O'ZBEKISTON RESPUBLIKASI OLIY TA'LIM, FAN VA INNOVATSIYALAR VAZIRLIGI
BUXORO DAVLAT UNIVERSITETI

"TASDIQLAYMAN"
Buxoro davlat universiteti rektori
_____ O.X. Xamidov
«29» avgust 2025 yil

Ro`yxatga olindi:
2025 yil "29" avgust
№ BD-60610100-1.12
№ BD-60610200-1.12
№ BD-60610400-1.12
№ BD-60610500-1.12

KIBERXAVFSIZLIK ASOSLARI
O'QUV DASTURI

Bilim sohasi:	600 000 – Axborot-kommunikatsiya texnologiyalari
Ta'lim sohasi:	610 000 - Axborot-kommunikatsiya texnologiyalari
Ta'lim yo'nalishi:	60610100-Axborot tizimlari va texnologiyalari 60610200 - Axborot xavfsizligi 60610400 – Dasturiy injiniring 60610500 - Sun'iy intellekt

Mazkur fan dasturi xalqaro tan olingan reytinglarda **Computational Science and Engineering sohasi bo'yicha** birinchi 300 talik ro'yxatga kiruvchi Technical **University of Munich (29 o'rin)** ta'lim dasturi asosida tayyorlandi.

Web havola: *https://www.cit.tum.de/cit/studium/studiengaenge/master-computational-science-engineering/*

Buxoro-2025

Fan/modul kodi	O‘quv yili	Semestr	ECTS - Kreditlar
KIA1406	2026-2027	4- semestr	6
Fan/modul turi	**Ta’lim tili**		**Haftadagi dars soatlari**
Majburiy	O‘zbek		5

1.	Fanning nomi	Auditoriya mashg‘ulotlari (soat)	Mustaqil ta’lim (soat)	Jami yuklama (soat)
	Kiberxavfsizlik asoslari	72	108	180

2. **I.Fanning mazmun**

Fanning maqsadi

“Kiberxavfsizlik asoslari” fanining maqsadi — talabalarni zamonaviy axborot muhitida yuzaga keladigan xavfsizlik tahdidlari, ularning turlari, oldini olish usullari hamda axborotni himoya qilishning texnik, tashkiliy va dasturiy mexanizmlari haqida fundamental bilimlar bilan qurollantirishdir.

Fan kiberxavfsizlik madaniyatini shakllantirish, axborot tizimlarini himoya qilishda zarur bo‘lgan amaliy ko‘nikmalarni rivojlantirishni ko‘zda tutadi.

Fanning vazifalari — talabalarni axborot xavfsizligining asosiy tushunchalari bilan tanishtirish, kiber tahdid va zaifliklarni aniqlash, ularning oldini olish bo‘yicha amaliy ko‘nikmalarni shakllantirish, kriptografiya, tarmoq xavfsizligi va himoya tizimlari tamoyillarini o‘rgatish, shuningdek kibergigiyena va axborot xavfsizligi madaniyatini rivojlantirishdan iborat.

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

II.I. Fan tarkibiga quyidagi mavzular kiradi:

1-mavzu. Kiberxavfsizlikning asosiy tushunchalari.

Konfidensiallik, yaxlitlik va foydalanuvchanlik tushunchalari. Kiberxavfsizlikda inson omili.

2-mavzu. Axborotning kriptografik himoyasi.

Kriptografiyaning asosiy tushunchalari. Simmetrik kriptografik tizimlar. Ochiq kalitli kriptotizimlar. Ma'lumotning yaxlitligini ta'minlash usullari. Disklari va fayllarni shifrlash. Ma'lumotlarni xavfsiz o'chirish usullari.

3-mavzu. Foydalanishni nazoratlash.

Foydalanishni nazoratlashning asosiy tushunchalari. Parolga asoslangan autentifikatsiya usuli. Ma'lumotlarni fizik himoyalash. Ma'lumotlardan foydalanishni mantiqiy boshqarish.

4-mavzu. Tarmoq xavfsizligi.

Tarmoq xavfsizligi zaiflikalari. Tarmoqlararo ekran va virtual himoyalangan tarmoq. Simsiz tarmoqlar xavfsizligi.

5-mavzu. Foydalanuvchanlikni ta'minlash usullari.

Foydalanuvchanlik va uning tizimlar uchun muhimligi. Ma'lumotlarni zaxira nusxalash usullari. Ma'lumotlari qayta tiklash usullari. Hodisalarni qaydlash.

6-mavzu. Dasturiy vositalar xavfsizligi.

Dasturiy vositalardagi xavfsizlik muammolari. Dasturiy vosita xavfsizligining fundamental prinsiplari. Zararkunanda dasturiy kodlar.

7-mavzu. Axborot xavfsizligi siyosati va risklarni boshqarish.

Tizimlarning umumiy arxitekturasi. Axborot xavfsizligi siyosati va uni amalga oshirish. Risklarni boshqarish.

8-mavzu. Kiberjinoyatlarning inson xavfsizligiga ta'siri.

Kiberjinoyatchilik, kiberhuquq va kiberetika. Inson xavfsizligi.

III. Amaliy mashg'ulotlari buyicha ko‘rsatma va tavsiyalar Amaliy mashg'ulotlar uchun quyidagi mavzular tavsiya etiladi:

1-mavzu. Kiberxavfsizlikning asosiy tushunchalari.

Konfidensiallik, yaxlitlik va foydalanuvchanlik tushunchalari. Kiberxavfsizlikda inson omili.

2-mavzu. Axborotning kriptografik himoyasi.

Kriptografiyaning asosiy tushunchalari. Simmetrik kriptografik tizimlar. Ochiq kalitli kriptotizimlar. Ma'lumotning yaxlitligini ta'minlash usullari. Disklarni va fayllarni shifrlash. Ma'lumotlarni xavfsiz o'chirish usullari.

3-mavzu. Foydalanishni nazoratlash.

Foydalanishni nazoratlashning asosiy tushunchalari. Parolga asoslangan autentifikatsiya usuli. Ma'lumotlarni fizik himoyalash. Ma'lumotlardan foydalanishni mantiqiy boshqarish.

4-mavzu. Tarmoq xavfsizligi.

Tarmoq xavfsizligi zaiflikalari. Tarmoqlararo ekran va virtual himoyalangan tarmoq Simsiz tarmoqlar xavfsizligi.

5-mavzu. Foydalanuvchanlikni ta'minlash usullari.

Foydalanuvchanlik va uning tizimlar uchun muhimligi. Ma'lumotlarni zaxira nusxalash usullari. Ma'lumotlarni qayta tiklash usullari. Hodisalarni qaydlash.

6-mavzu. Dasturiy vositalar xavfsizligi.

Dasturiy vositalardagi xavfsizlik muammolari. Dasturiy vosita xavfsizligining fundamental prinsiplari. Zararkunanda dasturiy kodlar.

7-mavzu. Axborot xavfsizligi siyosati va risklarni boshqarish.

Tizimlarning umumiy arxitekturasi. Axborot xavfsizligi siyosati va uni amalga oshirish. Risklarni boshqarish.

8-mavzu. Kiberjinoyatlarning inson xavfsizligiga ta'siri. Kiberjinoyatchilik, kiberhuquq va kiberetika. Inson xavfsizligi.

Amaliy mashg'ulotlar kompyuter bilan jihozlangan auditoriyada bir akademik guruhga bitta professor-o'qituvchi tomonidan o'tkazilishi zarur. Mashg'ulotlar faol va interfaktiv usullar yordamida o'tilishi, mos ravishda munosib pedagogik va axborot texnologiyalar qo'llanilishi maqsadga muvofiq.

IV. Mustaqil ta'lim va mustaqil ishlar

Mustaqil ta'lim uchun tavsiya etiladigan mavzular:

1. Kiberxavfsizlik tushunchasi.
2. Axborotni konfidensialligini ta'minlash. 3. Axborotni yaxlitligini ta'minlash.
4. Risk va uning kiberxavfsizlikdagi o'mi.
5. Axborot xavfsizligi va axborotni himoyalash tushunchalari.
6. Kiberxavfsizlikning bilim sohalari.
7. Kiberxavfsizlikda inson omili.
8. Kriptografiyaning asosiy tushunchalari shifrlash, deshifrlash, kalit, shifr, ochiq matn, shifrmatn.
9. Axborotni simmetrik va ochiq kalitli shifrlash algoritmlari yordamida shifrlash.
10. Kriptologiya va steganografiya.
11. Xesh funksiya, ularga qo'yilgan talablar va uni axborot himoyalashdagi o'rni.
12. Kriptografik akslantirishlar.
13. RSA algoritmi.
14. DES algoritmi.
15. Elektron raqamli imzo.
16. Elektron ko'rinishdagi ma'lumotlarni yo'q qilish.
17. Ruxsatlarni nazoratlashning asosiy tushunchalari.
18. Foydalanuvchilarni autentifikasiyalash usullari va ularning xususiyatlari.
19. Axborotning fizik himoyasi.
20. Foydalanishni boshqarishning DAC usuli va uning xususiyatlari.
21. Foydalanishni boshqarishning MAC usuli va uning asosiy xususiyatlari.
22. Foydalanishni boshqarishning RBAC usuli va uning asosiy xususiyatlari.
23. Foydalanishni boshqarishning ABAC usuli va uning asosiy xususiyatlari.
24. Tarmoq topologiyasi.
25. Tarmoq qurilmalarining: tarmoq kartasi, repitor, hub, switch, router, ko'priklar, shlyuzlar.
26. Asosiy tarmoq protokollari.
27. Tarmoq xavfsizligi zaifliklari.
28. Tarmoq xavfsizligiga hujumlar.
29. Tarmoqlararo ekran.

30. VPN tarmoqni qurish.
31. Dasturiy mahsulotlarda xafsizlik ta'minlash.
32. Kompyuter viruslari.
33. Antivirus dasturiy vositalari.
34. Internetdan foydalanish siyosati.
35. Kiberjinoyatchilik va uni oldini olish.

Mustaqil o'zlashtiriladigan mavzular bo'yicha talabalar tomonidan referatlar tayyorlash va uni taqdimot qilish tavsiya etiladi.

3. **V. Ta'lim texnologiyalari va metodlari:**

- ma'ruzalar;
- interfaol keys-stadilar;
- seminarlar (mantiqiy fikrlash, tezkor savol-javoblar);
- guruhlarda ishlash;
- taqdimotlar qilish;
- individual loyihalar;
- jamoa bo'lib ishlash va himoya qilish uchun loyihalar.

4. **VI. Kreditlarni olish uchun talablar:**

Fanga oid ilmiy-nazariy tushunchalarni to'la o'zlashtirish, egallagan nazariy bilimlarni amalda qo'llash va natijalarni to'g'ri aks ettira olish, o'rganilayotgan fan doirasida mustaqil mushohada yuritish va joriy, oraliq nazorat shakllarida berilgan vazifa hamda topshiriqlarni bajarish, yakuniy nazorat bo'yicha yozma ishni topshirish.

5. **Asosiy adabiyotlar**

1. Atayeva G.I. Axborot xavfsizligi asoslari. Buxoro: Durdona nashriyoti, 2024 y. -128 b.
2. Tahirov B.N. Axborot xavfsizligi asoslari. Buxoro:Fan va ta'lim nashriyoti, 2022 y. -156 b.
3. Akbarov D.E. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi // Toshkent, 2008, -B. - 394.
4. Ganiev S.K., Karimov M.M., Xudoyqulov Z.T., Kadirov M.M. Axborot xavfsizligi bo'yicha atama va tushunchalarning rus, o'zbek va inliz tillaridagi izohli lug'ati // Toshkent 2017, -B. - 480.

Qo'shimcha adabiyotlar

1. Alex Intrigue. Cybersecurity Bible: The Comprehensive Operational Handbook with Practical Tests for Training IT Security Specialists and Excelling in Industry Certification Exams. Independently published-2024. - 174-p.

2. Ferguson N., Schneier B. Practical cryptography // New York: Wiley. 2003. - P. - 432.
3. Lester Nichols. Cybersecurity Architect's Handbook: An end-to-end guide to implementing and maintaining robust security architecture. Packt Publishing-2024. 494-p.
4. Joseph Steinberg, Kevin Beaver CISSP, Ira Winkler CISSP, Ted Coombs. Cybersecurity All-in-One for Dummies. Tantor Audio-2023. 490 p.

Axborot manbaalari

1. http://smartkardtechnologies.com/productdetails/acr39u-smart-cardrader.
2. https://www.ptsecurity.com/ww-yen/analytics/web-vulnerabilities2020
3.https://www.fbi.gov/services/information-management/foipa/privacyimpact-assessments/iafis

7. Fan dasturi Buxoro davlat universitetida ishlab chiqilgan va tasdiqlangan.

Fan/ modul uchun mas'ullar:
Ramazonov Sh.H - BuxDU «Axborot tizimlari va raqamli texnologiyalar» kafedrasi o'qituvchisi _____

9. **Taqrizchilar:**
Ibragimov U. M. - BMTI "Texnologik jarayonlarni boshqarishda axborot kommunikatsiya texnologiyalari" kafedrasi dotsenti, p.f.f.d.(PhD);

I.I. Bakayev - BuxDU "Axborot tizimlari va raqamli texnologiyalari" kafedrasi dotsenti, t.f.f.d. (PhD).