O‘ZBEKISTON RESPUBLIKASI
OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

Ro‘yxatga olindi:
№ 10
2025-yil “28” 04

“TASDIQLAYMAN”
O‘quv ishlari bo‘yicha prorektor
_____ Dj.Sultanov
2025-yil “29” 04

TARMOQ XAVFSIZLIGI
FANINING O‘QUV DASTURI

Bilim sohasi:	600000	–	Axborot-kommunikatsiya texnologiyalari
Ta’lim sohasi:	610000	–	Axborot-kommunikatsiya texnologiyalari
Ta’lim yo‘nalishlari:	60610300	–	Axborot xavfsizligi(Axborot kommunikatsiya texnologiyalari va servis)
	60612100	–	Kiberxavfsizlik injiniringi

Toshkent-2025

Fan/modul kodi NWS1416		O‘quv yili 2025-2026	Semestr 6	ESCTS-kreditlar 4
Fan/modul turi majburiy		Ta’lim tili O‘zbek/rus		Haftadagi dars soatlari 3
1.	**Fanning nomi**	**Auditoriya mashg‘ulotlari (soat)**	**Mustaqil ta’lim (soat)**	**Jami yuklama (soat)**
	Tarmoq xavfsizligi	48	72	120

2.

I. Fanning mazmuni

Fanni o‘qitishdan maqsad – talabalarga tarmoq xavfsizligini ta’minlash sohasidagi xalqaro va milliy me’yoriy hujjatlarni bilish bilan bir qatorda tarmoq xavfsizligini ta’minlashda turli ssenariylarda maxfiylik, yaxlitlik, foydalanuvchanlik va autentifikatsiyalash usul va vositalaridan foydalanish, tarmoqni boshqarish bo‘yicha yuzaga keladigan muammoli vaziyatlarga yechimlarni ishlab chiqish va dasturiy vositalardan foydalangan holda xavfsizlik muammolarini hal qilish ko‘nikmalarini hosil qilishdan iborat.

Fanning vazifasi – talabalarga nazariy bilimlar, amaliy ko‘nikmalar berish, hamda tarmoq xavfsizligining asosiy tushunchalari, tarmoq turlari va tarmoq xavfsizligiga zamonaviy tahdidlar, tarmoq xavfsizligi standartlari va protokollari, tarmoq xavfsizligini ta’minlashda foydalaniladigan apparat va dasturiy vositalarning ahamiyatini ochib berish.

II. Asosiy nazariy qism (ma’ruza mashg‘ulotlari)

Fan tarkibiga quyidagi mavzular kiradi:

1-mavzu. Asosiy tarmoq texnologiyalari va komponentlari bilan tanishish.

Kompyuter xavfsizligi maqsadlari, xavfsizlik xizmatlari va mexanizmlari. X.800 xavfsizlik hujumlarini klassifikatori. Tarmoq va kriptografiya asoslari. Ochiq va yopiq kalitli shifrlashni qo‘llash. Transport qatlamidagi xavfsizlik. SSL va SSH/OpenSSHdan foydalanish. Xavfsiz loyihalashning asosiy tamoyillari.

2-mavzu. Tarmoq xavfsizligi tushunchasi va uning mohiyati.

Kompyuter tarmoqlarida xavfsizlik tushunchasi va tarmoqlarni qurishda tarmoq xavfsizligining mohiyati. Tarmoq topologiyalari va tarmoq tashkil etuvchilari.

3-mavzu. Tarmoq xavfsizligi siyosati va xavfsizlik standartlari.

Kompyuter tizimlari va tarmoqlarida xavfsizlik siyosati tushunchasi. Xavfsizlik monitori (yadro) va xavfsizlik siyosatining asosiy usullari. Tarmoq xavfsizlik siyosatini ishlab chiqish jarayoni. Tarmoq xavfsizligi standartlarining asosiy turlari: O'zDST ISO/IEC 270033. NIST, HIPAA, PCI DSS, GDPR standartlari.

4-mavzu. OSI va TCP/IP modellari.

Tarmoq modellarining yuzaga kelish tarixi. Tarmoq qurilmalari va protokolalarining o'zaro muvofiqligini ta'minlashda tarmoq modellarining o'rni. TCP/IP va OSI modellarining imkoniyatlari va sath protokollari.

5-mavzu. Tarmoq tahdidlari va mexanizmlari.

Internet protokollarining zaifliklari va ularga hujumlar. IP protokoli, TCP funksiyalari, ma'lumotlar formatlari va asosiy xavfsizlik muammolari. DNS qidiruvi, DNS keshlash va DNS paket formatlari tushunchalari. IP-spoofing mexanizmlari, DNS keshini zaharlash va DNS rebinding hujumi. Xizmatdan voz kechish (DoS) zaifligi va SSL handshake paytidagi DoS. SYN cookie-fayllari tushunchalari.

6-mavzu. Tarmoq xavfsizligi ilovalari va xizmatlari.

AH, ESP va IKE yordamida IP xavfsizligiga kirish. Simmetrik kalitlarni taqsimlash va foydalanuvchi autentifikatsiyasi. Ochiq kalitlarni sertifikatlash va ochiq kalitlar infratuzilmasi (X.509). Tarmoq;araro ekran va paketlarni filtrlash printsipiga kirish. Federativ identifikatsiyani boshqarish.

7-mavzu. Veb-ilovalar xavfsizligi va veb-nazorat.

Veb tahdid modellari bilan tanishish. Hujjat obyekti modeli (DOM) va cookie-fayllar uchun yagona manba siyosati (SOP). Saytlararo skript (CSS) va saytlararo so'rovlarni qalbakilashtirish (CSRF). Uchinchi tomon kuzatuv texnikasi; cookie-fayllarni sinxronlashtirish; veb-brauzerlarda sticky training va fingerprinting. "Do Not Track" (DNT) konsepsiyasi. Yagona kirish (SSO). Veb SSO uchun xavfsizlikni tasdiqlovchi belgilash tili (SAML).

8-mavzu. Tarmoqqa kirishni boshqarish va bulut xavfsizligi.

EAP yordamida tarmoqqa kirishni boshqarish tizimiga kirish. Bulutli xizmat modellari: IaaS, PaaS va SaaS. Bulutli muhitda ma'lumotlarni

shifrlash va kriptoboshqaruvining asosiy tushunchalari. Kirishni boshqarish tokenlari

9-mavzu. Tarmoqni boshqarish.

Tarmoqni boshqarish omillari va oddiy tarmoq boshqaruv protokollari (SNMP). Boshqaruv axborot bazasi (MIB) konsepsiyasi va ulardan foydalanish.

10-mavzu. Himoyalangan virtual tarmoq texnologiyalari asoslari.

Virtual tarmoq tushunchasi. Himoyalangan virtual tarmoq turlari. VPN texnologiyalarida PPTP, L2TP, IPSec, OpenVPN, WireGuard protokollaridan foydalanish asoslari. Virtual tarmoq xavfsizligini ta'minlash vositalari va ularning rivojlanish tendensiyalari.

11- mavzu. Tarmoqlararo ekran texnologiyalari.

Tarmoqlararo ekranlarning tarmoq hujumlarining oldini olishdagi o'rni. Tarmoqlararo ekranlarning turlari. Firewall texnologiyalarining afzalliklari va kamchiliklari. Mashhur firewall yechimlari va vositalari (pfSense, IPFire, Cisco ASA, FortiGate). Operatsion tizimlardagi standart firewallar (Windows Firewall, Linux Iptables/NFTables).

12-mavzu. Suqilib kirishlarni aniqlash va bartaraf etish tizimlari.

Kiberxavfsizlikda suqilib kirishlarni aniqlashning dolzarbligi. IDPS texnologiyasi. IDS/IPS tizimlarining farqlari va o'ziga xosliklari. Mashhur IDS/IPS tizimlari (Snort, OSSEC, Zeek, Cisco Firepower, Palo Alto Threat Prevention, McAfee Network Security). Monitoring va tahlil vositalari (SIEM, Loglar va trafikni kuzatuvchi tizimlar (ELK stack, Splunk)).

13-mavzu. Tarmoqda autentifikatsiya, avtorizatsiya va qayd etish masalalari. RADIUS va TACACS+ protokollari.

Tarmoqda autentifikatsiya, avtorizatsiya va qayd etish tushunchalari. RADIUS AAA protokoli uchun IETF-standarti. TACACS+ va uning qo'llanilishi. RADIUS va TACACS+ protokollarining asosiy imkoniyatlari.

III. Amaliy mashg'ulot ishlari bo'yicha ko'rsatma va tavsiyalar

Amaliy mashg'ulot ishlari uchun quyidagi mavzular tavsiya etiladi:

1. Tarmoq qurilmalarida xavfsizlik sozlamalarini o'rnatish va port xavfsizligini sozlash.
2. VTP protokolini sozlash.

3. ACL ro‘yxatini sozlash (standard, extended).
4. Marshrutizatorlarda NAT/PAT texnologiyasini sozlash.
5. Tarmoq marshruzatorida DMZ ni o‘rnatish.
6. Korxona va tashkilot axborot kommunikatsiya tizimlarida VPN tarmoq qurish.
7. DHCP Snooping – xavfsizlik texnologiyasi.
8. ASA xavfsizlik texnologiyasini sozlash.
9. AAA serverda autentifikatsiya rejimini sozlash (RADIUS, TACACS+).

IV. Mustaqil ta’lim va mustaqil ishlar

Mustaqil ta'lim uchun tavsiya etiladigan topshiriqlar:

1. Transmission Control Protocol (TCP) va Internet Protocol (IP) (TCP/IP protokollari) vazifasi va xavfsizligi.
2. Ilova qatlami protokoli (HTTPS)ning ishlash jarayoni va xavfsizligi.
3. Ilova darajasida axborot xavfsizligi protokoli - PGP protokoli (Pretty Good Privacy) xususiyatlari.
4. Transport darajasidagi axborot xavfsizligi protokoli (SSL kriptografik protokoli) qo‘llanilishi va uning ahamiyati.
5. Transport qatlamining xavfsizlik protokollari (TLS protokolidan foydalanganda ma’lumotlarni uzatish) va ularning o‘ziga xos xususiyatlari.
6. IPSec ma’lumotlar himoyasini ta’minlashda protokollar to‘plamining o‘ziga xos xususiyatlari.
7. Autentifikatsiyani ta’minlash protokoli AH protokoli (Authentication Header protocol) va uning muhim jihatlari.
8. Autentifikatsiyani ta’minlash protokoli ESP protokoli (Encapsulating Security Payload - Encapsulating Security Payload) qo‘llanilishi va uning xususiyatlari.
9. DNS (Domain Name System) protokoli va undan domen nomlarini hal qilishda foydalanish.
10. Tarmoq xavfsizligi standartlari (O‘z DSt ISO/IEC 27033) mazmuni va uning mohiyati.
11. BS 7799-1:2005 - Britaniya standarti (Axborot xavfsizligini boshqarish amaliyoti) tavsifi.
12. BS 7799-2:2005 - Britaniya standarti BS 7799 Axborot xavfsizligini boshqarish tizimining spetsifikatsiyasi mohiyati.
13. BS 7799-3:2006 - Britaniya standarti BS 7799. Axborot xavfsizligi risklarini boshqarishda yangi standart tavsifi.
14. ISO/IEC 27001 – “Axborot texnologiyalari – Xavfsizlik amaliyotlari – Axborot xavfsizligini boshqarish tizimlari – Talablar”. BS 7799-2:2005

	asosidagi xalqaro standartlarning muhim jihatlari. 15. ISO/IEC 27002 (2007) - Axborot texnologiyalari - Xavfsizlik texnologiyasi - Axborot xavfsizligini boshqarish amaliyotlari. 16. ISO/IEC 27005 - Axborot xavfsizligi risklarini boshqarish bo'yicha yo'riqnoma. BS 7799-3: 2006 mazmuni va uning mohiyati. 17. Simsiz tarmoqlar xavfsizligi uchun SNAP (Subnetwork Address Protocol) ning o'ziga xos xususiyatlari. 18. Simsiz tarmoqlar xavfsizligini ta'minlashda EAP (Extensible Authentication Protocol) protokolining qo'llanilishi. 19. WPA (Wireless Protected Access) xavfsiz simsiz kirish protokoli xususiyatlari va undan foydalanishdagi jihatlar.
3.	Fan o'qitilishining natijalari (shakllanadigan kompetensiyalar): Fanni o'zlashtirish natijasida talaba: – tarmoqni xavfsiz qurishda tarmoq xavfsizligining asosiy tushunchalari; – tarmoq xavfsizligiga zamonaviy tahdidlari; – tarmoq xavfsizligini ta'minlashning huquqiy - me'yoriy bazasi haqida ***tasavvurga ega bo'lishi***; – tarmoq xavfsizligi protokollari; – tarmoq xavfsizligini ta'minlashda foydalaniladigan usullar, apparat va dasturiy vositalarini qo'llashni ***bilishi va foydalana olishi;*** – tarmoq xavfsizligiga zamonaviy tahdidlarning asosiy turlari hamda ularga qarshi kurashish usullari va ulardan foydalanish; – tarmoq xavfsizligini ta'minlashda himoya qurilmalari va vositalarini qo'llash; – tarmoqdagi axborot xavfsizligi muammolari va ularning yechimlarini tahlil qilish; – tarmoq viruslari va antivirusli himoyalash usullarining muammolarini tahlil qilish; – "bulutli" hisoblash tizimlarida tarmoq xavfsizligini ta'minlash usullarini tahlil qilish ***ko'nikmalariga ega bo'lishi kerak.***
4.	**Ta'lim texnologiyalari va metodlari:** – ma'ruzalar; – interfaol keys-stadilar; – seminarlar (mantiqiy fikrlash, tezkor savol javoblar); – guruhlarda ishlash; – taqdimotlarni qilish; – individual loyihalar; – jamoa bo'lib ishlash va himoya qilish uchun loyihalar.

5.	**Kreditlarni olish uchun talablar:** Fanga oid nazariy va uslubiy tushunchalarni to‘la o‘zlashtirish, tahlil natijalarini to‘g‘ri aks ettira olish, o‘rganilayotgan jarayonlar haqida mustaqil mushohada yuritish va joriy va oraliq nazorat shakllarida berilgan vazifa va topshiriqlarni bajarish, yakuniy nazorat bo‘yicha yozma ishni topshirish.
6.	**Asosiy adabiyotlar** 1. Dijiang Huang, Ankur Chowdhary, Sandeep Pisharody, Software-Defined Networking and Security 1st Edition, c2021. 2. J. Michael Stewart, Denise Kinsey, Network Security, Firewalls, and VPNs (Issa) 3rd Edition, c2020. 3. Russell Scott, Computer Networking Beginners Guide: An Easy Approach to Learning Wireless Technology, Social Engineering, Security and Hacking Network, Communications Systems, c2020. 4. Н.Б.Насруллаев., С.Ш.Муминова., М.Ш.Агзамова. Безопасность сетей. O‘quv qo‘llanma. Toshkent. “Metodist” nashriyoti. 2024 y. 270-b. 5. Кучкаров Тахир Анварович, Безопасность сетей, 2022. 292 -с. **Qo‘shimcha adabiyotlar** 6. Quinn Kiser, Cybersecurity: A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering, c2020. 7. Ben Malisow, CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide & Practice Tests Bundle 2nd Edition, c2020. 8. Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals (MindTap Course List) 7th Edition, c2020. 9. Ian Neil, CompTIA security+ certification guide: master IT security essentials and exam topics for CompTIA security+ SY0-501 certification, Birmingham: Packt Publishing 2018, (eBook, online access) 10. Stallings, William, Cryptography and Network Security: Principles and Practice (7th Edition): Pearson, c2016. **Internet saytlari** 11. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.800-199103- I!!PDF-E&type=items) 12. https://csec.uz/ru/docs/OzDSt_27002_2016.pdf 13. https://lex.uz/acts/-3610935
7.	Mazkur o‘quv dastur universitet Kengashining 2025-yil “29” 04. 8/9/750/750-son bayonnomasi bilan tasdiqlangan.

8.	**Fan/modul uchun ma'sullar:** Haydarov E.D. – Muhammad al-Xorazmiy nomidagi TATU, "Axborot xavfsizligi" kafedrasi mudiri, PhD. Muminova S.Sh – Muhammad al-Xorazmiy nomidagi TATU, "Axborot xavfsizligi" kafedrasi katta o'qituvchisi.
9.	**Taqrizchilar:** Nasrullayev N.B. – Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Nurafshon filiali direktori, dotsent, PhD. Samarov H.K. – Muhammad al-Xorazmiy nomidagi TATU, "Axborot xavfsizligi" kafedrasi dotsenti, t.f.n.