TECH SCIENCE

ISSN 3030-3702

TEXNIKA FANLARINING DOLZARB MASALALARI

TOPICAL ISSUES OF TECHNICAL SCIENCES

№ 2 (3) 2025

TECHSCIENCE.UZ

№ 2 (3)-2025

TEXNIKA FANLARINING DOLZARB MASALALARI

TOPICAL ISSUES OF TECHNICAL SCIENCES

TOSHKENT-2025

OAK Ro‘yxati
Mazkur jurnal O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasi Rayosatining 2025-yil 8-maydagi 370-son qarori bilan texnika fanlari bo‘yicha ilmiy darajalar yuzasidan dissertatsiyalar asosiy natijalarini chop etish tavsiya etilgan ilmiy nashrlar ro‘yxatiga kiritilgan.

Muassislar: “SCIENCEPROBLEMS TEAM” mas’uliyati cheklangan jamiyati;
Jizzax politexnika insituti.

TECHSCIENCE.UZ- TEXNIKA FANLARINING DOLZARB MASALALARI
elektron jurnali 15.09.2023-yilda 130343-sonli guvohnoma bilan davlat ro‘yxatidan o‘tkazilgan.

TAHRIRIYAT MANZILI:
Toshkent shahri, Yakkasaroy tumani, Kichik Beshyog‘och ko‘chasi, 70/10-uy.
Elektron manzil:
scienceproblems.uz@gmail.com

TEXNIKA FANLARINING
DOLZARB MASALALARI
3-jild, 2-son (may, 2025). -143 bet.

M U N D A R I J A

Texnika fanlarining dolzarb masalalari
Topical Issues of Technical Sciences
2025-yil | 3-jild | 2-son
ISSN (onlayn): 3030-3702

AXBOROT XAVFSIZLIGINI TA’MINLASH TEXNOLOGIYALARI

Abduvoxobov Abbosbek Abdusamat o‘g‘li
Andijon Davlat Texnika Instituti
“Axborot texnologiyalar” kafedrasi assistant o‘qituvchisi,
vip.abduvahobov@mail.ru,
Tel: +998900606600
Andijon viloyati, O‘zbekiston

Annotatsiya. Ushbu maqolada axborot xavfsizligini ta’minlashda qo‘llanilayotgan zamonaviy texnologiyalar, ularning vazifalari hamda samaradorligi yoritilgan. Global axborot makonining kengayishi, kiberxavfsizlik tahdidlarining ortib borishi bilan bir qatorda, axborotni himoya qilish masalasi dolzarb ahamiyat kasb etmoqda. Maqolada axborot xavfsizligini ta’minlashda kriptografik usullar, autentifikatsiya, tarmoq xavfsizligi, xavf tahlili va himoya strategiyalari kabi yo‘nalishlar tahlil qilinadi. Shuningdek, axborot tizimlarining zaifliklarini aniqlash va ularni bartaraf etish bo‘yicha ilg‘or yondashuvlar ham ko‘rib chiqilgan. Maqola sohada faoliyat yurituvchi mutaxassislar hamda tadqiqotchilar uchun foydali bo‘lishi mumkin.

Kalit so‘zlar: axborot xavfsizligi, kiberxavfsizlik, kriptografiya, autentifikatsiya, tarmoq xavfsizligi, ma’lumotlarni himoya qilish, xavf tahlili, axborot tizimi, himoya strategiyalari, axborotni shifrlash.

INFORMATION SECURITY TECHNOLOGIES

Abduvoxobov Abbosbek Abdusamat ugli
Andijan State Technical Institute
Assistant Teacher, Department of “Information Technologies”,
Andijan region, Uzbekistan

Abstract. This article discusses modern technologies used in ensuring information security, their functions and effectiveness. Along with the expansion of the global information space and the increase in cybersecurity threats, the issue of information protection is gaining urgent importance. The article analyzes such areas as cryptographic methods, authentication, network security, risk analysis and protection strategies in ensuring information security. It also considers advanced approaches to identifying and eliminating vulnerabilities in information systems. The article may be useful for professionals and researchers working in the field.

Keywords: information security, cybersecurity, cryptography, authentication, network security, data protection, risk analysis, information system, protection strategies, information encryption.

DOI: https://doi.org/10.47390/ts3030-3702v3i2y2025N05

Axborot xavfsizligini ta’minlashda autentifikatsiya, avtorizatsiya va shifrlash texnologiyalari muhim texnik asos bo‘lib xizmat qiladi. Bu texnologiyalar foydalanuvchining shaxsini aniqlash, unga ruxsat berilgan resurslarga kirishni ta’minlash va ma’lumotlarni himoyalangan shaklda uzatish orqali axborot resurslarini ruxsatsiz kirish va buzilishdan

himoya qiladi. Ular birgalikda ishlaganda axborot xavfsizligining maxfiylik, yaxlitlik va mavjudlik kabi asosiy tamoyillarini amalga oshirishga xizmat qiladi.

Autentifikatsiya bu — foydalanuvchining kimligini aniqlash jarayonidir[4]. Bu jarayon orqali tizimga kirayotgan shaxs haqiqatan kim ekanini tekshiradi. Autentifikatsiyaning eng keng tarqalgan usuli bu login va parol orqali kirishdir. Biroq bu usul zaif bo‘lishi mumkinligi sababli hozirda ko‘p bosqichli autentifikatsiya (Multi-Factor Authentication — MFA) qo‘llaniladi. MFA foydalanuvchidan birdan ortiq isbot talab qiladi: bu biror narsani bilish (parol), biror narsaga egalik qilish (mobil qurilma yoki token), yoki kimdir bo‘lish (biometrik ma’lumotlar, masalan, barmoq izi, yuzni aniqlash) kabi mezonlarga asoslanadi[3][4].

Shuningdek, autentifikatsiya usullariga biometrik autentifikatsiya, bir martalik parollar (OTP), smart kartalar, USB tokenlar va tashqi autentifikatsiya xizmatlari (masalan, Google yoki Microsoft orqali kirish) kiradi. Bu usullar xavfsizlik darajasini oshirish bilan birga, qulaylikni ham ta’minlaydi. Korporativ darajadagi autentifikatsiya tizimlarida LDAP, Kerberos, RADIUS, SAML, OAuth kabi protokollar keng qo‘llaniladi[4].

Autentifikatsiyadan so‘ng navbat avtorizatsiyaga keladi. Avtorizatsiya bu — autentifikatsiyadan muvaffaqiyatli o‘tgan foydalanuvchining tizimda qanday resurslarga kirishi mumkinligini aniqlash jarayonidir. Ya’ni foydalanuvchining huquqlari, rollari va ruxsat darajalarini belgilash. Misol uchun, bir foydalanuvchi faqat o‘qish huquqiga ega bo‘lishi mumkin, boshqasi esa tahrirlash va o‘chirish imkoniyatiga ega bo‘lishi mumkin[4].

Avtorizatsiyani boshqarish jarayonida "Access Control" (kirishni boshqarish) siyosatlari ishlatiladi[9]. Bu siyosatlar discretionary access control (DAC), mandatory access control (MAC) va role-based access control (RBAC) kabi usullar asosida tashkil etiladi. RBAC ayniqsa katta korxonalarda samarali bo‘lib, unda foydalanuvchilarga ularning lavozimi yoki roli asosida huquqlar belgilanadi. MAC esa qat’iy xavfsizlik talablariga ega tizimlarda, masalan, harbiy yoki hukumat tizimlarida qo‘llaniladi[4][9].

Shifrlash texnologiyasi esa ma’lumotlarni uchinchi tomonlardan yashirish va faqat ruxsat etilgan foydalanuvchilargagina uni o‘qish imkonini yaratish uchun qo‘llaniladi. Bu texnologiya ma’lumotlarning maxfiyligini, yaxlitligini va uzatish davomida o‘zgartirilmaganligini kafolatlaydi. Shifrlash yordamida ma’lumotlar ochiq matndan kriptografik matnga aylantiriladi va faqat mos kalit bilan uni yana ochiq holatga qaytarish mumkin bo‘ladi[3].

Shifrlash algoritmlari ikki asosiy turga bo‘linadi: simmetrik va assimetrik[3][7]. Simmetrik shifrlashda bitta kalit orqali ham shifrlash, ham ochish amalga oshiriladi. Masalan, AES (Advanced Encryption Standard), DES, 3DES algoritmlari shular jumlasidandir. Assimetrik shifrlashda esa ikki xil kalit ishlatiladi: ochiq kalit (public key) va yopiq kalit (private key). RSA, ElGamal, ECC (Elliptic Curve Cryptography) kabi algoritmlar bunga misoldir[3].

Shifrlash texnologiyalari internet xavfsizligida ham keng qo‘llaniladi. Masalan, SSL/TLS protokollari veb-brauzerlar va serverlar o‘rtasida xavfsiz aloqani ta’minlash uchun ishlatiladi[6]. VPN (Virtual Private Network) texnologiyasi orqali tarmoqlar o‘rtasida shifrlangan kanal tashkil etiladi. Shuningdek, elektron pochtalar, fayllar, tarmoq trafiklari, ma’lumotlar bazalari ham shifrlanadi[3][6].

Zamonaviy axborot tizimlarida autentifikatsiya, avtorizatsiya va shifrlash texnologiyalari bir-biri bilan uzviy bog‘liq holda ishlaydi. Misol uchun, foydalanuvchi biror veb-xizmatga kirishda avval autentifikatsiyadan o‘tadi, so‘ng unga roli asosida tegishli

huquqlar beriladi, va tizimdagi ma’lumotlar esa uzatish yoki saqlash jarayonida shifrlanadi. Shu orqali ma’lumotlarga faqat vakolatli shaxslar kirish huquqiga ega bo‘ladi va ularning maxfiyligi ta’minlanadi[3][4].

Autentifikatsiya foydalanuvchining kimligini tasdiqlasa, avtorizatsiya uning tizimda nima qilish huquqiga ega ekanligini aniqlaydi, shifrlash esa butun bu jarayon davomida ma’lumotlarning maxfiyligini saqlaydi. Ularning birgalikdagi ishlatilishi zamonaviy axborot tizimlarining xavfsizlik darajasini sezilarli darajada oshirishga xizmat qiladi.

Tarmoqlar xavfsizligi: xavfsizlik devorlari

Zamonaviy axborot infratuzilmasida tarmoqlar muhim rol o‘ynaydi, chunki barcha axborot tizimlari, qurilmalar va foydalanuvchilar tarmoq orqali o‘zaro bog‘lanadi va ma’lumot almashadi[5][10]. Shu sababli, tarmoqlar axborot xavfsizligining asosiy va eng zaif bo‘g‘inlaridan biri hisoblanadi. Tarmoqlar xavfsizligini ta’minlash esa xavfsizlik devorlari (firewall), tajovuzlarni aniqlash va oldini olish tizimlari (IDS/IPS), virtual xususiy tarmoqlar (VPN), segmentatsiya va boshqa texnologiyalar orqali amalga oshiriladi. Ularning ichida ayniqsa xavfsizlik devorlari hamda IDS/IPS tizimlari eng asosiy texnologiyalar sirasiga kiradi[5][6].

Xavfsizlik devori — bu tarmoq xavfsizligini ta’minlash uchun ishlatiladigan dasturiy yoki apparat vositasi bo‘lib, u ichki tarmoq va tashqi tarmoq o‘rtasida nazorat punktini yaratadi. Asosiy vazifasi – kiruvchi va chiquvchi tarmoq trafikini belgilangan siyosat asosida nazorat qilish, ruxsat berilgan va taqiqlangan trafikni ajratishdan iborat. Firewall tizimlari orqali ma’lum portlar, IP manzillar, protokollar, xizmatlar asosida trafik cheklanishi mumkin. Oddiy misol sifatida, faqat HTTP (80-port) va HTTPS (443-port) orqali trafikga ruxsat berilishi, boshqa barcha portlar esa bloklanishi mumkin[5].

1-rasm (IDS/IPS) tizimlari

Zamonaviy xavfsizlik devorlari holatga asoslangan (stateful), kontekstga asoslangan (next-generation), ilovalar darajasida nazorat qiluvchi (application-aware) va hatto kiruvchi trafikni chuqur tahlil qiluvchi (Deep Packet Inspection – DPI) imkoniyatlarga ega. Bunday tizimlar foydalanuvchi faoliyatini tahlil qilish, xatti-harakatlarga qarab xavfli trafikni aniqlash va avtomatik bloklash funksiyalariga ega bo‘ladi.

Tarmoqlar xavfsizligini ta’minlashda faqatgina xavfsizlik devori yetarli emas, chunki ayrim xavfli trafiklar ruxsat berilgan portlar orqali o‘tishi yoki ichki tarmoqdan kelib chiqishi

mumkin. Shu bois, IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) kabi tizimlar qo‘llaniladi. IDS – tajovuzlarni aniqlash tizimi bo‘lib, u tarmoqda shubhali, noodatiy yoki potentsial zararli faoliyatni kuzatadi va bu haqda administratorga xabar beradi. U real vaqt rejimida trafikni skanerlash, ma’lum imzolar asosida tahdidlarni aniqlash yoki xatti-harakatga asoslangan analiz (anomaly detection) orqali tahdidlarni aniqlash imkonini beradi[5].

IPS esa IDS tizimidan farqli ravishda faqat kuzatibgina qolmay, balki aniqlangan tahdidga qarshi avtomatik choralar ko‘radi – masalan, trafikni to‘xtatadi, bog‘lanishni uzadi yoki foydalanuvchini bloklaydi. IPS tizimlari aynan aktiv xavfsizlikni ta’minlaydi, ya’ni tajovuzga real vaqtda javob qaytaradi. IDS/IPS tizimlari ko‘pincha xavfsizlik devori bilan birgalikda ishlaydi va ularning integratsiyasi orqali yanada kompleks himoya choralari yaratiladi[5].

IDS/IPS tizimlari quyidagi asosiy usullar orqali ishlaydi:
– imzoga asoslangan aniqlash (signature-based detection): avvaldan ma’lum bo‘lgan tahdidlar imzolari bilan trafikni solishtirib aniqlaydi
– xatti-harakatga asoslangan aniqlash (behavioral or anomaly-based detection): tarmoqda normal faoliyatdan chetga chiqqan holatlarni tahlil qiladi
– gibrid yondashuv (hybrid): ikkala metodni birgalikda qo‘llab, aniqlik va moslashuvchanlikni oshiradi[5].

Zamonaviy korxonalarda IDS/IPS tizimlari nafaqat tarmoq darajasida, balki host darajasida ham (HIDS/HIPS) qo‘llaniladi. HIDS – har bir kompyuter yoki serverda ishlovchi tajovuz aniqlash vositasi bo‘lib, u fayl tizimi, registr, ilova loglari, tizim faoliyati ustidan nazorat olib boradi. Bu esa tashkilotga ichki tahdidlarga qarshi kuchli himoya qatlamini yaratishga imkon beradi[5].

Xavfsizlik devorlari va IDS/IPS tizimlari birgalikda ishlagan holatda tarmoqqa kirish, ichki harakat va chiqish bosqichlarida to‘liq nazoratni ta’minlaydi. Masalan, xavfsizlik devori orqali kiruvchi trafik filtrlansa, IDS shubhali harakatlarni aniqlaydi, IPS esa tahdidni bartaraf qiladi. Bu yondashuv "Defense in Depth" ya’ni ko‘p qatlamli himoya konsepsiyasiga asoslanadi[5].

Bundan tashqari, xavfsizlikni yanada kuchaytirish uchun virtual xususiy tarmoqlar (VPN), tarmoq segmentatsiyasi, VLAN, DMZ zonalari, MAC-manzil filtratsiyasi va xavfsizlik siyosatlari ham joriy qilinadi. Ammo ularning samarali ishlashi aynan xavfsizlik devorlari va IDS/IPS tizimlari orqali asoslanadi[5][6][9].

tarmoq xavfsizligi — bu har qanday tashkilot uchun fundamental talab bo‘lib, uni ta’minlashda xavfsizlik devorlari va IDS/IPS tizimlarining o‘rni beqiyosdir. Ular nafaqat tashqi tahdidlarni aniqlash va to‘sishda, balki ichki tahdidlarni bartaraf qilishda ham asosiy himoya mexanizmlari sifatida xizmat qiladi. Ularni to‘g‘ri sozlash, doimiy yangilab borish va integratsiyalashgan xavfsizlik strategiyasiga asoslash orqali tashkilot o‘z axborot aktivlarini barqaror va ishonchli himoya ostida saqlashga erishadi[5].

Adabiyotlar/Литература/References:

1. ISO/IEC 27001:2013 – Information security management systems – Requirements. International Organization for Standardization, 2013.
2. ISO/IEC 27002:2013 – Code of practice for information security controls. International Organization for Standardization, 2013.
3. Stallings, W. (2017). Network Security Essentials: Applications and Standards. 6th Edition. Pearson Education.
4. Whitman, M.E., & Mattord, H.J. (2018). Principles of Information Security. 6th Edition. Cengage Learning.
5. Andress, J. (2019). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2nd Edition. Syngress.
6. Kaspersky, E. (2020). Network Security and Cryptography. 3rd Edition. McGraw-Hill.
7. Kaspersky, E. (2020). Network Security and Cryptography. 3rd Edition. McGraw-Hill.
8. Schneier, B. (2015). Secrets and Lies: Digital Security in a Networked World. Wiley.
9. ISO/IEC 27005:2018 – Information security risk management. International Organization for Standardization, 2018.
10. Bertino, E., Sandhu, R. (2005). Database Security: Concepts, Approaches, and Challenges. Springer.
11. Sommers, M. (2020). Cybersecurity and Information Security Fundamentals. CRC Press.
12. Rainer, M. (2020). Network Security: A Beginner's Guide. McGraw-Hill.
13. Merritt, M. (2017). Ethical Hacking and Countermeasures: Web Applications and Data Servers. McGraw-Hill.
14. Bishop, M. (2018). Computer Security: Art and Science. Addison-Wesley

ISSN: 3030-3702 (Onlayn)
САЙТ: https://techscience.uz

TECHSCIENCE.UZ

TEXNIKA FANLARINING DOLZARB MASALALARI

№ 2 (3)-2025

TOPICAL ISSUES OF TECHNICAL SCIENCES

Muassislar: “SCIENCEPROBLEMS TEAM” mas’uliyati cheklangan jamiyati;
Jizzax politexnika insituti.

TECHSCIENCE.UZ- TEXNIKA FANLARINING DOLZARB MASALALARI elektron jurnali 15.09.2023-yilda 130343-sonli guvohnoma bilan davlat ro‘yxatidan o‘tkazilgan.

TAHRIRIYAT MANZILI:
Toshkent shahri, Yakkasaroy tumani, Kichik Beshyog‘och ko‘chasi, 70/10-uy.
Elektron manzil:
scienceproblems.uz@gmail.com