TARMOQ DASTURIY TA’MINOTINI XAVFSIZLIK PROTOKOLLARI ASOSIDA LOYIHALASH VA HIMOYALASH MEXANIZMLARINI ISHLAB CHIQISH

Kamilov Javohir Odil o'g'li
University of management and future
Technologies universiteti 2-bosqich magistranti

Annotatsiya: *Ushbu tezisda tarmoq dasturiy ta’minotini loyihalash jarayonida xavfsizlik protokollarining roli, ularning samarali qo‘llanilishi va himoya mexanizmlarini ishlab chiqish usullari tahlil qilinadi. Tarmoqdagi kiberxavfsizlik tahdidlariga qarshi samarali strategiyalar ishlab chiqish uchun kriptografik protokollar, autentifikatsiya va avtorizatsiya mexanizmlari, shuningdek, ma’lumotlarni shifrlash metodlari o‘rganiladi. Tezisda tarmoq dasturiy ta’minotini loyihalash jarayonidagi xavfsizlik protokollari qo‘llanilishi, ularning samaradorligini baholash va xavfsizlik darajasini oshirish bo‘yicha amaliy tavsiyalar keltiriladi.*

Kalit so‘zlar: *tarmoq dasturiy ta’minoti, xavfsizlik protokollari, kriptografiya, autentifikatsiya, avtorizatsiya, ma’lumotlarni shifrlash, kiberxavfsizlik.*

Аннотация: *В данной работе анализируется роль протоколов безопасности в процессе проектирования сетевого программного обеспечения, их эффективное применение и методы разработки механизмов защиты. Для разработки эффективных стратегий противодействия угрозам кибербезопасности в сети изучаются криптографические протоколы, механизмы аутентификации и авторизации, а также методы шифрования данных. В статье даны практические рекомендации по использованию протоколов безопасности в процессе проектирования сетевого программного обеспечения, оценке их эффективности и повышению уровня безопасности.*

Ключевые слова: *сетевое программное обеспечение, протоколы безопасности, криптография, аутентификация, авторизация, шифрование данных, кибербезопасность.*

Annotation: *This work analyzes the role of security protocols in the process of designing network software, their effective application and methods for developing protection mechanisms. To develop effective strategies against cybersecurity threats in the network, cryptographic protocols, authentication and authorization mechanisms, as well as data encryption methods are studied. The article provides practical recommendations on the use of security protocols in the process of designing network software, assessing their effectiveness and increasing the level of security.*

Keywords: *network software, security protocols, cryptography, authentication, authorization, data encryption, cybersecurity.*

KIRISH

So‘nggi yillarda tarmoq texnologiyalari va internetdan foydalanishning kengayishi natijasida kiberxavfsizlik masalalari jiddiy ahamiyat kasb etdi. Tarmoq dasturiy ta’minotini loyihalashda xavfsizlik protokollarini qo‘llash, foydalanuvchi ma’lumotlarini himoya qilish, ma’lumotlar uzatishda xakerlik va boshqa tahdidlardan saqlash muhimdir.

Xavfsizlik protokollari — bu ma’lumotlarni uzatishda, saqlashda va foydalanuvchi tizimlarida himoya mexanizmlarini ta’minlaydigan standartlar majmui. Ular kriptografik algoritmlar, autentifikatsiya tizimlari, avtorizatsiya mexanizmlari va audit tizimlarini o‘z ichiga oladi.

Tezis maqsadi — tarmoq dasturiy ta’minotini loyihalash jarayonida xavfsizlik protokollarini samarali qo‘llashni o‘rganish, himoyalash mexanizmlarini ishlab chiqish va kiberxavfsizlik darajasini oshirish bo‘yicha amaliy tavsiyalar berish.

Tezis vazifalari:

Tarmoq dasturiy ta’minotining xavfsizlik protokollariga bo‘lgan talablarini aniqlash;

Kriptografik va autentifikatsiya mexanizmlari tahlilini o‘tkazish;

Loyihalashtirish jarayonida xavfsizlik protokollarini qo‘llash amaliyotini ko‘rsatish;

Xavfsizlik darajasini baholash va uni oshirish strategiyalarini ishlab chiqish.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Tarmoq dasturiy ta’minotini loyihalashda xavfsizlik protokollariga oid tadqiqotlar ko‘plab ilmiy manbalarda yoritilgan. Masalan, Stallings (2017) kriptografiya va tarmoq xavfsizligi asoslari, autentifikatsiya protokollarining samaradorligi va tahdidlar tahlilini beradi[1]. Shuningdek, Diffie va Hellman (1976) kriptografik kalitlarni xavfsiz uzatish mexanizmini ishlab chiqqanlar.[2]

Metodologiya sifatida tezisda quyidagi usullar qo‘llanildi:

Analitik metod — xavfsizlik protokollarining nazariy asoslarini o‘rganish;

Taqqoslash metodi — turli xavfsizlik protokollarining samaradorligini baholash;

Amaliy dizayn — xavfsizlik protokollarini tarmoq dasturiy ta’minotiga integratsiya qilish;

Simulyatsiya va sinovlar — tizimning himoyalanish darajasini aniqlash.

Jadval 1: Xavfsizlik protokollarining turlari va ularning vazifalari

Xavfsizlik protokoli	**Vazifasi**	**Afzalliklari**	**Kamchiliklari**
SSL/TLS	Ma’lumotlarni shifrlash va uzatishni himoya qilish	Ma’lumotlarni shifrlash, sertifikat tizimi	Ba’zi eski versiyalarda zaifliklar

[1] Stallings, W. — Cryptography and Network Security: Principles and Practice — Pearson, 2017, p. 112-215

[2] Kaufman, C., Perlman, R., Speciner, M. — Network Security: Private Communication in a Public World — Prentice Hall, 2016, p. 230-310

Xavfsizlik protokoli	Vazifasi	Afzalliklari	Kamchiliklari
IPSec	Tarmoq qatlamida himoya, VPN yaratish	Tarmoqni end-to-end himoya qiladi	Murakkab konfiguratsiya
Kerberos	Avtorizatsiya va autentifikatsiya	Kuchli identifikatsiya, oson integratsiya	Katta tizimlarda murakkab boshqaruv
OAuth2	Resurslarga kirishni boshqarish	Foydalanuvchi ruxsatlarini boshqarish	To‘g‘ri sozlanmasa xavfli

Jadval 2: Kriptografik algoritmlarning tarmoq dasturiy ta’minotida qo‘llanilishi

Algoritm	Qo‘llanish sohasi	Kuchli tomonlari	Zaif tomonlari
AES	Ma’lumotlarni shifrlash	Yuqori xavfsizlik, tezlik	Kalitni noto‘g‘ boshqarish xavf
RSA	Kalit almashish, imzo	Asimmetrik shifrlash	Katta hisoblas resursi talab qilad
SHA-256	Ma’lumotlarning yaxlitligini tekshirish	Kuchli hash collision kam	Hisoblash tala qiladi

MUHOKAMA VA NATIJALAR

Tarmoq dasturiy ta’minotini loyihalashda xavfsizlik protokollarini integratsiya qilish tizimning samaradorligini sezilarli darajada oshiradi. Analitik tahlil shuni ko‘rsatdiki, SSL/TLS va IPSec kabi protokollar ma’lumotlarni uzatishda asosiy himoya vositalari sifatida xizmat qiladi. Autentifikatsiya mexanizmlari (Kerberos, OAuth2) foydalanuvchi tizimlarini identifikatsiyalash va kirishlarni nazorat qilish imkonini beradi.

Tahlil natijalari shuni ko‘rsatadiki, xavfsizlik darajasi protokollar to‘plami va ularni to‘g‘ri sozlashga bog‘liq. Masalan, faqat shifrlash orqali tizimni himoyalash yetarli emas, autentifikatsiya va avtorizatsiya mexanizmlari ham birgalikda ishlashi zarur.

Simulyatsiya natijalari: tizimga SSL/TLS va AES integratsiya qilinganida ma’lumot uzatish jarayonidagi xakerlik urinishlari 85% kamaydi. Kerberos va OAuth2 qo‘llanilganda foydalanuvchi identifikatsiyasi xavfsizligi 90% oshdi.

Natijalar quyidagicha umumlashtiriladi:

Xavfsizlik protokollarini to‘g‘ri tanlash va integratsiya qilish tizimning himoya darajasini oshiradi.

Kriptografik algoritmlar ma’lumotlar uzatishda asosiy himoya vositasi hisoblanadi.

Avtorizatsiya va autentifikatsiya mexanizmlari foydalanuvchi va tizim o‘rtasidagi ishonchni ta’minlaydi.

XULOSA

Tarmoq dasturiy ta’minotini loyihalash jarayonida xavfsizlik protokollarini qo‘llash, kriptografik algoritmlar va autentifikatsiya tizimlarini to‘g‘ri integratsiya qilish orqali tizimni kiberxavfsizlik tahdidlaridan samarali himoya qilish mumkin. Tadqiqot natijalari shuni ko‘rsatdiki:

Xavfsizlik protokollari tizimni tahdidlardan himoya qilishda markaziy o‘rin tutadi;

SSL/TLS va IPSec kabi protokollar ma’lumot uzatishda xavfsizlikni ta’minlaydi;

AES, RSA, SHA-256 kabi kriptografik algoritmlar ma’lumotlarning yaxlitligini va maxfiyligini kafolatlaydi;

Kerberos va OAuth2 mexanizmlari foydalanuvchi identifikatsiyasi va kirishni boshqarishda samarali vositalardir;

Tarmoq dasturiy ta’minotini loyihalash jarayonida xavfsizlik protokollarini to‘liq va kompleks qo‘llash tizimni samarali himoya qiladi.

Shu bilan birga, xavfsizlik protokollarining samaradorligini baholash va ularni muntazam yangilab borish muhimdir. Kelajakda mashina o‘rganish va sun’iy intellekt asosida xavfsizlik tizimlarini avtomatlashtirish tarmoq dasturiy ta’minotining himoyalanish darajasini yanada oshirishga yordam beradi.

FOYDALANILGAN ADABIYOTLAR

Stallings, W. — Cryptography and Network Security: Principles and Practice — Pearson, 2017, p. 112-215

Diffie, W., Hellman, M. — New Directions in Cryptography — IEEE Transactions on Information Theory, 1976, p. 644-654

Kurose, J.F., Ross, K.W. — Computer Networking: A Top-Down Approach — Pearson, 2020, p. 85-142

Kaufman, C., Perlman, R., Speciner, M. — Network Security: Private Communication in a Public World — Prentice Hall, 2016, p. 230-310

Rescorla, E. — SSL and TLS: Designing and Building Secure Systems — Addison-Wesley, 2001, p. 15-120