

O'ZBEKISTON RESPUBLIKASI
OLIIY TA'LIM, FAN VA INNOVATSIYALAR VAZIRLIGI
TOSHKENT DAVLAT AGRAR UNIVERSITETI



AXBOROT XAVF
FSIZLIGI
O'QUV DASTURI

Bilim sohasi:	300 000	- Ijtimoiy fanlar
Ta'lim sohasi:	310 000	- Ijtimoiy va humanitar, jurnalistika va axborot
Ta'lim yo'nalishi:	60310500	- Raqamli iqtisodiyot (tarmoqlar va

Toshkent - 1025

Fan/modul kodi AXEX3M3406	O'quv yili 2025-2026	Semestr 7-8	ECTS - Kreditlar 4-4
Fan/modul turi Majburiy	Ta'lim tili O'zbek	Haftadagi dars soatlari 4-4	
1.	Fanning nomi	Auditoriya mashg'ulotlari (soat)	Jami yuklama (soat)
	Axborot xavfsizligi	96	144
2.	<p>I. Fanning mazmuni</p> <p>Fanni o'qitishdan maqsad – talabalarga axborot xavfsizligidan nazariy uslubiy va texnologik asoslarini, sohaga oid aniq masalalarni yechishda axborot texnologiyalarini qo'llashning amaliy yutuqlari va uslublari bilan chuqur haq tomonlama tanishtirish hamda ishlab chiqarishni konstruktorlik-texnologiyaviy tayyorlash bosqichlarini optimallashtirish asosida ma'lumotlarga ishlov berish usullari va algoritmlarini ishlab chiqarish va ularni integrallashgan axborot-tahlil tizimini ta'minlab beruvchi ishlab chiqarish jarayonlarini avtomatlashtirish va boshqarish masalalarini yechishda amaliy qo'llashdan iborat.</p> <p>Fanning vazifasi - talabalarni nazariy bilimlar, amaliy ko'nikmalar, axborot texnologiyalari bilan bog'liq jarayonlarga uslubiy yondashuv hamda ilmiy texnikaviy dunyoqarashini yanada shakllantirishdan iboratdir.</p> <p>II. Asosiy nazariy qism (ma'ruza mashg'ulotlari)</p> <p>II.I. Fan tarkibiga quyidagi mavzular kiradi:</p> <p>Asosiy nazariy qism (ma'ruza mashg'ulotlari)</p> <p>1-mavzu. Axborot xavfsizligi tushunchasi va xavfsizlik masalalari</p> <p>Axborot xavfsizligiga kirish. Milliy xavfsizlik tushunchasi. Axborot xavfsizligini ta'minlashning asosiy vazifalari va darajalari. Xavfsizlik siyosati. Axborot xavfsizligi arxitekturasini va strategiyasi.</p> <p>2-mavzu. Axborot xavfsizligiga bo'ladigan tahdidlar, hujumlar va zaifliklar</p> <p>Axborot xavfsizligiga tahdidlar va ularning tahlili. Axborot xavfsizligining zaifliklari. Axborotning maxfiyligini, yaxlitligini va foydalanuvchanligini buzish usullari. Bo'lishi mumkin bo'lgan tahdidlarni oldini olish.</p> <p>3-mavzu. Axborot xavfsizligi sohasiga oid xalqaro va milliy me'yoriy-huquqiy baza</p>		

Axborot xavfsizligi sohasiga oid xalqaro standartlar. Axborot xavfsizligi sohasiga oid 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 tarmoqlarida xavfsizlik modellari, Bell va La-Padula modeli, Denning modeli, Landver modeli. Xarrison-Ruzzo-Ulmanning diskretion modeli. Bell-Lapadulaning mandati (muxtor huquqli) modeli. Xavfsizlikning rolli modeli.

5-mavzu. Axborotlarni texnik, tashkiliy va dasturiy himoyalashni tashkil etish ta'moyillari

Axborotni himoyalash tizimlari, Funktsional xavfsizlik darajalari, Axborotlarni himoyalashning dasturiy texnik vositalari, Xavfsizlik tizimlarini qurish usullari.

6-mavzu. Axborotni himoyalash usullari, Identifikatsiya va autentifikatsiya

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.

7-mavzu. Identifikatsiya kartalari va elektron kalitlar

Identifikatsiya kartalari va elektron kalitlar. Umumiy ma'lumot. Magnit chiziqli kartalar. Smart kartalar va USB kalitlarga murojaat qiling. Kontaktsiz RFID kartalari.

8-mavzu. Kriptografik himoyalash usullari

Asosiy atamalar va ta'riflar. Kriptotizimlarga qo'yiladigan asosiy talablar. Kriptografik tizimlarning tasnifi. Shifrlash, deshifrlash. Shifrlarning sinflanishi. Kriptografiyaning asosiy qoidalar va ta'riflari. Shifrlash usullarining turkumlanishi, simmetrik (maxfiy) va asimmetrik (ochiq) kalitli shifrlash tizimlari, almashtirish (podstanovka) usullarining mohiyati.

9-mavzu. Tarmoq xavfsizligi

Computer tarmoqi 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 tarmoqlar xavfsizligi protokollari. Simsiz qurilmalar xavfsizligi muammolari.

10-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.

11-mavzu. Kompyuter viruslari va ulardan himoyalash mexanizmlari

Kompyuter virusining ta'riflari. Viruslarni asosiy alomatlari 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 choralari.

12-mavzu. Virtual himoyalangan tarmoqlar

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

13-mavzu. Foydalanuvchanlikni ta'minlash usullari

Foydalanuvchanlik tushunchasi va zahira nusxalash. Ma'lumotlarni zahiralash texnologiyalari va usullari. Ma'lumotlarni qayta tiklash va hodisalarni qayd etish.

14-mavzu. Elektron tijorat va onlayn to'lovlar xavfsizligi

Elektron savdo platformalarining xavfsizligi. Onlayn to'lov tizimlari va kredit karta ma'lumotlarini himoyalash. Internet banking xavfsizligi. Elektron imzo va raqamli sertifikatlar.

15-mavzu. Mobil qurilmalar va ilovalar xavfsizligi

Smartphone va planshetlar xavfsizligi. Mobil ilovalarning asosiy xavfsizlik muammolari. Mobil qurilmalarni himoyalash usullari. BYOD (shaxsiy qurilmalardan foydalanish) siyosati.

16-mavzu. Bulutli xizmatlar xavfsizligi

Cloud computing asoslari. Bulutli xizmatlarning xavfsizlik muammolari. Ma'lumotlarni bulutda xavfsiz saqlash. Bulutli xizmat provayderlari bilan ishlash qoidalar.

17-mavzu. Ijtimoiy tarmoqlar va shaxsiy ma'lumotlar xavfsizligi

Ijtimoiy tarmoqlardagi xavfsizlik risklari. Shaxsiy ma'lumotlarni himoyalash. Phishing va ijtimoiy muhandislik hujumlari. Onlayn shaxsiy hayot va maxfiylik.

18-mavzu. Elektron hukumat va raqamli xizmatlar xavfsizligi

E-government tizimlarining xavfsizligi. Raqamli xizmatlar va fuqarolar ma'lumotlarini himoyalash. Elektron hujjat aylanishi xavfsizligi. Raqamli imzo qonunchilik asoslari.

19-mavzu. Kichik biznes va tadbirkorlik xavfsizligi

Kichik korxonalar uchun axborot xavfsizligi. Oddiy va arzon himoya usullari. Xodimlarni o'qitish va xavfsizlik madaniyati. Biznes ma'lumotlarini himoyalash.

20-mavzu. Smart qurilmalar va IoT asoslari

Aqlli uy tizimlari xavfsizligi. Internet orqali ulangan qurilmalar (IoT) ning asosiy xavfsizlik muammolari. Smart qurilmalarni xavfsiz sozlash. Aqlli shahar tizimlarining xavfsizligi.

21-mavzu. Ma'lumotlar maxfiyligi va huquqiy himoya

Shaxsiy ma'lumotlar himoyasi qonunlari. GDPR va O'zbekistondagi ma'lumotlar himoyasi qonunlari. Ma'lumotlar subjektlarining huquqlari. Ma'lumotlarni qayta ishlash qoidalar.

22-mavzu. Kiberhujumlar va ulardan himoyalash

Zamonaviy kiberhujumlar turlari. Ransomware va ulardan himoyalash. DDoS hujumlari va himoya usullari. Kiberjinoyatchilik va huquqiy javobgarlik.

23-mavzu. Axborot xavfsizligi bo'yicha kasbiy faoliyat

Axborot xavfsizligi mutaxassisligi. Kasbiy sertifikatlar va malaka oshirish. Axborot xavfsizligi bo'yicha konsalting faoliyati. Freelance va o'z biznesini boshlash.

24-mavzu. Kelajakdagi texnologiyalar va xavfsizlik tendensiyalari

Raqamli texnologiyalarning rivojlanish yo'nalishlari. Sun'iy intellekt va xavfsizlik. Kelajakdagi xavfsizlik chora-tadbirlari. Raqamli transformatsiya va xavfsizlik.

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

Amaliy mashg'ulotlari uchun tavsiya etilayotgan mavzular:

1-amaliy. Tashkilot uchun xavfsizlik siyosati yaratish

Oddiy xavfsizlik qoidalarini ishlab chiqish. Xodimlar uchun yo'riqnoma tayyorlash.

2-amaliy. Kompyuter tizimidagi zaifliklarni aniqlash

Asosiy xavfsizlik tekshiruvlari. Parollar kuchini tekshirish. Dasturiy ta'minot yangilanishlarini nazorat qilish.

3-amaliy. Axborot xavfsizligi standartlari bilan tanishish O'zbekiston va xalqaro standartlarni o'rganish. Tashkilotda standartlarni qo'llash.
4-amaliy. Foydalanuvchilar huquqlarini boshqarish User account yaratish va boshqarish. Parol siyosatini o'rnatish. Foydalanuvchi guruhlarini tashkil etish.
5-amaliy. Antivirus va firewall o'rnatish Bepul antivirus dasturlarini o'rnatish va sozlash. Windows Defender bilan ishlash. Oddiy firewall sozlamalari.
6-amaliy. Ikki faktorli autentifikatsiya o'rnatish Google Authenticator va boshqa 2FA ilovalarini o'rnatish. Email va SMS orqali autentifikatsiya.
7-amaliy. USB kalitlar va smart kartalar bilan ishlash USB token yaratish va foydalanish. Oddiy smart karta operatsiyalari.
8-amaliy. Fayllarni shifrlash va himoyalash WinRAR va 7-Zip bilan parolli arxivlar yaratish. BitLocker yoki VeraCrypt bilan disk shifrlash.
9-amaliy. Wi-Fi tarmoq xavfsizligini sozlash Xavfsiz Wi-Fi tarmoq yaratish. WPA3 protokolini sozlash. Tarmoq parollarini himoyalash.
10-amaliy. Router va modem xavfsizlik sozlamalari Router admin panelini himoyalash. Port forwarding va DMZ sozlamalari. Guest network yaratish.
11-amaliy. Kompyuterni viruslardan tozalash Malware Bytes va boshqa tozalash vositalari. Tizimni to'liq tekshirish va tozalash.
12-amaliy. VPN o'rnatish va foydalanish Bepul VPN xizmatlarini sinash. OpenVPN mijoz sozlamalari. VPN orqali xavfsiz internet.
13-amaliy. Ma'lumotlarni zahiralash va qayta tiklash Google Drive, Dropbox bilan ishlash. Local backup yaratish. Ma'lumotlarni qayta tiklash.
14-amaliy. Onlayn xaridlar xavfsizligi Xavfsiz onlayn xarid qilish qoidalarini. To'lov ma'lumotlarini himoyalash. Iribgarlik saytlarini aniqlash.

15-amaliy. Mobil ilovalar xavfsizligini tekshirish Xavfli mobil ilovalarni aniqlash. App store'dan xavfsiz yuklash. Mobil qurilma sozlamalari.
16-amaliy. Bulutli xizmatlar bilan xavfsiz ishlash Google Drive, iCloud xavfsizlik sozlamalari. Fayllarni bulutda xavfsiz almashish.
17-amaliy. Ijtimoiy tarmoqlarda xavfsizlik Facebook, Instagram, Telegram xavfsizlik sozlamalari. Shaxsiy ma'lumotlarni himoyalash.
18-amaliy. Elektron hukumat xizmatlaridan xavfsiz foydalanish my.gov.uz va boshqa davlat saytlarida xavfsiz ishlash. Elektron raqamli imzo olish.
19-amaliy. Kichik ofis xavfsizligini tashkil etish 5-10 kompyuterli tarmoq xavfsizligi. Oddiy server sozlamalari. Printer va boshqa qurilmalar xavfsizligi.
20-amaliy. Smart uy qurilmalarini xavfsiz sozlash Smart TV, kamera va boshqa IoT qurilmalar sozlamalari. Uy tarmoqini segmentlash.
21-amaliy. Shaxsiy ma'lumotlar huquqlari GDPR talablari bo'yicha o'z huquqlarini amalga oshirish. Ma'lumotlar o'chirilishini so'rash.
22-amaliy. Phishing hujumlarini aniqlash Soxta email va SMS larni aniqlash. Link va fayllarni tekshirish usullari. Xavfsiz email amaliyoti.
23-amaliy. CV va portfolio tayyorlash Axborot xavfsizligi bo'yicha resume yozish. LinkedIn profilini yaratish. Intervyuga tayyorgarlik.
24-amaliy. Shaxsiy xavfsizlik rejasi yaratish O'z ma'lumotlari uchun xavfsizlik rejasi. Parollar menejerini sozlash. Muntazam backup va yangilanishlar rejasi.
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. Fanning tarkibiy tuzilishi:			
4.1 Ma'ruza mashg'ulotlari			
№	Mavzular	Ma'ruza mashg'ulotlar rejas 7-Semestr	Ma'ruza mashg'ulot lari soati
1	Axborot xavfsizligi tushunchasi va xavfsizlik masalalari	1. Axborot xavfsizligiga kirish va asosiy tushunchalar 2. Milliy xavfsizlik konsepsiyasi va axborot xavfsizligining o'rni 3. Axborot xavfsizligini ta'minlashning asosiy vazifalari va darajalari 4. Xavfsizlik siyosati va uning elementlari 5. Axborot xavfsizligi arxitekturasini va strategik yondashuvlar	2
2	Axborot xavfsizligiga bo'ladigan tahdidlar, hujumlar va zaifliklar	1. Axborot xavfsizligiga tahdidlar va ularning turlari 2. Ichki va tashqi tahdidlarning tahlili 3. Axborot xavfsizligining asosiy zaifliklari (maxfiylik, yaxlitlik, foydalanuvchanlik) 4. Tahdidlarni buzish usullari va hujum texnikalari 5. Tahdidlarni oldini olish va risk boshqaruvi	2
3	Axborot xavfsizligi sohasiga oid xalqaro va milliy me'yoriy-huquqiy baza	1. Axborot xavfsizligi sohasiga oid xalqaro standartlar (ISO/IEC 27001, NIST) 2. O'zbekiston Respublikasining axborot xavfsizligi bo'yicha qonunlari 3. Milliy standartlar va texnik reglamentlar	2

		4. Axborot xavfsizligi sohasiga oid normativ hujjatlar 5. Xalqaro hamkorlik va standartlarni tadbiq etish	
4	Axborot xavfsizligi siyosati va xavfsizlik modellari	1. Axborot xavfsizligini buzuvchining modeli va tasnifi 2. Buzuvchilar kategoriyalari (maqsad va usullarga bog'liq) 3. Bell va La-Padula xavfsizlik modeli 4. Denning va Landver modellari 5. Diskretion, mandatli va rolli xavfsizlik modellari	2
5	Axborotlarni texnik, tashkiliy va dasturiy himoyalashni tashkil etish tamoyillari	1. Axborotni himoyalash tizimlarining asoslari 2. Funktsional xavfsizlik darajalari va ularning tasnifi 3. Axborotlarni himoyalashning dasturiy-texnik vositalari 4. Himoya tizimlarini qurish usullari va arxitekturasini 5. Tashkiliy chora-tadbirlar va ularning samaradorligi	2
6.	Axborotni himoyalash usullari, identifikatsiya va autentifikatsiya	1. Identifikatsiya va autentifikatsiyaning asosiy tushunchalari 2. Foydalanuvchilarning haqiqiylikni aniqlash usullari 3. Avtorizatsiya va kirish huquqlarini boshqarish 4. Ma'lumotlarni uzatish kanallarida autentifikatsiya 5. Biometrik ma'lumotlardan foydalangan identifikatsiya/autentifikatsiya	2
7.	Identifikatsiya kartalari va elektron kalitlar	1. Identifikatsiya kartalari va elektron kalitlarning umumiy ma'lumoti	2

		2. Magnit chiziqli kartalar va ularning imkoniyatlari 3. Smart kartalar va USB kalitlarning afzalliklari 4. Kontaktsiz RFID kartalar texnologiyasi 5. Kartalar va kalitlarning xavfsizlik aspektlari	
8.	Kriptografik himoyalash usullari	1. Kriptografiyaning asosiy atamalar va ta'riflari 2. Kriptotizimlarga qo'yiladigan asosiy talablar 3. Shifrlash va deshifrlash jarayonlari 4. Simmetrik (maxfiy kalitli) shifrlash tizimlari 5. Asimmetrik (ochiq kalitli) shifrlash tizimlari va almashirish usullari	2
9	Tarmoq xavfsizligi	1. Kompyuter tarmoq'i tushunchasi va xavfsizlik muammolari 2. Tarmoq xavfsizligini ta'minlovchi vositalar 3. Simsiz tarmoqlar xavfsizligi va tuzilmasi 4. Simsiz shaxsiy, regional va global tarmoqlar 5. Simsiz tarmoqlar xavfsizligi protokollari va qurilmalar xavfsizligi	2
10	Kompyuter viruslari va ulardan himoyalash mexanizmlari	1. Tarmoqlararo ekranlarning ishlash tamoyillari 2. Ochiq tashqi va himoyalangan ichki tarmoq kontseptsiyasi 3. Tarmoqlararo ekranlarning asosiy komponentlari 4. Firewall asosidagi tarmoq himoyasining sxemalari 5. Yopiq va ochiq tarmoqlarni himoyalash strategiyalari	2

11.	Axborotni himoyalashda tarmoqlararo ekranlarning o'rni	1. Kompyuter virusining ta'riflari va asosiy xususiyatlari 2. Viruslarni yashash makoni bo'yicha turkumlash 3. Zarar keltiruvchi dasturlarning turlari (malware, trojan, worm) 4. Viruslar va zararli dasturlarni tarqatish kanallari 5. Antivirusli himoya va profilaktika choralar	2
12	Virtual himoyalangan tarmoqlar	1. Virtual himoyalangan tarmoqlarni qurish kontseptsiyasi 2. VPN (Virtual Private Network) ning asosiy tamoyillari 3. Himoyalangan virtual tarmoqlarni qurish variantlari 4. VPN turlarining tasnifi va qo'llanish sohalari 5. VPN xavfsizligi va konfiguratsiya masalalari	2
№	Mavzular	Ma'ruza mashg'ulotlar rejas	Ma'ruza mashg'ulotlari soati
13	Foydalanuvchanlikni ta'minlash usullari	8-Semestr 1. Foydalanuvchanlik (Availability) tushunchasi va ahamiyati 2. Ma'lumotlarni zahira nusxalash strategiyalari 3. Backup texnologiyalari va usullarining turlari 4. Ma'lumotlarni qayta tiklash jarayonlari 5. Hodisalarni qayd etish va monitoring tizimlari	2
14	Elektron tijorat va onlayn to'lovlar xavfsizligi	1. Elektron savdo platformalarining xavfsizlik talablari 2. Onlayn to'lov tizimlari va kredit karta ma'lumotlarini himoyalash	2

		3. Internet banking xavfsizligi va autentifikatsiya 4. Elektron imzo va raqamli sertifikatlar qo'llanilishi 5. E-commerce da fraud va uni oldini olish usullari	
15	Mobil qurilmalar va ilovalar xavfsizligi	1. Smartphone va planshetlar xavfsizligining o'ziga xos xususiyatlari 2. Mobil ilovalarning asosiy xavfsizlik muammolari 3. Mobil qurilmalarni himoyalash texnikalari va usullari 4. BYOD (Bring Your Own Device) siyosati va qoidalar 5. Mobil malware va ulardan himoyalalanish	2
16	Bulutli xizmatlar xavfsizligi	1. Cloud computing texnologiyalarining asoslari 2. Bulutli xizmatlarning asosiy xavfsizlik muammolari 3. Ma'lumotlarni bulutda xavfsiz saqlash tamoyillari 4. Bulutli xizmat provayderlar bilan ishlash qoidalar 5. Gibrilid va multi-cloud muhitlarida xavfsizlik	2
17	Ijtimoiy tarmoqlar va shaxsiy ma'lumotlar xavfsizligi	1. Ijtimoiy tarmoqlardagi xavfsizlik risklari va tahdidlar 2. Shaxsiy ma'lumotlarni himoyalash tamoyillari 3. Phishing va ijtimoiy muhandislik (social engineering) hujumlari 4. Onlayn maxfiylik va raqamli iz 5. Ijtimoiy tarmoqlarda xavfsiz foydalanish qoidalar	2
18	Elektron hukumat va raqamli	1. E-government tizimlarining xavfsizlik arxitekturasini	2

		2. Raqamli davlat xizmatlari va fuqarolar ma'lumotlarini himoyalash 3. Elektron hujjat aylanishi va uning xavfsizligi 4. Raqamli imzo qonunchiligining asoslari 5. Davlat ma'lumotlari bazalari va ularning himoyasi	
19	Kichik biznes va tadbirkorlik xavfsizligi	1. Kichik korxonalar uchun axborot xavfsizligining ahamiyati 2. Oddiy va arzon himoya usullarini amalga oshirish 3. Xodimlarni o'qitish va xavfsizlik madaniyatini shakllantirish 4. Biznes ma'lumotlarini himoyalash strategiyalari 5. SMB (Small and Medium Business) uchun xavfsizlik yechimlari	2
20	Smart qurilmalar va IoT asoslari	1. Internet of Things (IoT) va smart qurilmalar kontseptsiyasi 2. Aqlli uy tizimlari va ularning xavfsizlik masalalari 3. IoT qurilmalarning asosiy xavfsizlik zaifliklari 4. Smart qurilmalarni xavfsiz sozlash va boshqarish 5. Aqlli shahar tizimlarining xavfsizligi va kelajak istiqbollari	2
21	Ma'lumotlar maxfiyligi va huquqiy himoya	1. Shaxsiy ma'lumotlar himoyasi qonunlarining asoslari 2. GDPR (General Data Protection Regulation) talablari 3. O'zbekistondagi ma'lumotlar himoyasi qonunchiligi	2

		4. Ma'lumotlar subjektlarining huquqlari va majburiyatlari 5. Ma'lumotlarni qayta ishlash qoidalari va consent mexanizmi	
22	Kiberhujumlar va ulardan himoyalaniish	1. Zamonaviy kiberhujumlarning turlari va tendensiyalari 2. Ransomware (shifrlash viruslari) va ulardan himoyalaniish 3. DDoS hujumlari va ularga qarshi himoya usullari 4. Advanced Persistent Threats (APT) va targeted attacks 5. Kiberjinoyatchilik va huquqiy javobgarlik masalalari	2
23	Axborot xavfsizligi bo'yicha kasbiy faoliyat	1. Axborot xavfsizligi mutaxassisligi va kasbiy yo'nalishlar 2. Kasbiy sertifikatlar va malaka oshirish dasturlari 3. Axborot xavfsizligi bo'yicha konsalting faoliyati 4. Freelance va mustaqil faoliyat imkoniyatlari 5. O'z biznesini boshlash va startup loyihalari	2
24	Kelajakdagi texnologiyalar va xavfsizlik tendensiyalari	1. Raqamli texnologiyalarning rivojlanish yo'nalishlari 2. Sun'iy intellekt va mashina o'rganishining xavfsizlik aspektlari 3. Quantum computing va post-quantum kriptografiya 4. Blockchain texnologiyasi va uning xavfsizlik qo'llanishlari 5. Raqamli transformatsiya va kelajakdagi xavfsizlik chora-tadbirlari	2
	Jami:		48

№	Mavzular	Amaliy mashg'ulotlar Rejasi 7-Semestr	Amaliy mashg'ulotlari soati
1	Tashkilot uchun xavfsizlik siyosati yaratish	1. Tashkilot xavfsizlik ehtiyojlarini baholash va tahlil qilish 2. Oddiy va tushunarli xavfsizlik qoidalarini ishlab chiqish 3. Xodimlar uchun yo'riqnomalar va ko'rsatmalar tayyorlash 4. Xavfsizlik siyosatini hujjatlash va rasmiylashtirish 5. Siyosatni amalga oshirish va monitoring jarayonini tashkil etish	2
2	Kompyuter tizimidagi zaifliklarni aniqlash	1. Tizimdagi asosiy xavfsizlik zaifliklarini aniqlash usullari 2. Parollar mustahkamligini tekshirish va baholash 3. Dasturiy ta'minot yangilanishlarini nazorat qilish jarayoni 4. Vulnerability scanning vositalari bilan ishlash 5. Aniqlangan zaifliklarni bartaraf etish rejasi tuzish	2
3	Axborot xavfsizligi standartlari bilan tanishish	1. O'zbekiston milliy standartlari bilan tanishish va tahlil 2. ISO/IEC 27001 va boshqa xalqaro standartlarni o'rganish 3. Standartlar talablarini tashkilotda qo'llash usullari 4. Compliance (standartlarga muvofiqlik) ni baholash	2

		5. Standartlar bo'yicha hujjatlar va jarayonlarni ishlab chiqish	
4	Foydalanuvchilar huquqlarini boshqarish	1. Windows muhitida user account yaratish va boshqarish 2. Kuchli parol siyosatini o'rnatish va sozlash 3. Foydalanuvchi guruhlarini tashkil etish va huquqlar berish 4. Role-based access control (RBAC) ni amalga oshirish 5. Kirish huquqlarini audit qilish va monitoring	2
5	Antivirus va firewall o'rnatish	1. Bepul antivirusli dasturlarni (Avast, AVG) o'rnatish va sozlash 2. Windows Defender bilan ishlash va konfiguratsiyalash 3. Windows Firewall va uchinchi tomon firewall sozlamalari 4. Real-time himoya va scheduled scanning o'rnatish 5. Antivirusli himoyaning samaradorligini tekshirish	2
6.	Ikki faktorli autentifikatsiya o'rnatish	1. Google Authenticator ilovasini o'rnatish va sozlash 2. SMS va email orqali ikki faktorli autentifikatsiya 3. Microsoft Authenticator va boshqa 2FA ilovalar bilan ishlash 4. Backup kodlar yaratish va xavfsiz saqlash 5. Turli xizmatlar uchun 2FA ni yoqish (Google, Microsoft, Facebook)	2
7.	USB kalitlar va smart kartalar bilan ishlash	1. USB token yaratish va konfiguratsiyalash 2. VeraCrypt yordamida shifrlangan USB yaratish	2

		3. Smart karta o'quvchi qurilma bilan ishlash 4. Sertifikatlarni smart kartaga o'rnatish va boshqarish 5. USB va smart kartalar orqali secure login o'rnatish	
8.	Fayllarni shifrlash va himoyalash	1. WinRAR va 7-Zip yordamida parolli arxivlar yaratish 2. BitLocker orqali hard disk bo'limlarini shifrlash 3. VeraCrypt bilan konteyner va disk shifrlash 4. Individual fayllarni shifrlash (GPG, AES Crypt) 5. Shifrlab saqlangan ma'lumotlarni xavfsiz almashish	2
9	Wi-Fi tarmoq xavfsizligini sozlash	1. Xavfsiz Wi-Fi tarmoq yaratish va konfiguratsiyalash 2. WPA3 protokolini o'rnatish va sozlash 3. Tarmoq parollarini kuchli qilish va himoyalash 4. MAC address filtering va hidden SSID sozlamalari 5. Wi-Fi tarmoqni monitoring va xavfli qurilmalarni aniqlash	2
10	Router va modem xavfsizlik sozlamalari	1. Router admin panelini himoyalash (parol, IP restriction) 2. Firmware yangilanishlarini tekshirish va o'rnatish 3. Port forwarding va DMZ sozlamalarini xavfsiz qilish 4. Guest network yaratish va konfiguratsiyalash 5. UPnP va boshqa xavfli xizmatlarni o'chirish	2
11.	Kompyuterni viruslardan tozalash	1. Malwarebytes Anti-Malware o'rnatish va ishlatish	2

		2. AdwCleaner bilan reklama dasturlarini tozalash 3. Hijackthis va RootkitRevealer kabi maxsus vositalar 4. Tizimni offline antivirus bilan tekshirish (Rescue disk) 5. Tozalashdan keyin tizimni mustahkamlash va himoyalash	
12	VPN o'rnatish va foydalanish	1. Bepul VPN xizmatlarini (ProtonVPN, Windscribe) sinash 2. OpenVPN mijoz dasturini o'rnatish va sozlash 3. VPN serverga ulanish va connection testi 4. VPN orqali xavfsiz internet foydalanish qoidalarini 5. VPN performance va privacy settings ni optimallashtirish	2
№	Mavzular	Amaliy mashg'ulotlar Rejasi 8-Semestr	Amaliy mashg'ulotlari soati
13	Ma'lumotlarni zahiralash va qayta tiklash	1. Google Drive va Dropbox bilan sinxronizatsiya o'rnatish 2. Local backup yaratish (external HDD, DVD) 3. File History va System Restore sozlamalari 4. Backup schedule yaratish va automation 5. Ma'lumotlarni qayta tiklash jarayonini amalda sinash	2
14	Onlayn xaridlar xavfsizligi	1. Xavfsiz onlayn xarid qilish qoidalarini va best practices 2. SSL sertifikat va HTTPS ni tekshirish usullari 3. To'lov ma'lumotlarini himoyalash va virtual kartalar	2

		4. Firqabgarlik saytlarini aniqlash va phishing belgilari 5. Onlayn xarid uchun secure browser va payment methods	
15	Mobil ilovalar xavfsizligini tekshirish	1. Android va iOS da xavfli ilovalarni aniqlash usullari 2. App store'dan xavfsiz yuklab olish qoidalarini 3. Mobil qurilma privacy va security sozlamalari 4. Malicious apps ni aniqlash va o'chirish 5. Mobile antivirus va security apps o'rnatish	2
16	Bulutli xizmatlar bilan xavfsiz ishlash	1. Google Drive xavfsizlik va privacy sozlamalari 2. iCloud, OneDrive va Dropbox da encryption 3. Two-factor authentication bulutli xizmatlar uchun 4. Fayllarni bulutda xavfsiz almashish (password protection) 5. Bulutli xizmatlar uchun access control va sharing permissions	2
17	Ijtimoiy tarmoqlarda xavfsizlik	1. Facebook privacy va security sozlamalarini optimallashtirish 2. Instagram da personal information va location sharing 3. Telegram da secure messaging va encryption 4. Social media da phishing va scam dan himoyalash 5. Digital footprint ni minimallashtirish usullari	2
18	Elektron hukumat xizmatlaridan xavfsiz foydalanish	1. my.gov.uz portalida xavfsiz ro'yxatdan o'tish va ishlash 2. Davlat xizmatlarida secure login va 2FA	2

	3. Elektron raqamli imzo (ERI) olish jarayoni 4. E-government services da shaxsiy ma'lumotlarni himoyalash 5. Davlat portallari da fraud va phishing dan ehtiyot bo'lish	
19	Kichik ofis xavfsizligini tashkil etish 1. 5-10 kompyuterli tarmoq xavfsizligini rejalash 2. Oddiy server (Windows Server) ni xavfsiz sozlash 3. Printer, scanner va boshqa shared devices xavfsizligi 4. Network access control va user management 5. Backup strategy va disaster recovery planning	2
20	Smart uy qurilmalarini xavfsiz sozlash 1. Smart TV da privacy settings va firmware updates 2. IP kamera va smart doorbell xavfsizligi 3. Smart home hub (Alexa, Google Home) privacy sozlamalari 4. IoT qurilmalar uchun alohida tarmoq segmenti yaratish 5. Smart devices monitoring va firmware yangilanishlari	2
21	Shaxsiy ma'lumotlar huquqlari 1. GDPR talablari bo'yicha o'z huquqlarini o'rganish 2. Kompaniyalardan ma'lumotlar o'chirilishini so'rash (Data erasure) 3. Data portability huquqini amalga oshirish 4. Consent management va opting out jarayonlari	2

	5. Privacy policy larni tushunish va tahlil qilish	
22	Phishing hujumlarini aniqlash 1. Soxta email va SMS larni aniqlash belgilari 2. Suspicious links va attachments ni tekshirish usullari 3. URL shorteners va domain spoofing dan ehtiyot bo'lish 4. Phishing simulation va awareness training 5. Email clients da anti-phishing filters sozlash	2
23	CV va portfolio tayyorlash 1. Axborot xavfsizligi mutaxassisi uchun professional resume yozish 2. LinkedIn profilini cybersecurity career uchun optimizing 3. Technical skills va certifications ni to'g'ri ko'rsatish 4. Portfolio loyihalari va case studies tayyorlash 5. Interview jarayoniga tayyorgarlik va technical questions	2
24	Shaxsiy xavfsizlik rejasi yaratish 1. Shaxsiy digital assets va threats assessment 2. Password manager (LastPass, 1Password) sozlash va ishlatish 3. Muntazam backup schedule va testing jarayoni 4. Software updates va security patches rejasi 5. Personal cybersecurity checklist va monthly review jarayoni	2
	Jami:	48

<p>IV. Mustaqil ta'lim va mustaqil ishlar</p> <p>Mustaqil ta'lim uchun tavsiya etiladigan mavzular:</p> <ol style="list-style-type: none"> 1. Axborot xavfsizligining asosiy tushunchalari va tamoyillari 2. Raqamli iqtisodiyotda axborot xavfsizligining o'rni va ahamiyati 3. Kiberxavfsizlik va uning iqtisodiy ta'siri 4. Axborot aktivlarini tasniflash va baholash 5. Xavf va zaifliklar tahlili metodologiyasi 6. Axborot xavfsizligi siyosati va strategiyalari 7. Risk-menejmenti va axborot xavfsizligi 8. Konfidensiallik, yaxlitlik va mavjudlik (CIA) modeli 9. Axborot xavfsizligi bo'yicha huquqiy asoslar 10. Milliy va xalqaro standartlar (ISO 27001/27002) 11. Kriptografiya asoslari va raqamli iqtisodiyotda qo'llanilishi 12. Elektron raqamli imzo va uning iqtisodiy ahamiyati 13. Tarmoq xavfsizligi va himoya vositalari 14. Firewall va intruzion aniqlash tizimlari 15. Antivirusli himiya va zararli dasturlar 16. Veb-ilovalar xavfsizligi 17. Ma'lumotlar bazasi xavfsizligi 18. Bulut xizmatlarida axborot xavfsizligi 19. Mobil qurilmalar va ilovalar xavfsizligi 20. IoT qurilmalari xavfsizligi masalalari 21. Axborot xavfsizligi boshqaruv tizimlari (ISMS) 22. Incidentlarga javob berish va tiklanish rejalar 23. Axborot xavfsizligi auditlari va nazorat 24. Xodimlarni o'qitish va axborot xavfsizligi madaniyati 25. Biznes-jarayonlarda axborot xavfsizligi 26. Uchinchi tomon xizmat ko'rsatuvchilari bilan ishlash 27. Ma'lumotlarni zaxiralash va tiklanish strategiyalari 28. Fizik xavfsizlik choralari 29. Axborot xavfsizligi ko'rsatkichlari va monitoring 30. Compliance va regulativ talablar 31. Elektron tijorat va to'lov tizimlari xavfsizligi 32. Blockchain texnologiyasi va kriptovalyutalar xavfsizligi 33. Sun'iy intellekt va mashinali o'rganish xavfsizligi 34. Ijtimoiy muhandislik va psixologik hujumlar 35. Kiberterrorizm va kiberurushlar 36. Raqamli iqtisodiyotda axborot xavfsizligining istiqbolari 	
---	--

3.	<p>V. Fan o'qitilishining natijalari (shakllantirilgan kompetensiyalar)</p> <p>Fanni o'zlashtirish natijasida talaba:</p> <ul style="list-style-type: none"> • Axborot xavfsizligi fanining o'rni 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 axborotlarini 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;
4.	<p>VI. Ta'lim texnologiyalari va metodlari:</p> <ul style="list-style-type: none"> • ma'ruzalar; • interfaol keys-stadilar; • (mantiqiy fiklash, tezkor savol-javoblar); • guruhlarda ishlash; • taqdimotlarni qilish; • individual loyihalar; <p>jamoa bo'lib ishlash va himoya qilish uchun loyihalar</p>
5.	<p>VIII. Kreditlarni olish uchun talablar:</p> <p>Baholash:</p> <p>Fanning yakuniy bahosi uchta yo'nalishdagi baholarga asoslanadi:</p> <p>(1) Dars mashg'ulotlariga tayyorgarlik va faol ishtirok etish (15%).</p> <p>Dars jarayonida muntazam ishtirok etishdan tashqari, talabalar darslar boshlanishidan oldin onlayn o'quv materiallari bilan tanishgan bo'lishlari talab etiladi. Har bir talabdan ma'ruza va amaliy mashg'ulotlarda faol ishtirok etish talab qilinadi.</p> <p>(2) Auditoriyadagi mashg'ulotlar (15%)</p>

Har bir ma'ruza va amaliyot mashg'ulot bo'yicha topshiriqlar keying dars mashg'ulotiga qadar bajarilib topshirilishi lozim. Ma'ruza va amaliy mashg'ulotlarida berilgan topshiriqlarni bajarish (30%).

(3) Yakuniy baholash (40%) (Baholash turi, vaqti, baholash mezonlari)

Fan bo'yicha talabalarining bilim saviyasi va o'zlashtirish darajasining Davlat ta'lim standartlariga muvofiqligini ta'minlash uchun quyidagi nazorat turlari o'tkaziladi:

Joriy nazorat (JN) – o'quv semestr davomida dasturining amaliy, laboratoriya, seminar mashg'ulotlari bo'yicha talabalarining bilim va ko'nikmalarini o'zlashtirish darajasi 5 baholik tizim orqali baholanadi.

Oraliq nazorat (ON) – o'quv semestr davomida dasturining tegishli fanlarning bir necha mavzularini o'z ichiga olgan bo'limi tugallangandan keyin talabaning nazariy bilim va amaliy ko'nikma darajasini aniqlash va baholash usuli. Oraliq nazorat bir semestrda bir, ikkimarta o'tkaziladi va shakli (yozma, og'zaki, test va hokazo) o'quv faniga ajratilgan umumiy soatlar hajmidan kelib chiqqan holda belgilanadi;

Yakuniy nazorat (YaN) – semestr yakunida muayyan fan bo'yicha nazariy bilim va amaliy ko'nikmalarni talabalar tomonidan o'zlashtirish darajasini baholash usuli. Yakuniy nazorat asosan tayanch so'z va iboralarga asoslangan yozma, og'zaki, test va h.k. shakllarda o'tkaziladi.

Yakuniy nazorat turini o'tkazish va mazkur nazorat turi buyicha talabaning bilimni baholash o'quv mashg'ulotlarini olib bormagan professor-o'qituvchi tomonidan amalga oshiriladi.

Tegishli fan buyicha o'quv mashg'ulotlarini olib borgan professor-o'qituvchi yakuniy nazorat turini o'tkazishda ishtirok etishi taqiqlanadi.

Yakuniy nazorat turini o'tkazishda kelishuv asosida boshqa oliy ta'lim muassasalarining tegishli fan buyicha professor-o'qituvchilari jalb qilinishi mumkin.

Oliy ta'lim muassasasida yakuniy nazorat turlarini o'tkazilishi Ta'lim sifatini nazorat qilish bo'limi tomonidan doimiy ravishda o'rganib boriladi. Bunda nazorat turlarini o'tkazilish tartibi buzilganligi aniqlangan hollarda, o'tkazilgan nazorat turlarining natijalari bekor qilinishi hamda tegishli yakuniy nazorat turi qaytadan o'tkazilishi mumkin.

Talabaning bilim saviyasi, ko'nikma va malakalarini nazorat qilishning baho mezonini asosida talabaning fan bo'yicha o'zlashtirish darajasi 5 baholik tizim orqali ifodalanadi.

Talaba mustaqil xulosa va qarorlar qabul qila olsa, ijodiy fikrlab, mustaqil mushohada yuritisa, olgan bilimni amalda qullay oladi, fanning (mavzuning)

mohiyatini tushunadi, biladi, ifodalay oladi, aytib beradi xamda fan (mavzu) buyicha tasavvurga ega deb topilganda- 5(a'lo) baho bilan baholanadi.

Talaba mustaqil mushohada yuritadi, olgan bilimni amalda qo'llay oladi, fanning (mavzuning) mohiyatini tushunadi, biladi, ifodalay oladi, aytib beradi hamda fan (mavzu) buyicha tasavvurga ega deb topilganda

- 4(yaxshi) baho baholanadi.

Talaba olgan bilimni amalda qullay oladi, fanning (mavzuning) mohiyatini tushunadi, biladi, ifodalay oladi, aytib beradi xamda fan (mavzu) buyicha tasavvurga ega deb topilganda - 3(qoniqarli) baho baholanadi.

Talaba fan dasturini o'zlashtirmagan, fanning (mavzuning) mohiyatini tushunmaydi hamda fan (mavzu) buyicha tasavvurga ega emas deb topilganda - 2(qoniqarsiz) baho bilan baxolanadi.

Joriy nazorat va oraliq nazorat turini o'tkazish va mazkur nazorat turi buyicha talabaning bilimni baxolash tegishli fan buyicha o'quv mashg'ulotlarini olib borgan professor-o'qituvchi tomonidan amalga oshiriladi.

Talabaning amaliy, seminar, laboratoriya mashg'ulotlari va mustaqil ta'lim topshiriqlarini bajarishi, shuningdek uning ushbu mashg'ulotlardagi faolligi fan o'qituvchisi tomonidan baholab boriladi.

Talabani oraliq nazorat turi bo'yicha baholashda, uning o'quv mashg'ulotlari davomida olgan baholari inobatga olinadi.

JN, ON va YaN turlari kalendar tematik reja muvofiq dekanat tomonidan tuzilgan baholash nazorat jadvallari asosida o'tkaziladi.

Talaba uzli sabablarga ko'ra oraliq va (yoki) yakuniy nazorat turiga kirmagan taqdirda ushbu talabaga tegishli nazorat turini qayta topshirishga fakultet dekanining farmoyishi asosida ruxsat beriladi.

Joriy nazorat va oraliq nazorat turini topshirmagan, shuningdek ushbu nazorat turi buyicha "2"(qoniqarsiz) baho bilan baholangan talaba yakuniy nazorat turiga kiritilmaydi.

Yakuniy nazorat turiga kirmagan yoki kiritilmagan, shuningdek ushbu nazorat turi buyicha "2"(qoniqarsiz) baho bilan baholangan talaba akademik qarzdor hisoblanadi.

Talaba baholash natijasidan norozi bulgan taqdirda, baholash natijasi e'lon qilingan vaktidan boshlab 24 soat davomida apellyasiya berishi mumkin. Talaba tomonidan berilgan Apellyasiya komissiyasi tomonidan 2 kun ichida ko'rib chiqilishi lozim.

Talabaning apellyasiyasini ko'rib chiqishda talaba ishtirok etish huquqiga ega. Apellyasiya komissiyasi talabaning apellyasiyasini ko'rib chiqib, uning

yil "4" iyul dagi "13" – sonli bayoni bilan ma'qullangan.	
8. Fan/modul uchun ma'sullar: Noraliyev N.X. - "Axborot tizimlari va texnologiyalari" kafedrası professorı, f-m.f.n	
9. Taqrızchılar: Xayıtboyev K. - "Axborot tizimlari va texnologiyalari" kafedrası dotsenti Dauletov A.Yu - Al - Xarazmiy nomidagi Toshkent Axborot texnologiyalar universiteti dotsenti	

<p>natijasi buyicha tegishli qaror qabul qiladi. Qarorda talabani tegishli fanni o'zlashtirgani yoki o'zlashtira olmaganı ko'rsatiladi.</p> <p>Apellyasiya komissiyasi tegishli qarorni fakultet dekani va talabaga yetkazilishini ta'minlaydi.</p> <p>Yakuniy nazoratda "Yozma ish"larni baholash mezonı</p> <p>Yakuniy nazorat turi semestr yakunida tegishli fan bo'yicha talabani nazariy bilim va amaliy ko'nikmalarini o'zlashtirish darajasini aniqlash maqsadida amalga oshiriladi. (Yakuniy nazoratni yozma, og'zaki, test va boshqa usullarda olish mumkin.)</p>	
<p>6. Asosiy adabiyotlar</p> <ol style="list-style-type: none"> 1. G'aniev S. K., Karimov M. M., Tashev K. A. "Axborot xavfsizligi", "Fan va texnologiyalar" nashriyoti, Toshkent 2016 2. Mark Stamp. Information security. Principles and Practice. Second edition. A John Wiley & Sons, Inc., publication. Printed in the United States of America. 2011y. 584p. 3. Shagin V.F. «Informatsionnaya bezopasnost' i zashita informatsii», Uchebnoe posobie. M.: 2014 g. <p>Qo'shimcha adabiyotlar</p> <ol style="list-style-type: none"> 1. Mirziyoev Sh.M. Qonun ustuvorligi va inson manfaatlarini ta'minlash-yurt taraqqiyoti va xalq farovonligining garovi. 2017. 2. T.L. Partka, I.I. Popov. Informatsionnaya bezopasnost' . 4-e izdanie. Moskva «Forum», 2011 g. 3. "Axborot texnologiyasi. Axborotlarni kriptografik muxofazasi. Ma'lumotlarni shifrlash algoritmi" O'zbekiston Davlat standarti. O'zDSt 1105:2009. 4. Shnayer B. Prikladnaya kriptografiya. Protokoly, algoritmy, isxodnye tekсты na yazyke Si.- M.: Izdatel'stvo TRIUMF, 2003 – 816 <p>Internet saytlari</p> <ol style="list-style-type: none"> 1. http://www.ziyounet.uz 2. http://uz.denemetr.com/download/docs-229149/768-229149.doc 3. http://www.nasa.gov/statistics/ 4. http://www.security.uz 5. http://www.cert.uz 6. http://www.uzinfocom.uz 	
7. Fan dasturi Toshkent davlat agrar universiteti Ilmiy Kengashining 2025	