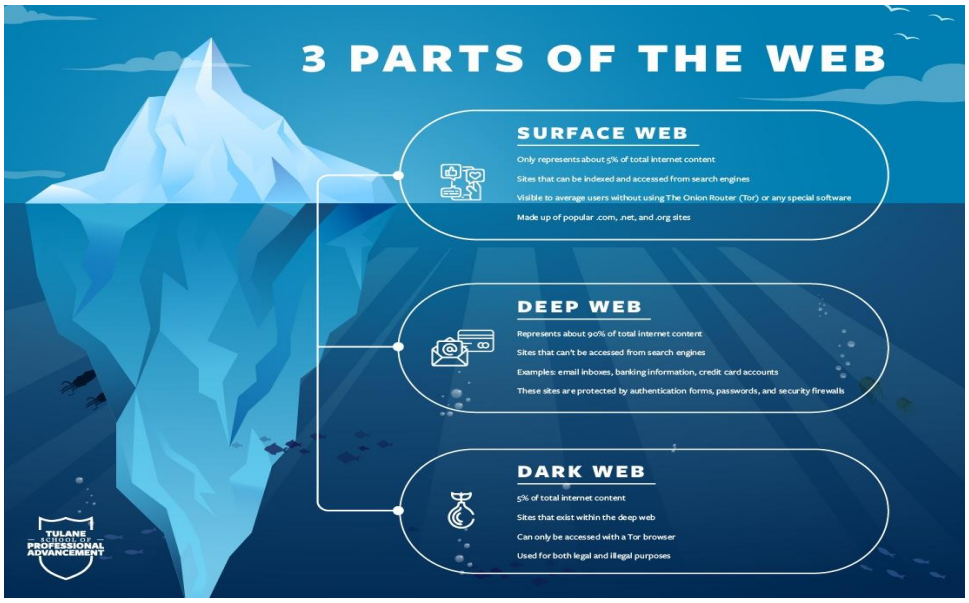
2-rasm. L2TP tarmoq protokolining ishlash prinsipi

PPTP (Point-to-Point Tunneling Protocol) – “nuqta-nuqta” turidagi kanal sathining tunnel protokoli. Ushbu protokol, tunnelga xizmat qilish uchun qo‘shimcha TCP - ulanish yordamida PPP - kadrlarni IP - paketlarga inkapsulyatsiyalaydi.



3-rasm. PPTP tarmoq protokolining ishlash prinsipi

“Bo‘sh” tarmoqlar (DarkNet) tuzoqlarning alohida sinfi hisoblanadi. Ularga muvofiq korporativ tarmoqda, biznes-masalalarni yechishda real ishlatilmaydigan, tashqi adreslar diapazoni ajratiladi. “Bo‘sh” tarmoqqa har qanday murojaat konfiguratsiyadagi xatolikni yoki noqonuniy faoliyatni anglatadi.

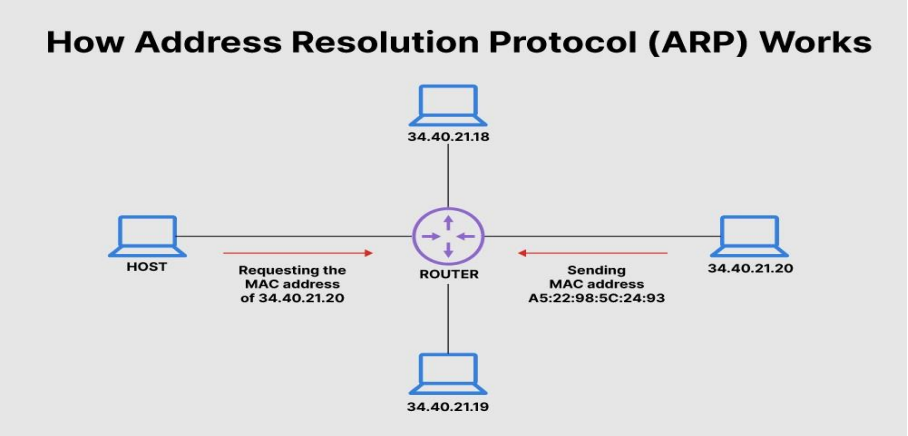


4-rasm. DarkNet tarmog’ining ifodalanishi

Ta’kidlash lozimki, IDS va DLP – yechimlar hujumlarning ma’lum sinfiga mo‘ljallangan. Amaliyotda axborot tizimi ishlashidagi har qanday xavfsizlik va ishonchlik hodisalarni yig‘ish masalasi paydo bo‘ladi. Bunday tizimlarga quyidagilar taaluqli:

- jurnallarni boshqarish tizimlari (log management). Ushbu tizimlar axborot xavfsizligi hodisalarini markazlashgan tarzda yig‘ishni tashkil etish uchun mo‘ljallangan;
- xavfsizlik xususidagi axborotni boshqarish tizimlari (Security Information Management, SIM). Ushbu tizimlar axborot xavfsizligi hodisalarini markazlashgan tarzda yig‘ishga, hamda turli hisobotlarni shakllantirishga va tahlillashga mo‘ljallangan;
- xavfsizlik hodisalari xususidagi axborotni boshqarish tizimlari(Security Event Manager, SEM). Ushbu tizimlar vaqtning real rejimida monitoringlashga, axborot xavfsizligi hodisalarini korrelyatsiyalashgamo‘ljallangan;
- xavfsizlik va xavfsizlik hodisalari xususidagi axborotni boshqarish tizimlari (Security Information and Event Management, SIEM). Ushbu tizimlar monitoring tizimlari rivojining keyingi qadami hisoblanadi, chunki SEM va SIM funksionalliklarini kombinatsiyalaydi.

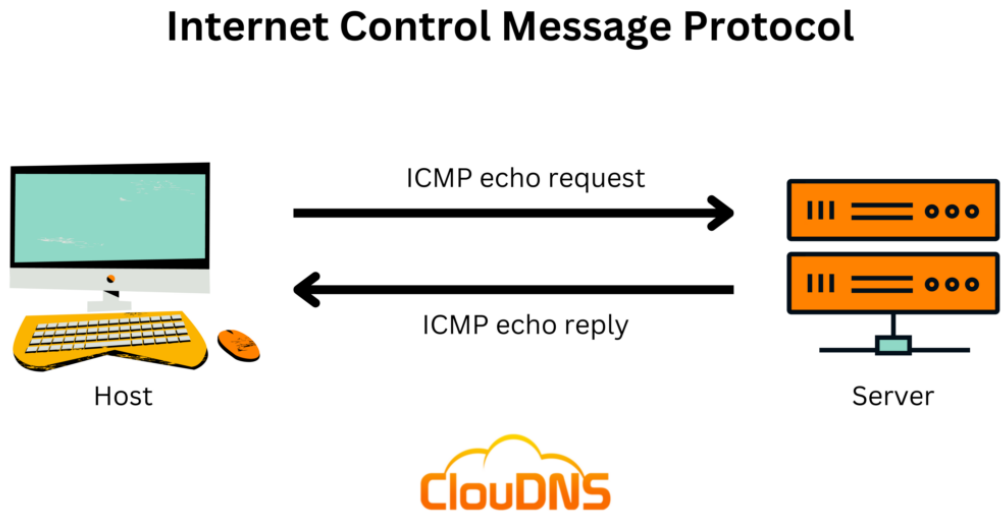
ARP (Adres Resolution Protocol) - ma’lum IP-manzil yordamida boshqa kompyuterning MAC manzilini aniqlash uchun mo‘ljallangan kompyuter tarmoqlaridagi protokol. Protokolning tavsifi 1982-yil noyabr oyida RFC 826 da nashr etilgan. ARP IP-paketlarni chekilgan paketlar (ramkalar) orqali tashish uchun mo‘ljallangan. ARP da qo‘llaniladigan maqsadli hostning apparat manzilini aniqlash prinsipi keyinchalik boshqa turdagi tarmoqlarda qo‘llanilgan.



5-rasm. ARP protokolining ishlash prinsipi

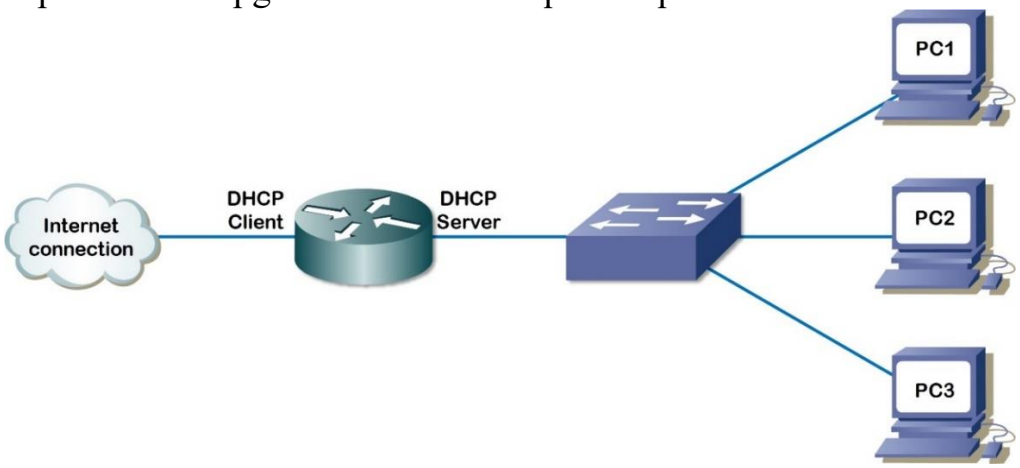
Tarmoq qatlami paketi Ethernet segmenti orqali yuborilishidan oldin, tarmoq stegi ARP keshini tekshiradi va kerakli maqsad xost ma’lumotlari uning jadvalida allaqachon ro‘yxatdan o‘tganligini tekshiradi. Agar ARP keshida bunday yozuv bo‘lmasa, u holda ARP translyatsiyasi so‘rovi amalga oshiriladi. Tarmoqdagi qurilmalar uchun ushbu so‘rov quyidagi ma’noga ega: "Falon IP-manzilga ega bo‘lgan qurilmaning jismoniy manzilini kimdir biladimi?" Ushbu IP-manzilga ega host bunday so‘rov paketini olganida, u javob berishi kerak: "Ha, bu mening IP-manzilim va mening apparat manzilim falonchi." So‘rovni jo‘natuvchi qabul qiluvchining apparat manzilini o‘zining ARP keshida saqlaydi va ma’lumotni qabul qiluvchiga yuborishi mumkin bo‘ladi. Yangi operatsion tizimlarda ARP jadvali yozuvlarini saqlash vaqti va saqlash usuli dasturiy jihatdan tanlanadi va agar kerak bo‘lsa o‘zgartirilishi mumkin.

ICMP (Internet Control Message Protocol**)** - TCP/IP protokoli stekining bir qismi bo‘lgan tarmoq protokolidir. ICMP, birinchi navbatda, so‘ralgan xizmat mavjud emas yoki host yoki yo‘riqnoma javob bermayotgani kabi ma’lumotlarni uzatish paytida yuzaga kelgan xatolar va boshqa istisno holatlar haqida xabar berish uchun ishlatiladi. ICMP ba’zi xizmat funksiyalarini ham bajaradi.



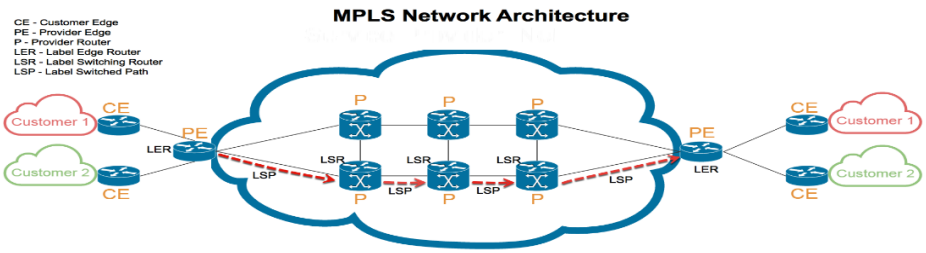
6-rasm. ICMP protokolining ishlash prinsipi

DHCP (Dynamic Host Configuration Protocol) - tarmoq protokoli bo‘lib, tarmoq qurilmalariga TCP/IP tarmog‘ida ishlash uchun zarur bo‘lgan IP-manzil va boshqa parametrlarni avtomatik ravishda olish imkonini beradi . Ushbu protokol mijoz-server modelida ishlaydi. Avtomatik konfiguratsiya qilish uchun mijoz kompyuteri tarmoq qurilmasini sozlash bosqichida DHCP serveri bilan bog‘lanadi va undan kerakli parametrlarni oladi. Tarmoq ma’muri server tomonidan kompyuterlar o‘rtasida taqsimlangan manzillar oralig‘ini belgilashi mumkin. Bu tarmoq kompyuterlarining qo‘lda konfiguratsiyasidan qochish imkonini beradi va xatolar sonini kamaytiradi. DHCP protokoli ko‘pgina TCP/IP tarmoqlarida qo‘llaniladi.



7-rasm. DHCP protokolining ishlash prinsipi

MPLS (multiprotocol label switching) – ko‘p protokolli belgilar kommutatsiya qilish texnologiyasi – integrallashgan xizmatlarni taklif qilish uchun IETF tomonidan yaratilgan. Ushbu yangi texnologiyada qurilgan magistral tarmoqlarda trafiklarni qayta ishlash tezligi va ko‘p karrali xizmatlarni taqdim etish imkoniyati kengayadi.



8-rasm. MPLS protokolining arxitekturasi

MPLS texnologiyasi o‘ziga ATM ning ishonchliligi, qulayligi va yuqori tezlikda ma’lumotlarni jo‘natish imkoniyatini IP tarmoqlarda birlashtira oldi. Bu texnologiyaning asosiy afzalligi – paketlarni kommutatsiyalash jarayonining IP adres sarlavhasi tahlilidan alohida bo‘limlarda amalga oshirilishidir. Bu holat paketlarni kommutatsiyalashga talab qilinadigan vaqtni sezilarli ravishda qisqartiradi. Mos ravishda, MPLS protokolida ishlovchi marshrutizatorlar va kommutatorlar har bir tarmoqqa kirish nuqtasida marshrutizatsiyalash jadvaliga maxsus belgi kiritadi va bu haqida qo‘shni qurilmalarga xabar beradi.

Xulosa qilib shuni aytish joizki, mazkur maqolada tarmoq protokollariga

qilinadigan hujum turlari va ularning xavfsizligini ta’minlovchi protokollar haqida so‘z yuritildi. Ushbu ishning e’tiborli jihati shundaki, o‘quvchilar bilimlarini yanada mustahkamlashga, ularni protokollarda ishlatiladigan kriptografik algoritmlarga, algoritm va protokollarni tadqiq qilishda ishlatiladigan kriptografik usullarga yoki protokollarning o‘ziga yo‘naltirilishi haqida nazariy ko‘nikmalarga ega bo‘la olishadi.

FOYDALANILGAN ADABIYOTLAR

1. “5523500 – Axborot xavfsizligi ta’lim yo’nalishi bo’yicha bakalavrlarning tayyorgarlik darajasi va zaruriy bilimlar mazmuniga qo’yiladigan TALABLAR” O’zbekiston davlat ta’lim standarti. Toshkent, 2008.
2. Bryus Shnayer. Prikladnaya kriptografiY. Protokoli, algoritmi, isxodniye teksti na yazike SI – Moskva: TRIUMF, 2002.
3. Galatenko V.A. Informatsionnaya bezopasnost. –M.: Finansы i statistika, 1997. –158 s.
4. Gregori S. Smit. Programmы shifrovaniya dannых // Mir PK –1997. -№3. - S.58 - 68.
5. Shnayer Bryus. Prikladnaya kriptografiya. Protokolы, algoritmы, isxodnые tekstы na yazыke Si. Triumf. 2002.

Internet resurslari

6. http://www.google.com
7. http://www.it-ebooks.info
8. www.poe.com