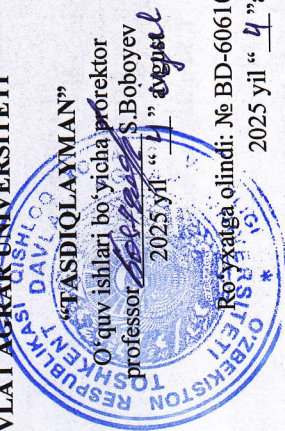


3

O'ZBEKISTON RESPUBLIKASI
OLIIY TA'LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

TOSHKENT DAVLAT AGRAR UNIVERSITETI



Ro'yxatga olindi: № BD-60610200-1.19
2025 yil "4" avgust

AXBOROT XAVFSIZLIGI

O'QUV DASTURI

Bilim sohasi:	600 000	-	Axborot kommunikatsiya texnologiyalari
Ta'lim sohasi:	610 000	-	Axborot kommunikatsiya texnologiyalari
Ta'lim yo'nalishi:	60610200	-	Axborot tizimlari va texnologiyalari (qishloq xo'jaligida raqamli texnologiyalar)

Toshkent - 2025

Fan/modul kodi AXXVFB1506	O'quv yili 2025-2026	Semestr 5	ECTS - Kreditlar 6
Fan/modul turi Majburiy	Ta'lim tili O'zbek/rus	Haftadagi dars soatlari 6	
Fanning nomi	Auditoriya mashg'ulotlari (soat)	Mustaqil ta'lim (soat)	Jami yuklama (soat)
1. Axborot xavfsizligi	72	108	180

2. I. Fanning mazmuni

Fanni o'qitishdan maqsad – talabalarga axborot xavfsizligidan nazariy, uslubiy va texnologik asoslarini, tizimlarning xavfsizligini ta'minlash usullarini o'rgatish, Ma'lumotlarning maxfiyligi (confidentiality), to'liqligi (integrity) va mavjudligini (availability) (CIA triad) himoya qilish tamoyillari. Kiberxavflar (viruslar, ransomware, DDoS hujumlari) va ularning oldini olish usullari. Zamonaviy tahdidlarga qarshi tayyorgarlikni shakllantirish, Amaliy ko'nikmalarni rivojlantirish, Sun'iy intellekt va ma'lumotlar tahlilidan (AI/ML) foydalangan holda xavfsizlikni avtomatlashtirish.

Fanning vazifasi - talabalarni nazariy bilimlar, amaliy ko'nikmalar, axborot texnologiyalari bilan bog'liq jarayonlarga uslubiy yondashuv hamda ilmiy-texnikaviy dunyoqarashini yanada shakllantirish, ma'lumotlarni barcha tahdidlardan himoya qilish, ularning ishonchiligi saqlash va zamonaviy dunyoda kiberxavfsizlikni global miqyosda mustahkamlashdir.

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

II.I. Fan tarkibiga quyidagi mavzular kiradi:

Asosiy nazariy qism (ma'ruza mashg'ulotlari)

1-mavzu. Axborot xavfsizligi tushunchasi va xavfsizlik masalalari

Axborot xavfsizligiga kirish. Milliy xavfsizlik tushunchasi. Axborot xavfsizligini ta'minlashning asosiy vazifalari va darajalari. Xavfsizlik siyosati. Axborot xavfsizligi arxitekturasini va strategiyasi.

2-mavzu. Axborot xavfsizligiga bo'ladigan tahdidlar, Xavfsizlikning asosiy printsiplari

Axborot xavfsizligiga tahdidlar va ularning tahlili. Axborot xavfsizligining zaifliklari. Axborotning maxfiyligini, yaxlitligini va foydalanuvchanligini

buzish usullari. Bo'lishi mumkin bo'lgan tahdidlarni oldini olish. Mahfiylik (shifrlash, access control). Butunlik (xemlap, digital imzo). Mavjudlik (DDoS-dan himoy).

3-mavzu. Axborot xavfsizligi sohasiga oid xalqaro va milliy me'yoriy-huquqiy baza

Axborot xavfsizligi sohasiga oid xalqaro standartlar. Axborot xavfsizligi sohasiga oid xalqaro va milliy standartlar. Axborot xavfsizligi sohasiga oid normativ hujjatlar.

4-mavzu. Axborot xavfsizligi siyosati va xavfsizlik modellari

Axborot xavfsizligini buzuvchining modeli. Maqsadlar va usullarga bog'liq holda axborot xavfsizligini buzuvchilar kategoriyalari. Kompyuter tizimlari va tarmoqlarda xavfsizlik modellari, Bella va La-Padula modeli, Denning modeli, Landver modeli. Xarrison-Ruzzo-Ulmannning diskretion modeli. Bella-Lapadulaning mandatli (muxtor huquqli) modeli. Xavfsizlikning roli modeli.

5-mavzu. Axborot xavfsizligidagi xavflar turlari

Zamonaviy xavflar va ularning manbalari, Fishing, malvar, ransomware. Ijtimoiy muhandislik va APT (Advanced Persistent Threat). Zero-day exploit va ularning ta'siri. WannaCry, NotPetya hujumlar tahlili. WannaCry, NotPetya hujumlar tahlili.

7-mavzu. Kriptografiya asoslari

Asosiy atamalar va ta'riflar. Kriptotizimlarga qo'yiladigan asosiy talablar. Kriptografik tizimlarning tasnifi. Shifrlash va deshifrlash. SSL/TLS va HTTPS ishlashi. Kriptografiyaning asosiy qoidalari va ta'riflari. Shifrlash usullarining turkumlanishi, simmetrik (maxfiy) va asimmetrik (ochiq) kaliti shifrlash tizimlari, almashtirish (podstar.ovka) usullarining mohiyati. RSA algoritmining matematik asoslari

6-mavzu. Autentifikatsiya va avtorizatsiya

Asosiy tushunchalar va turkumlanishi. Identifikatsiya, autentifikatsiya, foydalanuvchilarning haqiqiylikni aniqlash, avtorizatsiya, ma'murlash, ma'lumotlarni uzatish kanallarini himoyalashda sub'ektlarning o'zaro autentifikatsiyasi. Biometrik ma'lumotlardan foydalangan holda identifikatsiya/autentifikatsiya. Identifikatsiya kartalari va elektron kalitlar. Umumiy ma'lumot. Magnit chiziqli kartalar. Smart kartalar va USB kalitlarga murojaat qiling. Kontaktsiz RFID kartalari.

8-mavzu. Tarmoq xavfsizligi

Computer tarmog'i tushunchasi. Tarmoq xavfsizligi muammolari. Tarmoq xavfsizligi ta'minlovchi vositalar. Simsiz tarmoq xavfsizligi. Simsiz tarmoq tuzilmasi. Simsiz shaxsiy tarmoqlar. Simsiz regional tarmoqlar, simsiz global tarmoqlar. Simsiz tarmoq tuzilmasi, simsiz tarmoq xavfsizligi protokollari. Simsiz qurilmalar xavfsizligi muammolari.

9-mavzu. Axborotni himoyalashda tarmoqlararo ekranlarning o'rni
Tarmoqlararo ekranlarning ishlash xususiyatlari. Ochiq tashqi tarmoq, himoyalangan ichki tarmoq. Tarmoqlararo ekranni ulash sxemasi, Tarmoqlararo ekranlarning asosiy komponentlari. Tarmoqlararo ekranlar asosidagi tarmoq himoyasining sxemalari. Tarmoqlararo ekranlarni ulashning asosiy sxemalari, yopiq va ochiq qism tarmoqlarni alohida himoyalovchi sxemalar.

10-mavzu. Kompyuter viruslari va ulardan himoyalash mexanizmlari

Kompyuter virusining ta'riflari. Viruslarni asosiy alomatlar bo'yicha turkumlashi, yashash makoni bo'yicha kompyuter viruslarining turkumlanishi. Virusni xotiraga yuklash, zarar keltiruvchi dasturlarning boshqa turlari. Viruslar va zarar keltiruvchi dasturlarni tarqatish kanallari. Virusga qarshi dasturlar, virusga qarshi dasturlarning turlari, himoyaning profilaktika choralarlari.

11-mavzu. Virtual himoyalangan tarmoqlar

Himoyalangan virtual hususiy tarmoqlarni qurish kontseptsiyasi. VPN kontseptsiyasi. Virtual himoyalangan tarmoqlarni qurish variantlari. Himoyalangan virtual hususiy tarmoqlarning turkumlanishi.

12-mavzu. Hujumlarni aniqlash va tahlil qilish.

SIEM tizimlari (Splunk, ELK Stack). Digital forensics asoslari. Signature-Based Detection (Imzalar asosida aniqlash), Me'yoriylashtirilgan xarakatlardan chetlashgan faolliklarni aniqlash, IP manzil, MAC-manzil, foydalanuvchi akkauntini aniqlash, Wireshark yordamida trafikni tahlil qilish. Ma'lumotlarni zahiralash texnologiyalari va usullari. Ma'lumotlarni qayta tiklash va hodisalarni qayd qilish.

III. Amaliy mashg'ulotlari bo'yicha ko'rsatma va tavsiyalar

Amaliy mashg'ulotlari uchun tavsiya etilayotgan mavzular:

1. Axborot xavfsizligi tamoyillari va asosiy atamalarini o'rganish
2. Tashkilot axborot xavfsizligi siyosatini ishlab chiqish
3. Axborotga nisbatan bo'ladigan xavf-xatarlar va zaifliklarni o'rganish va tahlil qilish
4. Axborot xavfsizligi sohasiga oid xalqaro va milliy me'yoriy - huquqiy hujjatlar bilan tanishish
5. Axborotlarni himoyalashning tashkiliy va texnik choralarlari
6. Axborotlarni himoyalashning dasturiy choralarlari
7. Axborot xavfsizligini buzuvchining modeli va axborot xavfsizligini ta'minlash modellari
8. Identifikatsiyalash va autentifikatsiyalash usullari
9. Kriptografik himoyalash usullari
10. Ma'lumotlarni asimmetrik algoritmlar yordamida shifrlash
11. Simmetrik o'rin almashtirish algoritmlari yordamida shifrlash
12. Elektron raqamli imzo
13. Tarmoq xavfsizligi
14. Simsiz tarmoq xavfsizligini ta'minlash usullari
15. Tarmoqlararo ekranni o'rnatish va sozlash
16. Viruslar va ulardan himoyalash usullari
17. Antivirus dasturlarini o'rnatish va uni sozlash
18. Operatsion tizim himoyasi, Windows 7 O'ring "Xavfsizlik parametrlari" ni o'rnatish
19. Ma'lumotlarni ruxsatsiz chiqib ketishini oldini olish usul va vositalari
20. Virtual himoyalangan tarmoqlar bilan ishlash
21. Butunlikni nazorat qilish protokollari
22. Ma'lumotlarni arxivlash va tiklash
23. Ma'lumotlarni zahiralash texnologiyalari va usullari.
24. Ma'lumotlarni qayta tiklash va hodisalarni qayd qilish.

Amaliy mashg'ulotlar multimedia qurilmalari bilan jihozlangan auditoriyada bir akademik guruhga bir professor-o'qituvchi tomonidan o'tkazilishi zarur.

IV. Mustaqil ta'lim va mustaqil ishlar

Mustaqil ta'lim uchun tavsiya etiladigan mavzular:

1. Axborot xavfsizligiga tahdidlarga qarshi O'zbekiston Respublikasida ishlab chiqilgan qonunlar, farmoyishlar va qarorlar tahlili.
2. Axborot-kommunikatsiya texnologiyalari xavfsizligiga bo'ladigan tahdidlar.
3. Zararkunanda dasturlarning turlari.

<p>4. Axborot xavfsizligini ta'minlash bo'yicha ishlab chiqilgan xorijiy davlatlar standartlari tahlili.</p> <p>5. Axborot xavfsizligida identifikatsiya va autentifikatsiya</p> <p>6. Tarmoqlararo ekran texnologiyasi.</p> <p>7. Himoyalangan virtual xususiy tarmoqlar (VPN).</p> <p>8. Axborot-kommunikatsiya tizimlariga ruxsatsiz kirishlarni aniqlash.</p> <p>9. Simsiz aloqa tizimlarida axborotni himoyalash.</p> <p>10. Axborotni ruxsatsiz foydalanishlardan himoyalash.</p> <p>11. Elektromagnit nurlanishlar va ular orqali axborotlarni sirqib chiqish xavflari.</p> <p>12. Operatsion tizimlar xavfsizligini ta'minlash</p>	<p>3. V. Ta'lim natijalari (shakllantirilgan kompetensiyalar) Fanni o'zlashtirish natijasida talaba:</p> <ul style="list-style-type: none"> Axborot xavfsizligi fanining o'imi va ahamiyati, axborotning nazariy asoslari va ularning kompyuterda tasvirlanish jarayonlari, axborot jarayonlarining apparat va dasturiy ta'minoti, obyekt va jarayonlar holati haqida axborotlarni yig'ish, qayta ishlash, saqlash va uzatish usul va vositalari, zamonaviy axborot texnologiyalarining yo'nalishlari haqida tasavvurga ega bo'lishi; amaliy dasturiy vositalar orqali qishloq xo'jaligi va iqtisodiy soxaga oid masalalarni yechish, axborotlarga ishlov berish dasturlari orqali matn, tasvir va grafika ko'rinishdagi elektron resurslarini yaratish, ularni qayta ishlash, axborot texnologiyaning dasturiy va apparat vositalari va usullaridan xamda axborot tizimlaridan sohani boshqarish jarayonlarida foydalana olish, boshqaruv jarayonlariga oid axborotlarni qayta ishlash va ular asosida boshqaruv qarorlarini qabul qilish haqida bilishi va ulardan foydalana olishi; zamonaviy kompyuter va uning dasturiy vositalari, kompyuterga xizmat ko'rsatuvchi dasturlari bilan ishlash, axborotlarga ishlov beruvchi dasturiy vositalardan, internet tarmog'i va milliy tarmoq resurslaridan, davlat interaktiv xizmatlaridan, ma'lumotlar bazalaridan, axborot tizimlaridan foydalanish bo'yicha ko'nikmalarga ega bo'lishi kerak;
<p>4. VI. Ta'lim texnologiyalari va metodlari:</p> <ul style="list-style-type: none"> ma'ruzalar; interfaol keys-stadilar; (mantiqiy fikrlash, tezkor savol-javoblar); guruhlarda ishlash; taqdimotlarni qilish; individual loyihalar; 	

	<p>mushohada yuritish va nazorat uchun berilgan vazifa va topshiriqlarni bajarish, yakuniy nazorat bo'yicha (yozma yoki test) ishni topshirish.</p> <p>6. Asosiy adabiyotlar</p> <ol style="list-style-type: none"> G'aniev S. K., Karimov M. M., Tashev K. A. "Axborot xavfsizligi", "Fan va texnologiyalar" nashriyoti, Toshkent 2016 Mark Stamp. Information security. Principles and Practice. Second edition. A John Wiley & Sons, Inc., publication. Printed in the United States of America. 2011y. 584p. Шангин В.Ф. "Информационная безопасность и защита информации", Учебное пособие. Москва: 2014. <p>Qo'shimcha adabiyotlar</p> <ol style="list-style-type: none"> Mirziyoev Sh.M. Qonun ustuvorligi va inson manfaatlarini ta'minlash-yurt taraqqiyoti va xalq farovonligining garovi. 2017. Т.Л. Партка, И.И. Попов. Информационная безопасность. 4-е издание. Москва «Форум», 2011. "Axborot texnologiyasi. Axborotlarni kriptografik muhofazasi. Ma'lumotlarni shifrlash algoritmi" O'zbekiston Davlat standarti. O'zDSt 1105:2009. Шнафер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.- М.: Издательство ТРИУМФ, 2003 – 816 <p>Internet saytlari</p> <ol style="list-style-type: none"> http://www.ziyounet.uz http://uz.denemetr.com/download/docs-229149/768-229149.doc http://www.nasa.gov/statistics/ http://www.security.uz http://www.cert.uz http://www.uzinfocom.uz
6.	<p>7. Fan dasturi Toshkent davlat agrar universiteti Ilmiy Kengashining 202 <u>5</u> yil "<u>4</u>" <u>iyul</u> dagi "<u>3</u>" – sonli bayoni bilan ma'qullangan.</p>
8.	<p>Fan/modul uchun ma'sullar: Noraliyev N.X. - "Axborot tizimlari va texnologiyalari" kafedrasini professori, f.m.f.n</p>
9.	<p>Taqrizchilar: Xayitboyev K. – "Axborot tizimlari va texnologiyalari" kafedrasini dotsenti Turgunov A. - AI - Xarazmiy nomidagi Toshkent Axborot texnologiyalar universiteti dotsenti</p>