

9

O'ZBEKISTON RESPUBLIKASI

OLIY TA'LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

TOSHKENT DAVLAT AGRAR UNIVERSITETI



Ro'yxatga olingdi: № BD-60610100-1.12  
2025 yil 04'

### KIBERXAVFSIK ASOSLARI O'QUV DASTURI

Bilim sohasi:

600 000 - Axborot kommunikatsiya texnologiyalari

Ta'lim sohasi

610 000 - Axborot kommunikatsiya texnologiyalari

Ta'lim yo'nalishlari:

60610100 - Axborot tizimlari va texnologiyalari

Toshkent - 2025



Fan/modul kodi	O'quv yili	Semestr	ECTS - Kreditlar
KIA1406	2025-2026	4	6
Fan/modul turi	Ta'lim tili	Xaftadagi dars soatlari	
Majburiy	Uzbek/rus	6	
Fanning nomi	Auditoriya mashg'ulotlari (soat)	Mustaqil ta'lim (soat)	Jami yuklama (soat)
1. Kiberxavfsizlik asoslari	72	108	180

2. **1. Fanning mazmuni.**  
**Fanni o'qitishdan maqsad** – Kiberxavfsizlik asoslari fani kasbiy faoliyatida axborot tizimlari va axborot resurslarining axborot xavfsizligini ta'minlash bo'yicha masalalarni yechishda bilim, ko'nikma va malaka shakllantirishdan iborat. Respublikamizda axborot texnologiyalarining rivojlanishi bilan bir qatorda xo'jalik va davlat boshqaruvi organlarida axborot xavfsizligini, xususan, kompyuter bilan bog'liq bo'lgan xavfsizlik muammolarini bartaraf etish yo'nalishiga alohida e'tibor qaratilmoqda.
- Fanning vazifasi** – talabalarga kiberxavfsizlikning asosiy tizimlari bilan tanishtirish va kriptografiya asoslari, foydalanishni nazoratlash, tarmoq va kompyuter xavfsizligini ta'minlashning hamda axborot xavfsizligini ta'minlashga oid dasturlar yaratish, mavjudlarini takomillashtirish. Axborotni ishlab, uzatish va ta'limning zamonaviy usullarining rivojlanishi foydalanuvchilar axborotini yo'qolishi, buzilishi va oshkor etilishi bilan bog'liq tahdidlarning ortishiga olib kelmogda. Shu sababli, kompyuter tizimlari va tarmoqlarida axborot xavfsizligini ta'minlash axborot texnologiyalari rivojining yetakchi yo'nalishlaridan biri hisoblanadi.

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

### II.1 Fan tarkibiga quyidagi mavzular kiradi:

#### Asosiy nazariy qism (ma'ruza mashg'ulotlari)

##### 1- Mavzu. Kiberxavfsizlik asoslari.

Sertifikatlangan axborot tizimlari xavfsizligi bo'yicha mutaxassis (CISSP) tamoyillari asosida kiberxavfsizlik asoslarini yaratishning asosiy tushunchalari, kirishni boshqarish, telekommunikatsiya va tarmoq xavfsizligi, xavflarni boshqarish, dasturiy ta'minotni ishlab chiqish xavfsizligi tushunchasi, tizimini tahlillashga yaxlitli yondashuv kabi tushunchalarni tavsiflaydi.

##### 2- Mavzu. Kiberxavfsizlik arxitekturasini, strategiyasi va siyosati

Kiberxavfsizlik arxitekturasini va strategiyasi. Kiberxavfsizlik arxitekturasini jarayonlarni, inson rolini, texnologiyalarni va turli xil axborotni tavsiflaydi, hamda zamonaviy korxonaning murakkabligini va o'zgaruvchanligini hisobga oladi. Kiberxavfsizlikning arxitekturasini tashkilotning va u bilan bog'liq boshqa komponentlar va interfeyslarning istalgan axborot xavfsizligi tizimi xolatini tavsiflaydi.

### 3- Mavzu. Kriptografiyaning asosiy tushunchasi

Kriptografiyaning asosiy tushunchalari. Ochiq kalitli kriptotizimlar. Shifrlash / deshifrlash; shifrlarga xujumlarning turkumlanishi; simmetrik va assimetrik kriptografiya, kriptografiyaning tarixi, klassik shifrlar, bir martalik bloknot, stenografiya

### 4- Mavzu. Simmetrik kriptografik algoritmlar.

Simmetrik kriptografik algoritmlar. Haqiqiy ma'nosini inson tushunmaydigan belgilar ko'rinishiga o'kazish. Blokli shifrlash, oqimli shifrlash qo'llanilishi. Blokli shifrlash (Block Cipher). Ma'lumot bloklarga bo'linadi (masalan, har biri 128 bit). Har bir blok alohida shifrlanadi. Disklarni va fayllarni shifrlash.

### 5- Mavzu. Assimetrik shifrlar

Tushuncha, namuna, qo'llanilishi assimetrik shifrlash tizimlari hamda ularning matematik asoslari. Assimetrik shifrlash — bu kriptografik tizim bo'lib, u ikkita kalitdan foydalanadi: Ochiq kalit (public key) — hamma bilan baham ko'riladi. Yopiq kalit (private key) — faqat egasida bo'ladi va maxfiy saqlanadi.

### 6- Mavzu. HACs – ACES – kiberxavfsizlik

ACES dasturida ishlash. UNIX operatsion tizimi bilan hamkorlikda ishlash. Cybergiene (kibergigiena) and Cyber-Ethics (kiberaxloq) texnologiyalari bo'yicha kiberxavfsizlikning turli jihatlarini o'rganadilar va amalda qo'llash.

### 7- Mavzu. Ko'p sathli xavfsizlik modellari

Ko'p sathli xavfsizlikning (multilevel security, MLC) modellari. Bell-LaPadul modeli. Biba modeli. Lug'at bo'yicha hujum, kombinatsiyalarni to'liq ko'rib chiqish, fishing va ijtimoiy injineriya, zararkunanda kod, oflayn tahlil, parollarni buzish vositalari, kriptografik xesh – funksiyalar turlari.

### 8- Mavzu. Ma'lumotlarning fizik xavfsizligi

Ma'lumotlarni fizik himoyalash. Ma'lumotlarning ishlab markazining xavfsizligi, foydalanish kaliti, odamlarning xarakatlanishi, foydalanish kartasi va videokuzatuv. Bu serverlar, kompyuterlar, saqlash qurilmalari, kabellar va texnik inshootlar singari real, jismoniy infratuzilmani himoya qilish.

### 9- mavzu. Tarmoq xavfsizligi

Kompyuter tarmoqlarining asosiy tushunchalari. Tarmoq xavfsizligi muammolari. Tarmoq xavfsizligini ta'minlovchi vositalar. Kompyuter tarmoqlari resurslarini almashish maqsadida bir necha kompyuterlarning birlashuvidan iborat. Fayllar, dasturlar, printerlar, modemlar va har qanday tarmoq uskunasini birlashtirishda foydalaniluvchi yoki taqsimlanuvchi resurslar bo'lishi mumkin.

### 10- mavzu. Foydalanuvchanlikni ta'minlash usullari

Foydalanuvchanlik tushunchasi va zaxira nusxalash. Ma'lumotlarni zaxiralash texnologiyalari va usullari. Ma'lumotlarni qayta tiklash va hodisalarni qaydlash. Ma'lumotlarning turkumlanishi; himoya domenlari, ACL, C-list. Guruhli siyosat, parol. Parollar va guruh siyosati (Group policy) Har bir foydalanuvchi guruhga tegishli bo'lishi. (Admin, User, Guest) Guruhlar uchun alohida huquq siyosati.

### 11- mavzu. Simsiz tarmoqlarning xavfsizligi.

Simsiz tarmoq turlari. Simsiz tarmoqlarning asosiy xarakteristikalar. Asosiy tushunchalar, topologiyalari, TCP/IP modeli. Simsiz tarmoqlarda axborot



xavfsizligiga tahdid va zaifliklar, turkumlanishi, qarshi choralar. Tarmoqdan foydalanishning yolg'on nuqtalari (zararli egizak hujumi).

## 12- mavzu. Qarorlar qabul qilishda axloqiy tamoyillarni kiberxavfsizlikda qo'llash.

Axbortga tahdidlar, hujumlar, imtiyozlar, kirishni boshqarish parollarini boshqarish, xavfsizlik siyosati, muhim boshqaruvlar va hodisalarni boshqarish. Hujumga uchrashi mumkin bo'lgan soha maydonini minimallashtirish. Xavfsiz standart sozlamalarini o'rnatish.

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

Amaliy mashg'ulotlar uchun quyidagi mavzular tavsiya etiladi:

1. Axborot xavfsizligining timsollari(Bob, Alisa, Tridi)
2. Axborot xavfsizligini ta'minlash darajalari (huquqiy, tashkiliy, texnik)
3. Korxona arxitekturasini va uning boshqa arxitekturalar bilan bog'liqligi
4. Kiberxavfsizlik arxitekturasini
5. Hozirda kriptografiya doirasida yechiladigan masalalar.
6. Rasshifrovlash va deshifrlash algoritmlari.
7. Simmetrik kriptografik algoritmlar.
8. Blokli shifrlash va oqimli shifrlash.
9. Assimmetrik shifrlash usullari va ularning qo'llanilishi.
10. Ochiq va yopiq kalit.
11. Identifikatsiya, autentifikatsiya va avtorizatsiya.
12. Kriptografik qurilmalar.Biometrik autentifikatsiya
13. Bell-LaPadul modeli.
14. Bfba modeli.
15. Ma'lumotlarni ishlash markazining xavfsizligi. Foydalanish kaliti.
16. Odamlarning xarakatlanishi, foydalanish kartasi va videokuzatuv.
17. Himoya domenlari, ACL, C-list. Guruhli siyosat.
18. Apparatlari va dasturiy shifrlash, afzalliklari va kamchiliklari.
19. Yuqori foydalanuvchanlikni uch omili.
20. Ma'lumotlarni zaxira nusxalash.
21. Simsiz tarmoq turlari.
22. Simsiz tarmoqlarda tahdid va zaifliklar.
23. Dasturiy vositalar xavfsizligi.
24. Kompyuter viruslari va virusdan himoyalani.

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

### IV. Mustaqil ta'lim va mustaqil ishlar

Mustaqil ta'limni baholash - bu talabalarining jamoaviy tartibda yakka tartibda berilgan amaliy loyihalarni bajarishlari orqali amalga oshiriladi. Bunda har bir talabaga bitta jamoaviy loyiha va ikkita tartibda bajariladigan loyiha

beriladi. Talaba berilgan loyihaing maqsad va vazifalarini, mohiyatini tushungan holda qo'yilgan vazifani o'rganib izlanishlar olib boradi. Olingan natijalarni tahlil qilib, hulosalari bilan taqdimotlar tayyorlab himoya qiladi. Ishchi fan dasturida loyihalarning soni, mavzusi, mazmuni bajarish usullari va topshirish muddatlari tuluq ochib beriladi.

### Mustaqil ta'lim uchun tavsiya etiladigan mavzular

1. Kiberhujumlarning asosiy turlari va ularning ko'rinishlari.
2. Tarmoqlararo himoya devorlarining (firewalls) asosiy turlari va ishlash prinsiplari.
3. VPN (Virtual Private Network) texnologiyasining xavfsizlik jihatlari va foydalanish usullari
4. O'chirilgan ma'lumotlarni tiklash usullari kiberxavfsizlikda uning ahamiyati.
5. Kiberxavfsizlikda inson omilining roli va ijtimoiy injiniring usullari.
6. Ma'lumot bazalarining xavfsizligi; zaifliklar va himoya choralarlari
7. Web –sayt xavfsizligi; Cross-site scripting (XSS) xujumlari va himoya choralarlari
8. Zero-day hujumlari; kiberxavfsizlikdagi xavf va javob choralarlari.
9. Kompyuter viruslari va trojanlar; turlari, tarixi va qarshi choralar.
10. Kiberjinoyatchilikga qarshi xalqaro qonunchilik.
11. Zararkunanda dasturlarning asosiy turlari va ularni aniqlash usullari.
12. Blockchain texnologiyasining kiberxavfsizlikdagi o'rni.
13. Kiberxavfsizlikda mashinaviy o'rganish (machine learning) va su'niy intellektning roli.
14. Sim kartalarning klonlanishi va mobil qurilmalarning xavfsizligi.
15. Ma'lumotlarning zaxira nusxalarini yaratish va tiklash texnologiyalari.
16. Cloud Computing xavfsizligi; tarmoq xavfsizligi, malumotlarning zaifliklari
17. Phishing hujumlari; usullari va foydalanuvchilarni himoya qilish choralarlari.
18. Internet-of-Things (IoT) qurilmalarining xavfsizligi.
19. Kiberjinoyatlarning iqtisodiy zararlari va tahlili.
20. Kiberxujumlarga javob berish va xavfsizlikni tiklash rejalarlari.
21. USB qurilmalari orqali kiberxujumlar va ularning oldini olish choralarlari.
22. Simsiz tarmoqlar uchun WPA3 protokolining xavfsizlik yaxshilanishlari.
23. Kiberxavfsizlikda ommaviy ma'lumotlarning himoyasi.
24. Kiberxavfsizlikda blockchain va kriptografik tokenlarning ishlatilishi

### V. Fan o'qitilishining natijalari (shakllanadigan kompetensiyalar)

“Kiberxavfsizlik asoslari” fanining tushunchasi, kategoriyasi va asosiy prinsiplarini xavf - xatarlarni aniqlash va baholash, axborot tizimlari va tarmoqlarga tahdid soluvchi potentsial xavf –xatarlarni aniqlash va ularni baholash bo'yicha ko'nikmalarga ega bo'ladi. Himoya choralarini qo'llash; Axborot xavfsizligini ta'minlash uchun zarur bo'lgan himoya choralarini qo'llash shu jumladan xavfsizlik siyosatlarini ishlab chiqish va amalga oshirish. Kriptografik usullarni qo'llash haqida tasavvurga ega bo'lish;(bilim)

Ma'lumotlarni himoyalash uchun kriptografik usullarni qo'llash va ularni samarali



boshqarish kunikmalarini o'zlashtiradi. Hujumlarni aniqlash va ularga qarshi choralar ko'rish: Xavfsizlik tizimlarida xujumlarni aniqlash, ularga qarshi choralar ko'rish va himoya mexanizmlarini sinovdan o'tkazish imkoniyatiga ega bo'ladi. Qonunchilik va axborot xavfsizligi siyosatlar: Kiber xavfsizlik sohasidagi qonunchilik, standartlar va siyosatlar tushunish hamda ularga rioya qilish. Voqealar monitoring va tahlili: Axborot xavfsizligi voqealarini kuzatish, tahlil qilish va ularga javob berish imkoniyatidan foydalana olish; (ko'nikma) Xavfsizlik tahlili va auditi: Axborot tizimlari xavfsizligini muntazam ravishda baholash va audit o'tkazish. Etik xakerlik (penetration testing): Tizim va tarmoqlarning himoya darajasini tekshirish uchun etik xakerlik usullaridan foydalanish. Inson omili va ijtimoiy muhandislik: Ijtimoiy muhandislik hujumlariga qarshi turish uchun inson omili va xavfsizlikka oid choralarini tushinish. Xavfsizlikka oid hodisalar haqida xabar berish va ularni boshqarish: Xavfsizlikka oid hodisalar va tahdidlar haqida tezkorlik bilan xabar berish hamda ularga javob berish tartiblari haqida **malakalariga ega bo'lishi kerak.**

#### VI. 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

#### VII. 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 va tushunchalar haqida mustaqil mushohada yuritish, joriy va oraliq nazorat shakllarida berilgan vazifa va topshiriqlarni bajarish, yakuniy nazorat bo'yicha variantlar asosida yozma topshiriqlarni bajarishni zarur.

#### VIII. Asosiy adabiyotlar

1. S.K.Ganiyev, A.A.Ganiyev, Z.T. Xudoyqulov. Kiberxavfsizlik asoslari, o'quv qo'llanma, 2020 yil. Elektron.
2. Хилл Б. "Полный спровочник по Cisco" Пер. с англ. М. Изд. Дом Вильямс. 2008 г.
3. S.K. Ganiyev, M.M. Karimov, K.A. Tashayev. Axborot xavfsizligi. "Toshkent" darslik. 2017-yil. Elektron.
4. Rick Howard. Cybersecurity First Principles. Пер. с англ. Питер. 2024.

#### IX. Qo'shimcha adabiyotlar

1. "Axborot texnologiyasi. Axborotlarni kriptografik muhofazasi. Ma'lumotlarni shifrlash algoritmi". O'zbekiston Davlat standarti. O'zDSt 11.05.2009
2. Jurayev G.U., Aliyev R.H., Muxamadiyev F.R. Kompyuter tarmoqlari

xavfsizligi. Axborot xavfsizligi, o'quv qo'llanma, Innovatsiya-Ziyo. 2022-yil.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М. Издательства ТРИУМФ, 2003 г. -816.
4. Mirziyoyev SH.M. Buyuk kelajagimizni mard va olijanob xalqimiz bilan birga quramiz. T.: "O'zbekiston" NMIU, 2017. 488 b.
5. ЭМэйволд. Безопасность сетей. Москва. 2021. 570 стр.
6. Д. У. Хаббард. Как оценить риски в кибербезопасности. Лучшие инструменты и практики. «Эксмо», 2023.
7. Магама Базаров. Сети глазами хакера. Санкт-Петербург. 2025. 226 с.
8. М.Ховард. Д.Лебланк. Защищенный код. Пер. с англ. — 2-е изд., испр. — М.: Издательство «Русская Редакция», 2005. — 698 стр.
9. А. А. Афанасьев, Л. Т. Веденев, А. А. Воронцов и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. М.: Горячая линия—Телеком, 2009. — 552 с.

#### Axborot manbalari

1. www.lib.espi.uz
2. www.denemetr.com
3. www.security.uz
4. www.uzinfocom.uz
5. www.unilibary.uz
6. https://dox.utdallas.edu/sy154463?utm\_source=chatgpt.com
7. https://academiccatalog.umd.edu/undergraduate/approved-courses/hacs/?utm\_source=chatgpt.com
8. https://uwex.wisconsin.edu/cybersecurity/wp-content/uploads/sites/2/2021/01/CYB700.pdf?utm\_source=chatgpt.com

7. Fan dasturi Toshkent davlat agrar universiteti Kengashining 2025 yil "04" 07 dagi "13" – sonli bayoni bilan ma'qullangan.

#### Fan/modul uchun mas'ullar:

Noraliyev N.X. - "Axborot tizimlari va texnologiyalari" kafedrası professori, f-m.f.n

Qilichov N.M. - "Axborot tizimlari va texnologiyalari" kafedrası katta o'qituvchisi.

#### Taqrizchilar:

Xayitboyev K. – "Axborot tizimlari va texnologiyalari" kafedrası dotsenti  
Jumanazarov S.S. – "Axborot tizimlari va texnologiyalari" kafedrası dotsenti



**Mazkur o'quv dasturi dunyoning e'tirof etilgan xalqaro QS va THE reytinglarida nufuzli TOP-300 talikka kirgan quyidagi oliy ta'lim tashkilotlarining ta'lim dasturlari asosida ishlab chiqilgan.**

<b>№</b>	<b>OTM nomi</b>	<b>QS</b>	<b>THE</b>	<b>TOP-300 ta'lim dasturi asosida kiritilgan qo'shimcha mavzular</b>	<b>Mazkur dastur dastur dastur nomi</b>	<b>Havolalar</b>
1	University of Texas at Dallas	297	251	(The course provides an overview of building and breaking the fundamentals of cyber security based on the principles behind the coveted Certified Information Systems Security Professional (CISSP). Topics include access controls, telecommunications and network security, risk management, software development security, cryptography, security architecture and design, operations security, business continuity, regulations, investigations, forensics, compliance, physical security, and emerging technologies).	1-mavzu. Kiberxav fizik asoslari	<a href="https://dox.utdallas.edu/syl54463?utm_source=chatgpt.com">https://dox.utdallas.edu/syl54463?utm_source=chatgpt.com</a>
2	University of Maryland	218	112	Interdisciplinary foundational course of the ACES program. Through lectures, lab activities, and discussions, students will learn and practice various aspects of cybersecurity. Weekly technical lectures will introduce students to the operating system UNIX. Students will partner with the Division of Information Technology in a project to engage the University of Maryland community in a cyber-hygiene and cyber-ethics campaign based on the concepts learned in class.	6-mavzu. HACs – ACES – kiberxav fizik	<a href="https://academic.catalog.umd.edu/undergraduate/approved-courses/hacs/?utm_source=chatgpt.com">https://academic.catalog.umd.edu/undergraduate/approved-courses/hacs/?utm_source=chatgpt.com</a>
3	University of Wisconsin	116	56	This course introduces fundamental concepts and design principles in cybersecurity. Students will understand what, why, and how to protect in the cyberworld. Topics include CIA (Confidentiality, Integrity, and Availability), threats, attacks, defense, least privilege, access control and password management, security policies, critical controls, incident-handling and contingency planning, risk assessment and management.	Qarorlar qabul qilishda axloqiy tamoyillarni kiberxav fizikda qo'llash	<a href="https://uwex.wiscconsin.edu/cybersecurity/wp-content/uploads/sites/2/2021/01/CYB700.pdf?utm_source=chatgpt.com">https://uwex.wiscconsin.edu/cybersecurity/wp-content/uploads/sites/2/2021/01/CYB700.pdf?utm_source=chatgpt.com</a>

<https://europe.gatech.edu/sites/default/files/01/C%2036000%2035%20labov.pdf>

<https://www.umd.edu/courses/6-034-artificial-intelligence/2005/pages/cylibov/>