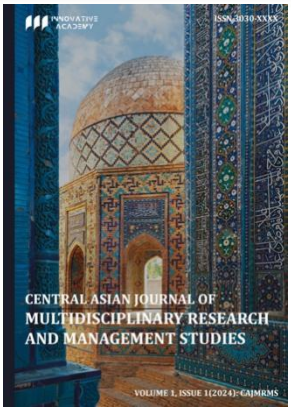

AXBOROTLANI TARMOQDA UZATISHDA HIMOYALASH USULLARI

Saidov Jasur Doniyor o‘g‘li

Guliston Davlat universiteti

Asrorova Mavludaoy Umurzoq qizi

Guliston Davlat universiteti Amaliy matematika yo’nalishining 1-kurs talabasi

https://doi.org/10.5281/zenodo.15430054

ARTICLE INFO

Received: 5 th May 2025
Accepted: 10th May 2025
Published: 16th May 2025

KEYWORDS

tarmoq serverlari, LAN obyektlari, tarmoq protokollari, neyron tarmoqlar, kriptografiya, kriptotahlil, stenografik himoya, stenografiya, statistic usul, ekspert tizimlari, simmetrik shifrlash, parollar, autentifikatsiya.

ABSTRACT

Ushbu maqola axborotlarni tarmoq orqali uzatishda himoyalashning turli usullarini ko'rib chiqadi. Axborot texnologiyalarining rivojlanishi bilan, tarmoqda uzatilayotgan ma'lumotlarning xavfsizligini ta'minlash zarurati ortmoqda. Maqolada, tarmoqda axborot uzatishda qo'llaniladigan asosiy himoya usullari — shifrlash, VPN (Virtual Private Network), autentifikatsiya, fayl tizimlari va tarmoqni himoyalash, tarmoq trafigini monitoring qilish, xavfsizlik protokollari va siyosatlarining ahamiyati yoritilgan. Shuningdek, tarmoq xavfsizligini ta'minlash uchun foydalanuvchilar va tashkilotlar uchun asosiy xavfsizlik choralariga e'tibor qaratilgan. Bu usullar, kiberhujumlar va ma'lumot yo'qotishining oldini olishda samarali bo'lib, axborot almashish jarayonini xavfsiz va ishonchli qiladi.

Hozirgi davrda tashkilotlar samarali va produktiv muloqot qilish uchun asosan kompyuter tarmoqlariga suyanadilar. Har bir xodimning maxsus ish stantsiyasi bor deb taxmin qilsak, yirik kompaniyalarda ularning soni bir necha mingga yetishi mumkin, shuningdek, tarmoqda ko’plab serverlar ham mavjud bo’lishi mumkin.

Ehtimol, ushbu ish stantsiyalarini markazdan boshqarish mumkin emas va ularning atrof-muhiti xavfsizligi ta’minlanmagan. Foydalanuvchilar orasida turli xil sir tutilishi darajalariga ega bo’lgan xabarlarni, turli xil operatsion tizimlarga, qo’shimcha qurilmalarga, dasturlarga va protokollarga ega bo’lishi mumkin bo’lgan o’rtalikda almashish holatlari juda ko’p. Endi tasavvur qiling, kompaniya tarmog’idagi ushbu minglab ish stantsiyalari to’g’ridan - to’g’ri Internetga ulangan. Ko’plab zaifliklarga ega qimmatbaho ma’lumotlarni o’z ichiga olgan ushbu xavfli tarmoq bir nechta xakerlar hujumi uchun oson nishonga aylanadi.

Tarmoq, muxofazasini tashkil etishda quyidagilarni e‘tiborga olish lozim: - muxofaza tizimining nazorati; - fayllarga kirishning nazorati; - tarmoqda ma‘lumot uzatishning nazorati; - axborot zaxiralariga kirishning nazorati; - tarmoq bilan ulangan boshqa tarmoqlarga ma‘lumot tarqalishining nazorati. Tarmoq himoyasini tashkil qilish asoslari. Maxfiy axborotni qayta ishlash uchun kerakli tekshiruvdan o’tgan kompyuterlarni ishlatish lozim bo’ladi. Muxofaza vositalarining funksional to’lik bo’lishi muxim hisoblanadi. Bunda tizim

administratorining ishi va olib borayotgan nazorati katta ahamiyatta egadir. Masalan, foydalanuvchilarning tez-tez parollarni almashtirib turishlari va parollarning juda uzunligi ularni aniqlashni qiyinlashtiradi. Shuning uchun ham yangi foydalanuvchini qayd etishni cheklash (masalan, faqat ish vaqtida yoki faqat ishlayotgan korxonasida) muximdir. Foydalanuvchining xaqiqiyligini tekshirish uchun teskari aloqa qilib turish lozim (masalan, modem yordamida). Axborot zaxiralariga kirish huquqini chegaralash mexanizmini ishlatish va uning ta‘sirini LAN obyektlariga to’laligicha o’tkazish mumkin. Tarmoq, elementlari urtasida o’tkazilayotgan ma‘lumotlarni muxofaza etish uchun quyidagi choralarni ko’rish kerak: - ma‘lumotlarni aniqlab olishga yo’l qo’ymaslik; - axborot almashishni tahlil qilishga yo’l qo’ymaslik; - xabarlarni o’zgartirishga yo’l qo’ymaslik; - yashirincha ulanishga yo’l qo’ymaslik va bu xollarni tezda aniqlash. Ma‘lumotlarni tarmoqda uzatish paytida kriptografik himoyalash usullaridan foydalaniladi, qayd etish jurnaliga ruxsat etilmagan kirishlar amalga oshirilganligi xaqida ma‘lumotlar yozilib turilishi kerak. Bu jurnalga kirishni chegaralash ham himoya vositalari yordamida amalga oshirilishi lozim. Kompyuter tarmogida nazoratni olib borish murakkabligining asosiy sababi — dasturiy ta‘minot ustidan nazorat olib borishning murakkabligidir. Bundan tashqari kompyuter viruslarining ko’pligi ham tarmoqda nazoratni olib borishni qiyinlashtiradi. Hozirgi vaqtgacha muxofazalash dasturiy ta‘minoti xilma-xil bo’lsa ham, operatsion tizimlar zaruriy muxofazaning kerakli darajasini ta‘minlamas edi.

Himoyalanishni tahlillash vositalari zaifliklarni topib va o`z vaqtida yo`q qilib xujumni amalga oshirish imkoniyatini bartaraf qiladi. Natijada, himoyalash vositalarini ishlatilishiga bo`ladigan barcha sarf-harajatlar kamayadi. Himoyalanishni tahlillash vositalari tarmoq sathida, operattsion tizim sathida va ilovalar sathida ishlashi mumkin. Ular tekshirishlar sonini bora-bora ko`paytirish, axborot tizimiga "ichkarilab borish" va uning barcha sathlarini tadqiqlash orqali zaifliklarni qidirishi mumkin. Tarmoq protokollari va servislari himoyalanishini tahlillash vositalari. Har qanday tarmoqda abonentlarning o`zaro aloqasi ikkita va undan ko`p uzellar orasida axborot almashinish muolajalarini belgilovchi tarmoq protokollari va servislaridan foydalanishga asoslangan. Tarmoq protokollari va servislarini ishlab chiqishda ularga ishlanuvchi axborot xavfsizligini ta’minlash bo`yicha talablar qo`yilgan. SHu sababli, tarmoq protokollarida aniqlangan zaifliklar xususida axborotlar paydo bo`lmoqda. Natijada, korporativ tarmoqda foydalanadigan barcha protokol va servislarni doimo tekshirish zaruriyati tug’iladi. Himoyalanishni tahlillash tizimi zaifliklarni aniqlash bo`yicha testlar seriyasini bajaradi. Bu testlar niyati buzuq odamlarning korporativ tarmoqlarga xujumlarida qo`llaniladiganiga o`xshash. Zaifliklarni aniqlash maqsadida skanerlash tekshiruvchi tizim xususidagi dastlabki axborotni, xususan, ruxsat etilgan protokollar va ochiq portlar, operattsion tizimning ishlatiluvchi versiyalari va h. xususidagi axborotni olish bilan boshlanadi. Skanerlash keng tarqalgan xujumlar, masalan, to`liq saralash usuli bo`yicha parollarni tanlashdan foydalanib, suqilib kirishni imitatsiyalashga urinish bilan tugaydi. Himoyalanishni tahlillash vositalari yordamida tarmoq sathida nafaqat Internetning korporativ tarmoqdan ruxsatsiz foydalanishi imkoniyatini testlash, balki tashkilot ichki tarmog’ida tekshirishni amalga oshirish mumkin. Tarmoq sathida himoyalanishni tahlillash tizimi tashkilot xavfsizlik darajasini baholashga hamda tarmoq dasturiy va apparat ta’minotini sozlash samaradorligini nazoratlashga xizmat qiladi.

Tarmoq axborotini tahlillash usullari. Mohiyati bo`yicha, xujumlarni aniqlash jarayoni korporativ tarmoqda bo`layotgan shubhali harakatlarni baholash jarayonidir. Boshqacha aytganda xujumlarni aniqlash - hisoblash yoki tarmoq resurslariga yo`naltirilgan shubhali harakatlarni identifikattsiyalash va ularga reaktsiya ko`rsatish jarayoni. Hozirda xujumlarni aniqlash tizimida quyidagi usullar ishlatiladi: - statistik usul; - ekspert tizimlari; - neyron tarmoqlari. Statistik usul. Statistik yondashishning asosiy afzalligi allaqachon ishlab chiqilgan va o`zini tanitgan matematik statistika apparatini ishlatish va sub’ekt xarakteriga moslash. Avval tahlillanuvchi tizimning barcha sub’ektlari uchun profillar aniqlanadi. Ishlatiladigan

profillarning etalondan har qanday chetlanishi ruxsat etilmagan foydalanish hisoblanadi. Statistik usullar universal hisoblanadi, chunki mumkin bo`lgan xujumlarni va ular foydalanadigan zaifliklarni bilish talab etilmaydi. Ammo bu usullardan foydalanishda bir qancha muammolar paydo bo`ladi:

1. Statistik tizimlar xodisalar kelishi tartibiga sezuvchanmaslar; ba'zi xollarda bir xodisaning o`zi, kelishi tartibiga ko`ra anomal yoki normal faoliyatni xarakterlashi mumkin.
2. Anomal faoliyatni adekvat identifikattsiyalash maqsadida xujumlarni aniqlash tizimi tomonidan kuzatiluvchi xarakteristikalar uchun chegaraviy qiymatlarni berish juda qiyin.
3. Statistik usullar vaqt o`tishi bilan buzunchilar tomonidan shunday "o`rnatilishi" mumkinki, xujum harakatlari normal kabi qabul qilinadi. Ekspert tizimlari- odam-ekspert bilimlarini qamrab oluvchi qoidalar to`plamidan tashkil topgan. Ekspert tizimidan foydalanish xujumlarni aniqlashning keng tarqalgan usuli bo`lib, xujumlar xususidagi axborot qoidalar ko`rinishida ifodalanadi. Bu qoidalar harakatlar ketma-ketligi yoki signaturalar ko`rinishida yozilishi mumkin. Bu qoidalarning har birining bajarilishida ruxsatsiz faoliyat mavjudligi xususida qaror qabul qilinadi. Bunday yondashishning muhim afzalligi - yolg'on trevoganing umuman bo`lmasligi. Ekspert tizimining ma'lumotlari bazasida hozirda ma'lum bo`lgan aksariyat xujumlar stsenariyasi bo`lishi lozim. ekspert tizimlari, dol-zarblikni saqlash maqsadida, ma'lumotlar bazasini muttasil yangilashni talab etadi. Garchi ekspert tizimlari qaydlash jurnallaridagi ma'lumotlarni ko`zdan kechirishga yaxshi imkoniyatni tavsiya qilsada, so`ralgan yangilanish e'tiborsiz qoldirilishi yoki ma'mur tomonidan qo`lda amalga oshirilishi mumkin. Bu eng kamida, ekspert tizimi imkoniyatlarining bo`shashiga olib keladi.

Ekspert tizimlarining kamchiliklari ichida eng asosiysi - noma'lum xujumlarni akslantira olmasligi. Bunda oldindan ma'lum xujumning xatto ozgina o`zgarishi xujumlarni aniqlash tizimining ishlashiga jiddiy to`siq bo`lishi mumkin. Neyron tarmoqlari. Xujumlarni aniqlash usullarining aksariyati qoidalar yoki statistik yondashish asosida nazoratlanuvchi muhitni tahlillash shakllaridan foydalanadi. Nazoratlanuvchi muhit sifatida qaydlash jurnallari yoki tarmoq trafigi ko`rilishi mumkin. Bunday tahlillash ma'mur yoki xujumlarni yaniqlash tizimi tomonidan yaratilgan, oldindan aniqlangan qoidalar to`plamiga tayanadi. Xujumni vaqt bo`yicha yoki bir necha niyati buzuq odamlar o`rtasida har qanday bo`linishi ekspert tizimlar yordamida aniqlashga qiyinchilik tudiradi. Xujumlar va ular usullarining turli-tumanligi tufayli, ekspert tizimlari qoidalarining ma'lumotlar bazasining hatto doimiy yangilanishi ham xujumlar diapazonini aniq identifikattsiyalashni kafolatlamaydi.

Eng keng tarqalgan usul — foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Bunda fayllarga o`qish va yozishdan himoyalash atributlari o`rnatiladi (masalan, operattsion tizimdan foydalanishni nazoratlash ruyxatidagi mos imtiyozlarni tavsiflash yordamida). Tizim foydalanuvchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funktsiyalar kabi kriptografik mexanizmlar ishlatilmaydi. Ushbu usulning kamchiligi - niyati buzuq odamning tizimda ma'mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir. Oddiy autentifikatsiyani tashkil etish sxemalari nafaqat parollarni uzatish, balki ularni saqlash va tekshirish turlari bilan ajralib turadi. eng keng tarqalgan usul — foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir

Xavfsizlik nuqtai nazaridan parollarni bir tomonlama funktsiyalardan foydalanib uzatish va saqlash qulay hisoblanadi. Bu holda foydalanuvchi parolning ochiq shakli urniga uning bir tomonlama funktsiya h(.) dan foydalanib olingan tasvirini yuborishi shart. Bu o`zgartirish anim tomonidan parolni uning tasviri orqali oshkor qila olmaganligini kafolatlaydi, chunki anim echilmaydigan sonli masalaga duch keladi.

Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning ikkinchi usuli foydalanuvchi va tekshiruvchi uchun umumiy bo`lgan tasodifiy parollar ruyxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanishga asoslangan. Bir martali parollarning bo`linuvchi ro`yxati maxfiy parollar ketmaketligi yoki to`plami bo`lib, har bir

parol faqat bir marta ishlatiladi. Ushbu ro`yxat autentifikattsion almashinuv taraflar o`rtasida oldindan taqsimlanishi shart. Ushbu usulning bir variantiga binoan so`rov-javob jadvali ishlatiladi. Bu jadvalda autentifikattsilash uchun taraflar tomonidan ishlatiluvchi so`rovlar va javoblar mavjud bo`lib, har bir juft faqat bir marta ishlatilishi shart.

Tarmoq steganografiyasi katta hajmdagi ma'lumotlarni real vaqtda yashirib uzatish imkonini beradi. Ya'ni, steganografik usulga teskari usulni qo'llash bilan ochiq kontent tarkibiga yashirib uzatilgan xabarni ajratib olish mumkin bo'ladi. Yuqorida keltirilgan steganografiya va kriptografiyani birlashtirishga asoslangan
usullarning aksariyatida ma'lumotlarni shifrlash uchun simmetrik algoritmlar taklif qilingan. Ma'lumki, simmetrik shifrlash algoritmlarida kalitni qabul qiluvchiga xavfsiz yetkazib berish muammosi mavjud. Ushbu muammoni yechish uchun asimmetrik algoritmlardan foydalanish maqsadga muvofiq.

Ma'lumki, kriptografiyada ruxsatsiz o'qishdan himoyalash maxfiy xabarlar ma'nosini o'zgartirish orqali amalga oshiriladi. Shuningdek, kriptografiya ma'lumotlarning yaxlitligi, obyektning va ma'lumotlarning haqiqiyligi tekshirish kabi axborot xavfsizligi bilan bog'liq masalalarni yechadi. Biroq, shifrlab uzatilgan xabarlar o'rtada turib tinglovchi shaxslar uchun muhim bo'lganligi uchun ularni kalitsiz ochishga qaratilgan kriptotahlil usullari ham rivojlangan. Kriptotahlil usullari yordamida shifrlangan xabarlarni kalitsiz ochish imkoniyati mavjud. Shuning uchun shifrlangan xabarlarni steganografik usullaryordamida yashirib uzatish uning xavfsiz yetib boorish imkoniyatini oshiradi. Ushbu muammoni bartaraf etish uchun biz taklif qilgan usul, kriptografiyaning simmetrik shifrlash algoritmlari asosan ma'lumotlarni shifrlashda, asimmetrik algoritmlar esa kalitlarni almashtirishda qo'llaniladi. Shuning uchun kriptobardoshliligi yuqori simmetrik AES va asimmetrik RSA shifrlash algoritmlarini qo'llash tarmoqda uzatilayotgan axborotning xavfsizligini oshiradi.

Tarmoq steganografiyasi usullaridan foyda-lanib uzatilayotgan paketlarni tutib, uning tarkibidan yashirilgan xabarni topish imkoniyati mavjud. Shuning uchun, taklif qilingan real vaqtda ma'lumotni yashirish algoritmi tarkibida kripto-
grafik shifrlash usulidan foydalanish maqsadga muvofiq. Ushbu masala hal qilish uchun kripto-steganografiya usulidan foydalanib ikkalasini birga qo'llash usuli ishlatilsa maqsadga muvofiq bo'ladi.

Steganografik himoyadaga mavjud kamchilik-larni bartaraf etishda kriptografik himoya mexanizmlaridan foydalanish mumkinligini inobatga olgan holda kriptografik-staganografik himoyalash usuli taklif etilib, ushbu usul asosida ishlab chiqilgan himoya mexanizmi to'laqonli himoyani ta'minlashi isbotlandi. Ushbu usullarni birlashtirish yaxshilangan axborot xavfsizligini ta'minlaydi va muhim ma'lumotlarni ochiq kanallar orqali uzatish xavfsiz uzatish imkoniyatini berdi. Ma'lumotni uzatishda foydalanilgan kontent hajmi va yashirish sig'imi parametrlari orqali steganografik algoritmlarning yashirish samaradorligi hisoblab chiqildi. Ishlab chiqilgan usul turli stegonografik usullar uchun axborotni yashirish samaradorligini aniqlash imkonini yana ham oshirib berdi.

Foydalanilgan adabiyotlar ro'yxati:

1. Ganivev, Abduhalil, Obid Mavlonov, and Baxtiyor Turdibekov. "Improving data hiding methods in network steganography based on packet header manipulation." 2021 International Conference on Information Science and Communications Technologies (ICISCT). IEEE, 2021.

2. Mavlonov O. Advancements in retransmission steganography: an enhanced algorithm and its steganalysis approaches //International Scientific and Current Research Conferences. – 2023. – C. 127-131.

3. Karthikeyan B, Kosaraju A C and Gupta S 2016 March Enhanced security in steganography using encryption and quick response code In Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on (pp. 2308-2312) IEEE.

4. Pillai B, Mounika M, Rao P J and Sriram P 2016 September Image steganography method using K-means clustering and encryption techniques In Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on (pp. 1206-1211) IEEE.
5. **Islomov I.M.** – *Axborot xavfsizligi asoslari* – Toshkent: TDPU, 2010.
– Axborot xavfsizligi, tarmoq himoyasi va foydalanuvchi autentifikatsiyasi haqida keng yoritilgan.
6. **Kurbanov A.X., Tursunov B.A.** – *Kompyuter tarmoqlari va ularning xavfsizligi* – Toshkent, 2012.
– Tarmoqlardagi zaifliklar va himoyalash usullari haqida ma'lumot beradi.
7.**Stallings W.** – *Cryptography and Network Security* – Prentice Hall, turli nashrlari (2005, 2011, 2017).
– Kriptografik usullar, xavfsizlik protokollari, tarmoq xavfsizligi asoslari.
8. **Tanenbaum A.S., Wetherall D.J.** – *Computer Networks* – 5th Edition, Pearson, 2011. – Kompyuter tarmoqlari arxitekturasi va xavfsizlik haqida chuqur bilim beradi.
9. **RFC hujjatlari (Request for Comments)** – Internet arxitekturasi, xavfsizlik protokollari (masalan, IPsec, SSL/TLS, HTTPS) haqida texnik tavsiflar.
10. Saidov, J. D. *Study of the process of database and creation in higher education. Guliston. 2021*.
11. Saidov, J. D. O. G. L., Allayorov, S. P., & Islikov, S. X. (2021). MA'LUMOTLAR OMBORINI YARATISH BO 'YICHA KASBIY KOMPETENTLIGINI BAHOLASH MEZONLARI. *Scientific progress*, *2*(1), 1804-1807.
12. Islikov, S., Saidov, J., & Xolmuminov, D. (2023). MUSTAQIL TA'LIMNI SHARQ MUTAFAKKIRLARINING QARASHLARI ASOSIDA TASHKIL QILISH. *Евразийский журнал технологий и инноваций*, *1*(5), 172-174.
13. Saidov, J. D., Qudratov, A. N., Islikov, S. X., Normatova, M. N., & Monasipova, R. F. (2023). Problems of Competency Approach in Developing Students' Creativity Qualities for.
14 Eshbaevich, T. D. Gulistan State University, 120100, 4th microdistrict, Gulistan city, Syrdarya region, Uzbekistan E-mail: doniyor120373@ gmail. com Abstract. The article describes the creation of modern e-learning resources for educational process, their purpose, content, structure and stages of creation. The article also gives recommendations on how to create e-learning resources, and. *Pedagogika*, *21*.
15. Тоштемиров, Д. Э. (2010). Таълим порталининг таркибий тузилиши ва услубий таъминоти. *Касб-ҳунар таълими*, *2*, 10-11.
16. Anarbaev, A., Tursunov, O., Kodirov, D., Khudaev, I., Isakhodjayev, K., & Islikov, S. (2021). Pre-sowing activation of seeds by ultraviolet (UV) radiation. In *E3S Web of Conferences* (Vol. 304, p. 03040). EDP Sciences.
17. Kalandarov, A. A., Kulmamatov, S., Islikov, S., Adilov, A., Kalandarov, A., & Allayarov, S. (2020). Numerical modeling of partially coupled problems of thermoelasticity. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(3), 3095-3099.