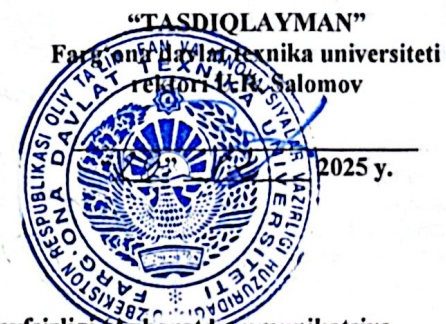


**O'ZBEKISTON RESPUBLIKASI
OLIIY TA'LIM, FAN VA INNOVATSIYALAR VAZIRLIGI
FARG'ONA DAVLAT TEXNIKA UNIVERSITETI**



**60610300 – Axborot xavfsizligi (Axborot kommunikatsiya
texnologiyalari va servis)
Yakuniy Davlat Attestatsiya sinovlaridan o'tkazish bo'yicha**

(mutaxassislik fanlaridan va bitiruv malakaviy ishi)

BAHOLASH MEZONLARI

Farg'ona – 2025 y.

Ushbu dastur 60610300 – Axborot xavfsizligi (Axborot kommunikatsiya texnologiyalari va servis) bakalavr ta'lim yo'nalishining 2022-2023 o'quv yilida tasdiqlangan o'quv rejasidagi ixtisoslik fanlar asosida tuzilgan.

Tuzuvchilar

O.V.Porubay		- "Dasturiy injiniring va kiberxavfsizlik" kafedrası mudiri
M.Turdimatov		- "Dasturiy injiniring va kiberxavfsizlik" kafedrası dotsenti
Sh.G'aniyeva		- "Dasturiy injiniring va kiberxavfsizlik" kafedrası v.b. dotsenti
M.Xusanova		- "Dasturiy injiniring va kiberxavfsizlik" kafedrası katta o'qituvchisi
X.Mamatova		- "Dasturiy injiniring va kiberxavfsizlik" kafedrası katta o'qituvchisi
J.Mirzayev		- "Dasturiy injiniring va kiberxavfsizlik" kafedrası katta o'qituvchisi
R.Raxmatov		- "Dasturiy injiniring va kiberxavfsizlik" kafedrası assistenti
X.Sadirova		- "Dasturiy injiniring va kiberxavfsizlik" kafedrası assistenti
O.Raxmonov		- "Dasturiy injiniring va kiberxavfsizlik" kafedrası assistenti
A.Umarov		- "Dasturiy injiniring va kiberxavfsizlik" kafedrası assistenti
A.Arabbayev		- "Dasturiy injiniring va kiberxavfsizlik" kafedrası assistenti

Ushbu dastur Axborot texnologiyalari va telekommunikatsiya fakultetining _____ dagi № _____-sonli yig'ilishida muhokama qilingan va tasdiqlashga avsiya etilgan.

KIRISH

60610300 – "Axborot xavfsizligi (Axborot kommunikatsiya texnologiyalari va servis)" ta'lim yo'nalishining asosiy vazifasi – axborot-kommunikatsiya texnologiyalari sohasida chuqur nazariy va amaliy bilimlarga ega, axborot xavfsizligini ta'minlash bo'yicha zamonaviy texnologiyalarni puxta o'zlashtirgan, raqobatbardosh, innovatsion fikrlovchi mutaxassislar tayyorlashdan iborat. Ushbu yo'nalish talabalarga axborotni himoya qilish usullari, kriptografiya, tarmoq xavfsizligi, operatsion tizimlar xavfsizligi, kompyuter tarmoqlari, dasturlash asoslari hamda sun'iy intellekt asosida xavfsizlikni ta'minlash sohalarida zamonaviy bilimlarni beradi. Ta'lim jarayoni orqali talabalar axborot xavfsizligi siyosati, risklarni baholash, tahdid va zaifliklarni aniqlash, hamda himoya vositalarini qo'llash bo'yicha chuqur bilimga ega bo'ladi.

Ta'lim yo'nalishining vazifasi – axborot xavfsizligi sohasida zamonaviy bilim va ko'nikmalarga ega, innovatsion fikrlovchi, raqobatbardosh mutaxassislarni tayyorlashdan iborat. Ushbu yo'nalish kriptografik tizimlar, tarmoq va tizimlar xavfsizligi, axborotlarni himoyalash texnologiyalari, risklarni boshqarish, kompyuter tarmoqlari hamda zamonaviy kiberxavfsizlik yechimlari bo'yicha chuqur nazariy va amaliy bilimlarni berishga qaratilgan. Talabalarda mustaqil fikrlash, tahdidlarni tahlil qilish, ularni oldini olish va bartaraf etish, hamda zamonaviy texnologiyalar asosida ilmiy-tadqiqot va amaliy loyihalar olib borish qobiliyatini shakllantirish asosiy maqsad qilib qo'yilgan.

60610300 – Axborot xavfsizligi ("Axborot kommunikatsiya texnologiyalari va servis") bakalavr ta'lim yo'nalishi bitiruvchi kurs uchun ixtisoslik fanlaridan o'tkaziladigan yakuniy davlat attestatsiyasi

DASTURI

60610300 – Axborot xavfsizligi (Axborot kommunikatsiya texnologiyalari va servis) ta'lim yo'nalishi bitiruvchi kurs talabalari uchun ixtisoslik fanlaridan o'tkaziladigan yakuniy davlat attestatsiyasi "Kriptografiya", "Kiberxavfsizlik siyosati", "Kiberhuquq-kiberetika", "Steganografik algoritmlar", "Tarmoq xavfsizligi" fanlaridan yozma ravishda o'tkazilishi belgilandi.

"Kriptografiya" fani bo'yicha

Fanni o'qitishdan maqsad - talabalarni axborot xavfsizligi sohasidagi asosiy tushunchalar, kriptografik algoritmlar, ma'lumotlarni shifrlash va autentifikatsiya qilish usullari bilan tanishtirish hamda ularni amaliyotda qo'llash ko'nikmalarini shakllantirishdir.

Fanning vazifasi - talabalarda kriptografiya fanini axborotni himoyalashdagi o'rni tushuntirish, shifrlarni va deshifrlash usullaridan foydalanilgan holda xavfsizlikni ta'minlash, kriptografik bilim, amaliy ko'nikma va tahliliy fikrlash qobiliyatini rivojlantirish, shuningdek, ularni real axborot xavfsizligi muammolarini yechishga tayyorlasdan iborat.

"Kiberxavfsizlik siyosati" fani bo'yicha

Fanni o'qitishdan maqsad - talabalarga kiberxavfsizlikni ta'minlash sohasidagi xalqaro va milliy me'yoriy, nazariy va amaliy izlanishlar natijalari bilan tanishtirish bilan bir qatorda kiberxavfsizlik siyosatini tashkil etishda foydalaniladigan turli

zamonaviy yondashuvlar, tashkiliy va huquqiy me'yorlarni qo'llashga doir bilimlar va ko'nikmalar hosil qilishdan iborat.

Fanning vazifasi - talabalarga axborot tizimlari va tarmoqlarda xavfsizlikni ta'minlash, xavf-xatarlarni boshqarish hamda tashkilot faoliyatini himoyalash uchun siyosiy-huquqiy, tashkiliy va texnik choralarni o'rgatishdan iborat.

"Kiberhuquq-kiberetika" fani bo'yicha

Fanni o'qitishdan maqsad - talabalarga kiberxavfsizlikni ta'minlash sohasidagi xalqaro va milliy me'yoriy, nazariy va amaliy izlanishlar natijalari bilan tanishtirish bilan bir qatorda axborot tizimlarini, resurslarni himoyalangan texnologiya asosida qurish, himoyalangan axborotga nisbatan bo'ladigan tahdidlarga zamonaviy yondashuvga asoslangan holda huquqiy tahlil qilishga doir bilimlar va o'quvlar hosil qilishdan iborat.

Fanning vazifasi - talabalarga nazariy bilimlar, amaliy ko'nikmalar hamda kibermakonda huquq normalariga va kiberetikaning qoidalariga rioya qilgan holda axborotni himoyalashning ahamiyatini ochib berish.

"Steganografik algoritmlar" fani bo'yicha

Fanni o'qitishdan maqsad - talabalar tomonidan steganografiyadan foydalanish xususiyatlarini va unga qo'yiladigan talablarni, stegotizimlarga hujumlar va ularga qarshi turish texnologiyalarini, steganografik tizimlarning bardoshligini baholash shuningdek, tasvirlar, video va audio signallarga ma'lumotlarni joylashtirish algoritmlari o'rganishdan iborat.

Fanning vazifasi - talabalarda steganografiya va uning kriptografiyadan farqini tushuntirish, steganografik tizimlarning ishlash prinsiplari, asosiy atamalar va modellari bilan tanishtirish, rasm, audio, video va matnli fayllarda ma'lumotni yashirish usullarini o'rgatish, steganografik dasturlar bilan ishlash ko'nikmalarini shakllantirish, maxfiy axborotni ruxsatsiz uchinchi tomonlardan yashirish usullarini ko'rsatish, steganoanaliz usullarini o'rganishi iborat.

"Tarmoq xavfsizligi" fani bo'yicha

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.

60610300 – Axborot xavfsizligi (Axborot kommunikatsiya texnologiyalari va servis) ta'lim yo'nalishi bitiruvchi kurs talabalari uchun "Kriptografiya", "Kiberxavfsizlik siyosati", "Kiberhuquq-kiberetika", "Steganografik algoritmlar", "Tarmoq xavfsizligi" fanlaridan o'tkaziladigan yakuniy davlat attestatsiyasi asosiy

SAVOLLARI

Kriptografiya fani bo'yicha

- 1. Kriptografiyada qo'llaniladigan matematik atama va tushunchalar.**
Tayanch iboralar: To'plamlar, akslantirishlar, binar amallar, to'plamlar ustida matematik amallar
- 2. Kriptografiyada modulyar arifmetikasi qo'llanishi va ahamiyati.**
Tayanch iboralar: Evklid algoritmi va kengaytirilgan Evklid algoritmi, modulyar arifmetika va uning xossalari, sonni modul bo'yicha teskarisini topish
- 3. Sonlarni tublikka tekshirish algoritmlari.**
Tayanch iboralar: Ehtimolikka asoslangan sonlarni tublikka tekshirish usullari. Aniqlashtirilgan sonlarni tublikka tekshirish usullari
- 4. Faktorizatsiyalash algoritmlari qo'llanishi va ahamiyati.**
Tayanch iboralar: Ferma usuli, Pollard usuli
- 5. Diskret logariflash muammosi va uning ahamiyati.**
Tayanch iboralar: Diskret logariflash algoritmlari, Diskret logariflash muammosiga qaratilgan hujumlar.
- 6. Klasik shifrlash usullari.**
Tayanch-iboralar: O'rni qo'yish, o'rin almashtirish usullari. Shifrlashning asosiy tushunchalari. Rotor mashinalari. Vigenere va vernam shifri.
- 7. Simmetrik blokli shifrlar.**
Tayanch-iboralar: Simmetrik shifrlar tasnifi. Blokli shifrlarni qurish usullari. Blokli shifrlarning parametrlari. DES shifrlash standarti.
- 8. Simmetrik oqimli shifrlar.**
Tayanch-iboralar: Pseudotasodifiy sonlar generatori. RC4 algoritmi. A5/1 algoritmi.
- 9. Zamonaviy blokli shifrlar.**
Tayanch-iboralar: 3DES, Blowfish shifrlash algoritmi, Camellia shifrlash algoritmi.
- 10. Ochiq kalitli kriptografiya.**
Tayanch-iboralar: Ochiq kalitli kriptografiyaning ishlash prinsipi. RSA algoritmi
- 11. Ochiq kalitli kriptografik algoritmlar.**

Tayanch-iboralar: El-Gamal algoritmi. Diffi-Xellman kalitlarni taqsimlash protokoli.

12. Xesh funksiyalar va ularning qo'llanilishi.

Tayanch-iboralar: xeshlash algoritmllari, SHA256, SHA512

13. Xesh funksiyalar va ma'lumotlarni autentifikatsiyalash.

Tayanch-iboralar: Autentifikatsiya talablari. Xabarlar autentifikatsiyalash kodi. Xesh funksiyalar va ularga qo'yiladigan talablar.

14. Elektron raqamli imzo.

Tayanch-iboralar: Raqamli imzo, ishlash prinsipi, DSA standarti.

15. Ochiq kalitlar infratuzilmasi.

Tayanch-iboralar: Ochiq kalitlarni ro'yxatga olish markazi. X.509 sertifikat.

16. Kriptografiyaning zamonaviy sohalari.

Tayanch-iboralar: Bulutli hisoblashda kriptografik algoritmldan foydalanish, kvant kriptografiyasi, yengil kriptografik algoritmlar.

17. GOST R 28147-89 blokli shifrlash algoritmi.

Tayanch-iboralar: Feystel tarmog'i, GOST R 28147-89 algoritmidan kalit generatori, S-blok.

18. Simmetrik va ochiq kalitli kriptografik tizimlarning ma'lumotlarni shifrlashdagi afzallik va kamchiliklari.

Tayanch-iboralar: simmetrik kriptografiya, asimmetrik kriptografiya.

19. Diffi-Xellman kalitlarni ochiq taqsimlash protokoli va uning xavfsizlik tahlili.

Tayanch-iboralar: kalit taqsimlash protokollari ishlash tartibi, maqsadi va vazifalari

20. AES shifrlash standarti.

Tayanch-iboralar: matematik asosi, shifrlash algoritmidan foydalanilgan akantirishlar, S-blok.

Kiberxavfsizlik siyosati fani bo'yicha

1. Kiberxavfsizlik evolyutsiyasi. Kiberxavfsizlik siyosati domenlari.

Domenlarga asoslangan xavfsizlik siyosati.
Tayanch so'zlar: Kiberxavfsizlik evolyutsiyasi, xavfsizlik domenlari, domenlarga asoslangan siyosat

2. Kiberxavfsizlik siyosatini amalga oshirish va rivojlantirish bosqichlari.

Tayanch so'zlar: Siyosatni joriy etish, rivojlantirish bosqichlari, monitoring

3. Xavfsizlik freymvorki tushunchasi. NIST Cybersecurity Framework ISO/IEC 27001/27002.

Tayanch so'zlar: Xavfsizlik freymvorki, NIST, ISO/IEC 27001, ISO/IEC 27002

4. Kiberxavfsizlik siyosati turlari va asosiy bo'limlari.

Tayanch so'zlar: Siyosat turlari, xavfsizlik bo'limlari, tashkiliy hujjatlar

5. Kiberboshqaruv tushunchasi. Kiberboshqaruvning davlat va xalqaro miqyosdagi roli.

Tayanch so'zlar: Kiberboshqaruv, davlat roli, xalqaro hamkorlik

6. Kiberxavfsizlik siyosatida AQSH, Rossiya va O'zbekiston yondashuvlari. Davlat siyosatining kiberxavfsizlikdagi o'rni.

Tayanch so'zlar: AQSH modeli, Rossiya modeli, O'zbekiston siyosati, davlat roli

7. Kiberxavfsizlik siyosatida Rossiya yondashuvlari (strategik hujjatlar, asosiy tamoyillar, amaliy choralar).

Tayanch so'zlar: Rossiya strategiyasi, tamoyillar, amaliy choralar

8. Kiberxavfsizlik siyosatida O'zbekiston yondashuvlari (strategik hujjatlar, asosiy tamoyillar, amaliy choralar).

Tayanch so'zlar: O'zbekiston strategiyasi, milliy xavfsizlik, siyosiy hujjatlar

9. Milliy kiberxavfsizlik agentliklarini tashkil etish va uni qo'llab-quvvatlash.

Tayanch so'zlar: Agentliklar, tashkil etish, qo'llab-quvvatlash

10. Milliy kiberxavfsizlik agentliklarini tashkil etish sabablari. Agentliklarning asosiy vazifalari.

Tayanch so'zlar: Tashkil etish sabablari, asosiy vazifalar, boshqaruv

11. Yuridik, jismoniy shaxslar va huquqni muhofaza qiluvchi organlarning kiberxavfsizlikni oldini olishdagi o'rni.

Tayanch so'zlar: Yuridik shaxslar, jismoniy shaxslar, huquqni muhofaza qilish

12. Kiberxavfsizlikni oldini olishda davlat, jamiyat va shaxsiy darajadagi rollar.

Tayanch so'zlar: Davlat roli, jamiyat, shaxsiy xavfsizlik

13. Tizimdan foydalanishni boshqarishdagi kibersiyosatlar.

Tayanch so'zlar: Foydalanishni boshqarish, ruxsatlar, autentifikatsiya

14. Ma'lumotlarni boshqarishdagi kibersiyosatlar (maxfiylik, yaxlitlik, mavjudlik).

Tayanch so'zlar: Maxfiylik, yaxlitlik, mavjudlik, CIA triadasi

15. Fizik xavfsizlikni ta'minlovchi texnik va tashkiliy vositalar.

Tayanch so'zlar: Fizik xavfsizlik, texnik vositalar, tashkiliy choralar

16. Internet va mobil qurilmalardan foydalanish siyosati (ruxsat etilgan foydalanish, kontent filtratsiyasi).

Tayanch so'zlar: Internet siyosati, mobil qurilmalar, filtratsiya

17. Ma'lumotlarni himoya qilish vositalari.

Tayanch so'zlar: Shifrlash, antivirus, himoya tizimlari

18. Tizim va foydalanuvchi darajasidagi vositalar.

Tayanch so'zlar: Tizim vositalari, foydalanuvchi vositalari, xavfsizlik darajalari

19. Raqamli kriminalistika vositalari.

Tayanch so'zlar: Digital forensika, tahlil vositalari, dalillar yig'ish

20. Kiberxavfsizlikda risklarni baholash va boshqarish jarayonlari.

Tayanch so'zlar: Risklarni baholash, risklarni boshqarish, tahdidlar, zaifliklar

Kiberhuquq-kiberetika fani bo'yicha

1. Kiberjinoyatchilik tushunchasi, kiberjinoyatchilik turlari.

Tayanch iboralar: kibermakon, kiberxavfsizlik, kiberjinoyat, tahdidlar, kiberjinoyat turlari, kiberjinoyat maqsadlari.

2. O'zbekistonda kiberxavfsizlikni ta'minlashning asosiy yo'nalishlari.

Tayanch iboralar: axborot, kiberxavfsizlik, me'yoriy hujjatlar, axborotga oid qonunlar.

3. Axborotni himoyalash usullari.

Tayanch iboralar: axborot, axborot himoyasi, axborot himoyalash usullari, dasturiy himoyalash, texnik himoyalash usuli, tashkiliy himoyalash usuli.

4. Kiberhuquq tushunchasi, kiberhuquq rivojlanish bosqichi.

Tayanch iboralar: axborot, kiberxavfsizlik, kiberhuquq, kiberhuquq rivojlanishi.

5. Axborot xavfsizligi sohasidagi subyektlar va obyektlar o'rtasidagi munosabatlarni tartibga soluvchi me'yoriy hujjatlar.

Tayanch iboralar: axborot, xavfsizlik, subyekt, obyekt, qonunlar, axborot xavfsizlikka oid me'yoriy hujjatlar.

6. Intelektual mulk tushunchasi, intellektual mulkni himoyalash.

Tayanch iboralar: intellektual mulk tushunchasi, Intellektual mulk huquqi, "Mualliflik huquqi va turdosh huquqlar to'g'risida"gi qonun, intellektual mulk sohasida davlat siyosati.

7. Kompyuter dasturlariga mualliflik huquqlari. Kompyuter dasturlari ro'yxatga olish.

Tayanch iboralar: axborot, kompyuter dasturi, mualliflik huquqi, intellektual mulk, dasturlarni ro'yxatga olish, intellektual mulk agentligi

8. Kiberxavfsizlikning ijtimoiy va etik jihatlari.

Tayanch iboralar: axborot, kiberxavfsizlik, etika, ijtimoiy jamiyat, kiberxavfsizlikni jamiyatga ta'siri, kiberxavfsizlikda etika masalalari

9. Kibermakonda axborot xavfsizligini ta'minlashda risk tushunchasi.

Tayanch iboralar: axborot, risk tushunchasi, risk darajalari, tahdid, zaiflik, risk omili, risk ta'siri, risk darajalari.

10. Konfidensial axborotning turlari va darajalari bo'yicha klassifikatsiyasi.

Tayanch iboralar: axborot, axborot xavfsizligi, konfidensial axborot, axborot turlari, axborot darajalari

11. Elektron resurs tushunchasi. Elektron resurslari kategoriyalari.

Tayanch iboralar: axborot, elektron resurs, elektron resurs turlari, elektron resurs kategoriyalari, elektron resurs qo'llanish sohalari.

12. Internet etikasining muhim masalalari.

Tayanch iboralar: axborot, internet, etika, internet afzalliklar, innernet kamchiliklari, internet etikasi, internet etikasi muammolari

13. Kibermajaro etikasining paydo bo'lishi va hozirda foydalanish omillari.

Tayanch iboralar: kiberxavfsizlik, kibermajaro, kiberurush, kiberqurol, kibermajaro sabablari, buzg'unchi, kiberhujum maqsadlari, kibermajaro etikasi

14. Yirik mamlakatlardagi mavjud kibermojarolar.

Tayanch iboralar: kiberxavfsizlik, kibermajaro, kiberurush, kiberqurol, kibermajaro sabablari, AQSHda kibermojarolar, Rossiyada kibermojarolar, Yevropada kibermojarolar

15. Davlat sirlari, tijorat sirlari, xizmat sirlar, kasbiy, shaxsiy sirlar muxofazasi.

Tayanch iboralar: Davlat siri, davlat sirlari turlari, tijorat sir, xizmat sir, kasbiy sir, shaxsiy, sirlarni himoyalashda me'yoriy hujjatlar.

16. Xujjatlarni maxfiylik darajasini belgilash va yuritish qoidalari.

Tayanch iboralar: axborot, ma'lumot, maxfiylik, xujjatlarda maxfiylik darajasi, maxfiylik yorliqlari, maxfiy hujjat egasi

17. Axborot urushining milliy xavfsizlikka tahdidi

Tayanch iboralar: axborot, axborot urushi, milliy xavfsizlik, tahdid, axborot urushiga misollar, axborot urushidan himoya

18. Kompyuter xavfsizligi bilan bog'liq ahloqiy muammolar: Hakerlik, haktivizm va konturhaking.

Tayanch iboralar: kompyuter xavfsizligi, kibermakon, haker, hakerlik, haktivizm, konturhaking, xavfsizlik hakerlari.

19. Zamonaviy kiberjinoyatlarning ko'rinishlari va ularni kelib chiqish sabablari

Tayanch iboralar: axborot, kibermakon, kiberxavfsizlik, kiberjinoyatchi, kiberjinoyat turlari, kiberjinoyat maqsadlari, kiberjinoyat sabablari, kiberjinoyatga qarshi kurash usullari.

20. Suniy intellekt va undagi kiber etika masalalari.

Tayanch iboralar: Sun'iy intellekt tushunchasi, sun'iy intellekt tizimi, sun'iy intellekt turlari va shakllari, Sun'iy intellektni meyoriy hujjatlashtirish, O'zbekistonda sun'iy intellekt rivojlanishi

Steganografik algoritmlar fani bo'yicha

1. Steganografiyada xabarni yashirishning klassik usullari.

Tayanch iboralar: stegonografiya tushunchasi, xabar yashirish usullari, niqoblash usuli, ko'rinmas siyoh usuli, mikronuqta, gazeta kodi

2. Stegonografik tizim umumiy sxemasi va vazifalari.

Tayanch iboralar: stegonografiya, aloqa kanali, xabar, konteyner, bo'sh konteyner, to'ldirilgan konteyner, stegonografik maydon, kalit.

3. Ma'lumot yashirish stegonografik sxemalari.

Tayanch iboralar: birinchi darajali himoya, ikkinchi darajali himoya, Uchinchi darajali himoya, to'rtinchi darajali himoya, xabar, kalit, konteyner, funksiya.

4. Stegonografik tizimlarga qarshi asosiy hujum turlari

Tayanch iboralar: Axborot xavfsizlik, butunlik, konfidentsiallik, konteyner, hujum, tahdid.

5. Raqamli stegonografiya: Asosiy usullar va qo'llanilishi

Tayanch iboralar: Raqamli stegonografiya, Raqamli suv belgilari, identifikatsiya raqamlari, Prekoder, Stegokoder, Stegodetektor, Dekoder

6. Raqamli suv belgilari (Digital Watermarking) va stegonografiya

Tayanch iboralar: Raqamli suv belgilar, Bardoshli belgi, Identifikatsiya raqami, Ko'r-ko'rona joylashtirish, Axborotni modulyatsiya qilish

7. Matnli hujjatlarda ma'lumotlarni yashirish.

Tayanch iboralar: matn, habar, Sintaktik usul, Orfografik usul, Semantik usul, Matn formatini o'zgartirish, Lingvistik usullar

8. Fotosurat va tasvirlarda ma'lumotni yashirish usullari..

Tayanch iboralar: raqamli tasvir, piksel, raqamli suv belgilari, stegokonteyner, Eng kam ahamiyatli bitni almashtirish usuli, tasvirlarning fazoviy sohasi

9. Ovozli signallarda ma'lumotni yashirish.

Tayanch iboralar: audio signal, absolyut faza, nisbiy faza, shovqin, akustika, chastota, amplituda, raqamli suv belgi, spektrni kengaytirish, signallarni kodlash

10. Video fayllarda stegonografiya.

Tayanch-iboralar: video, raqamli video formatlari, kadrlar (frames), piksel, dct (diskret kosinus transformatsiyasi), dwt (diskret to'lqin

transformatsiyasi), mpeg kodlash, fazoviy (spatial) soha, chastota (frequency) sohasi, video siqish

11. Web ilovalarda stegonografiya va uning qo'llanilishi

tayanch-iboralar: web sayti, web ilova, http/https, http protokoli, axborotni yashirish, cookie va metadata orqali yashirish, trafikni maskalash

12. Sun'iy intellekt va stegonografiya.

Tayanch-iboralar: suniy intellekt, sun'iy intellekt va stegonografiya, sun'iy neyron tarmoqlar, konvolyutsiyali neyron tarmoqlar, spektrli tasvir stegonografiyasi

13. Biometrik stegonografiya.

tayanch-iboralar: biometrik parameter, stegonografiya, axborot, xavfsizlik, axborot yashirish, eng kam ahamiyatli bit usuli, obyektga yo'naltirilgan yashirish.

14. Stegonografik tahlil usullari

Tayanch-iboralar: stegonografik tahlil, stegonografik tahlil usullari xususiyatlari, stegonografik tahlil usullari samaradorligini baholash, Kerkgofs prinsipi, stegotizim xavfsizligi.

15. Stegonografiya usullarini optimallashtirish.

Tayanch-iboralar: xabar, xabar xatoliklari, Stegonografiya optimallashtirish, yolg'ondan haqiqiy deb baholash, yolg'ondan rad etish, ta'sirchan model foydalanish.

16. Stegonografiya uchun dasturiy yechimlarni ishlab chiqish va sinovdan o'tkazish.

Tayanch-iboralar: Stegonografik dasturiy ta'minot, domen, ilovalar, dasturlash tili, fazoviy va chastotali domenlar, Kodlash va dekodlash, Testlash (testing)

17. Tarmoq stegonografiyasi usullar

Tayanch-iboralar: tarmoq, stegonografiya, yashirin kanal o'tkazuvchanligi, aniqlanish ehtimoli, stegonografik qiymat, trafik.

18. Biometrik stegonografiya tushunchasi va uning qo'llanilish sohasini izohlang.

Tayanch iboralar: Biometrik ma'lumotlar, barmoq izi, yuz aniqlash, identifikatsiya, xavfsizlik

19. Stegonografiyaning samaradorligini baholash mezonlarini tushuntiring.

Tayanch iboralar: PSNR, MSE, sifat baholash, aniqlik, signal/shovqin nisbati

20. Zamonaviy stegonografiya rivojlanish yo'nalishlari va istiqbollari haqida fikr yuritish.

Tayanch iboralar: Yangi texnologiyalar, sun'iy intellekt, xavfsizlik, innovatsiyalar, kelajak yo'nalishlari

Tarmoq xavfsizligi fani bo'yicha

1. Tarmoqda autentifikatsiya, avtorizatsiya va qayd etish tushunchalari.

Tayanch-iboralar: Autentifikatsiya (identity tekshirish), Avtorizatsiya (ruxsat berish), Accounting (qayd etish, log), Access control

2. RADIUS AAA protokoli uchun IETF-standarti. TACACS+ va uning qo'llanilishi. RADIUS va TACACS+ protokollarining asosiy imkoniyatlari.

Tayanch-iboralar: RADIUS (UDP, markazlashgan AAA), TACACS+, IETF standarti, AAA modeli, shifrlash, transport protokoli

3. Bulutli hisoblash tizimlari xizmatlaridan foydalanishda axborot xavfsizligi muammolari, bulutli hisoblash tizimi platformalari turlari, bulutli tizimlarda foydalanuvchilar ma'lumotlarining xavfsizligini ta'minlash.

Tayanch-iboralar: Cloud computing, IaaS, PaaS, SaaS, Ma'lumot maxfiyligi, Shifrlash (encryption).

4. Hujumlarni aniqlash tizimi. IDS/IPS texnologiyalari. IPS signaturasi. IPSni qo'llash.

Tayanch-iboralar: IDS (monitoring), IPS (active blocking), Signatura (pattern), Anomaly detection, Tarmoq hujumlari.

5. Himoyalangan virtual tarmoq texnologiyalari. IPsec VPN komponentalari.

Tayanch-iboralar: VPN (Virtual Private Network), IPsec (AH, ESP), Tunnel, transport mode, Encryption, authentication.

6. Axborotni himoyalashning tashkiliy-texnik usullari.

Tayanch-iboralar: Tashkiliy choralar, texnik vositalar, fizik himoya, siyosatlar (policy).

7. OSI modelining transport sathi imkoniyatlari va xususiyatlari. Transport sathi xavfsizlik protokollari.

Tayanch iboralar: TCP, UDP, End-to-end aloqa, Portlar, TLS, SSL

8. SSL/TLS va SOCKS protokollari va ularni tarmoq xavfsizligini ta'minlashdagi o'rni.

Tayanch-iboralar: SSL/TLS (shifrlash), HTTPS, SOCKS proxy, Secure communication

9. Kanal sathida himoyalangan kanallarni shakllantirish protokollari. PPTP, L2F va L2TP protokollari.

Tayanch-iboralar: Tunnel protokollari, VPN texnologiyasi, PPP asosida, L2TP + IPsec.

10. Ochiq tizimlar o'zaro ishlashining etalon modeli.

Tayanch-iboralar: 7 sath, Fizik → Ilova, Standart model

11. OSI va TCP/IP modellarining imkoniyatlari va protokollari

Tayanch-iboralar: TCP/IP (4 sath), OSI (7 sath), Protokollar: IP, TCP, HTTP

12. Xavfsizlik shlyuzlarini qo'llagan holda tarmoqlararo xavfsizlikni ta'minlash kommunikatsiyalari (O'z DSt ISO/IEC 27033).

Tayanch-iboralar: Firewall, Gateway, Filtrlash, ISO/IEC 27033

13. OSI modelining fizik sathida ma'lumotlarni himoyalash.

Tayanch-iboralar: Kabel himoyasi, Elektromagnit himoya, Fizik kirish nazorati.

14. OSI modelining kanal sathida ma'lumotlarni himoyalash.

Tayanch-iboralar: MAC adres, Switch xavfsizligi, VLAN, ARP spoofing

15. OSI modelining tarmoq sathida ma'lumotlarni himoyalash.

Tayanch-iboralar: IP xavfsizligi, IPsec, Routing, Paket filtrlash

16. OSI modelining transport sathida ma'lumotlarni himoyalash.

Tayanch-iboralar: TCP/UDP xavfsizlik, Port scanning, TLS

17. OSI modelining seans sathida ma'lumotlarni himoyalash.

Tayanch-iboralar: Session management, Autentifikatsiya, Session hijacking

18. OSI modelining taqdimot sathida ma'lumotlarni himoyalash.

Tayanch-iboralar: Shifrlash, Kodlash (encoding), Formtlash

19. OSI modelining ilova sathida ma'lumotlarni himoyalash.

Tayanch-iboralar: HTTP, FTP, SMTP, Web xavfsizlik, SQL injection, XSS

20. OSI modeli va TC/IP modeli farqlanishi va ularda xavfsizlik muammolari.

Tayanch-iboralar: Sathlar soni, Amaliy qo'llanish, Xavfsizlik kamchiliklari

**Davlat attestatsiya sinovlarida Ixtisoslik fanlari bo'yicha bitiruvchilar
bilimini baxolash**

MEZONLARI

O'zbekiston Respublikasi Prezidentining 2018-yil 5-iyundagi PQ-3775-son «Oliy ta'lim muassasalarida ta'lim sifatini oshirish va ularning mamlakatda amalga oshirilayotgan keng qamrovli islohotlarda faol ishtirokini ta'minlash bo'yicha qo'shimcha chora-tadbirlar to'g'risida»gi qaroriga asosan amalga oshiriladi.

1. Bitiruvchi kurs talabalari uchun o'tkaziladigan yakuniy davlat attestatsiyasi sinovlari Farg'ona davlat texnika universitetida o'qiydigan tillar, ya'ni o'zbek va rus tillarida topshiriladi.

2. Bitiruvchi kurslar uchun o'tkaziladigan yakuniy davlat attestatsiyasi sinovlari tanlangan mutaxassislik fanlari bo'yicha o'tkaziladi.

Farg'ona davlat texnika universitetida 2018-2019-o'quv yilidan boshlab o'qitishning kredit tizimi joriy etilganini inobatga olgan holda ballar taqsimoti quyidagicha holatda amalga oshiriladi:

“5” - “A”lo — 90 – 100;

“4” - “Yaxshi” — 70 – 89;

“3” - “Qoniqarli” — 60 – 69;

“2” - “Qoniqarsiz” — 0 – 59;

0 – 59 oralig'ida ball to'plagan talabalar yakuniy davlat attestatsiya sinovlaridan o'ta olmagan hisoblanadi. Yakuniy davlat attestatsiyasi sinovidan o'ta olmagan shaxs o'qish muddati tugagandan so'ng, arizasiga muvofiq yakuniy davlat attestatsiyasi sinovini keyingi yillarda qayta topshirish huquqiga ega. Bunda oliy ta'lim muassasasi rektori (direktori) shaxsni yakuniy davlat attestatsiyasi sinovini qayta topshirishga qo'yish bo'yicha buyruq chiqarishi lozim bo'ladi.

Bitiruvchi kurslar uchun o'tkaziladigan yakuniy davlat attestatsiyasi tanlangan mutaxassislik bo'yicha bilim darajasini belgilovchi maxsus fanlardan sinov o'tkaziladi, baholash mezonlari 0 balldan 100 ballgachani tashkil qiladi. Sinov maxsus yozma ish ravishda tashkil etilib, yakuniy davlat attestatsiyasini topshiruvchilar tanlangan mutaxassislik bo'yicha nazariy bilimi aniqlanadi. Maxsus fanlar bo'yicha savollar ushbu fanlar dasturlari asosida tuzilgan. Har bir variant 5 ta savoldan iborat bo'lib 100 ballni to'plash mumkin.

Mutaxassislik bo'yicha har bir savolga javob to'g'ri va to'liq yoritilsa, savolning ahamiyati, amaliy jihatlari, natijalari mustaqil aniq fikrlar asosida muammolarga jiddiy yondashilgan holda yoritilsa, javobda mantiqiy yaxlitlikka erishilgan bo'lsa, o'zlashtirish ko'rsatkichi 20 ball oralig'ida baholanadi.

Berilgan savolga to'g'ri javob yozilsa, javoblar ilmiy-amaliy jihatdan asosli, mantiqli yoritilgan bo'lsa, biroq ta'lim islohatlarni bugungi yangilanishlar amaliyoti

bilan bog'lashda ayrim noaniqliklarga yo'l qo'yilgan bo'lsa, o'zlashtirish ko'rsatkichi 18 ball oralig'ida baholanadi.

Savolga asosan to'g'ri javob yozilsa, biroq qo'yilgan masalaning mohiyati, mazmuni, natijalari yuzaki yoritilsa, fikr-mushohada bayonida tarqoqlik kuzatilsa o'zlashtirish ko'rsatkichi 15 ball oralig'ida baholanadi.

Savolga javob noto'g'ri yozilsa, o'quv adabiyotidan so'zma-so'z ko'chirilgan bo'lsa, savollarga umuman javob yozilmagan bo'lsa yoki savolni mohiyatini tushunmaydi, lekin atroflicha yondashsa o'zlashtirish ko'rsatkichi 0-15 ball oralig'ida baholanadi.

№	Umumiy ball	Yakuniy davlat attestatsiyasini topshiruvchining bilim darajasi	Ball
1.	20	Qo'yilgan savolga javob mazmunan aniq yoritilgan, uning mazmun va mohiyati to'liq ochib berilgan, javobda mantiqiy yaxlitlikka erishilgan.	4
		Mamlakatimizda amalga oshirilayotgan ta'lim islohotlar tahlili, uning amaliy samaralari, natijalari bo'yicha mustaqil, ijodiy fikrning mavjudligi.	4
		Muammolarni aniq misollar bilan tahlil qilish qobiliyatiga ega.	4
		Mantiqiy ketma-ketlikka erishilganlik, savol bo'yicha umumiy xulosalar chiqarilganlik.	4
		Imlo va stilistik xatolarga yo'l qo'yilmagan.	4
2.	18	Berilgan savolga to'g'ri javob yozilgan, ammo noaniqliklar va cheklanishlarga yo'l qo'yilgan.	4
		Savolga javob yozishda bitiruvchining mustaqil fikrlash qobiliyati seziladi.	4
		Amaliy masala ko'rsatilgan.	3
		Javoblarga ijodiy yondashuv mavjud.	3
		Imlo va stilistik xatolarga yo'l qo'yilmagan.	4
3.	15	Javobda masalaning mohiyati tushuntirilgan, biroq mazmun va natijalar yuzaki yoritilgan.	3
		Javobda fikrlar tarqoq.	3
		Mantiqiy ketma-ketlik mavjud emas.	3
		Berilgan savol bo'yicha umumiy tasavvurga ega, lekin tahlil yetarli emas.	3
		Imlo va stilistik xatolarga yo'l qo'yilmagan.	3

4.	0-15	Noto'g'ri javob berilgan. Savol bo'yicha aniq tasavvurga ega emas. O'quv adabiyotlaridan so'zma-so'z ko'chirilgan. Savolni mohiyatini tushunmaydi, lekin atroflicha yondashilgan.	0-15
----	------	--	------

ASOSIY ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasining Konstitutsiyasi. - T., 2023.
2. O'zbekiston Respublikasining 560-II-sonli «Axborotlashtirish to'g'risida»gi 2003 yil 11 dekabr qonuni // O'zbekiston Respublikasi Oliy Majlisining axborotnomasi. - 2004. - № 1-2. - 10-m.
3. O'zbekiston Respublikasining 848-XII-sonli «Davlat sirlarini saqlash to'g'risida»gi 1993 yil 7 may qonuni // O'zbekiston Respublikasi Oliy Kengashining axborotnomasi. - 1993. - № 5 - 232-m.
4. O'zbekiston Respublikasining 1060-XII-sonli «Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma'lumotlar bazasining huquqiy himoyasi to'g'risida»gi 1994 yil 6 may qonuni // O'zbekiston Respublikasi Oliy Kengashining axborotnomasi. - 1994. - № 5 - 136-m.
5. O'zbekiston Respublikasining 1006-XII-sonli «Maxsulotlar va xizmatlarni sertifikatlashtirish to'g'risida»gi 1993 yil 28 dekabr qonuni // O'zbekiston Respublikasi Oliy Kengashining axborotnomasi. -T., 1994. - № 2 - 50-m.
6. M.M.Aripov, B.F.Abdurahimov, A.S.Matyakubov. Kriptografik usullar: O'quv qo'llanma/Toshkent, "Tafakkur avlodi", 2023. -188 bet.
7. Akbarov D.Y., Xasanov P.F., Xasanov X.P., Axmedova O.P., Xolimtayeve I.U.: "Kriptografiyaning matematik asoslari". O'quv qo'llanma. -Toshkent. TATU. 2019 – 192 bet
8. Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; - T.: "Nihol print", 2021. - 224 b.
9. L.K. Mamadaliyeva, I.A. Jo'rayev. Axborot xavfsizligi. Darslik. "Navro'z" nashriyoti, 184b. 2020-yil.
10. M.M.Turdimatov. Kiberxavfsizlik siyosati. Darslik. Toshkent. Cho'lpon. 2025 y. 308 b
11. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. Darslik. "Fan va texnologiya". 2017yil. 372 b.
12. S.K.Ganiev. Kiberxavfsizlik asoslari. O'quv qo'llanma. Toshkent. Nihol print. 2021 y. 224 b.
13. Sh.Umarov. Kiberxavfsizlik asoslari. O'quv qo'llanma. Toshkent. Fer-Teach. 2024 y. 152 b.

14. A.O.Po'latov. Axborot xavfsizligi protokollari. O'quv qo'llanma. Toshkent. Aloqachi nasriyoti 2019- yil. 168 b
15. S.K. Ganiev va boshq. Axborot xavfsizligi. Darslik. "Fan va texnologiya". 2017-yil. 372b
16. A.N. Qudratov va boshq. Axborot xavfsizligi asoslari. Darslik. "NIF MSH" nashriyoti. 2024-yil. 248b.
17. Ganiev A.A va boshq. Kompyuter tizimlari va tarmoqlarini buzish va himoyalash. O'quv qo'llanma. Toshkent. Metodist nashriyoti. 2024-y. 232b.
18. В.Ф.Шаньгин. Информационная безопасность компьютерных систем и сетей. Учебник. Ид"Форум"-Инфра-М. 2019 год. 416 стр.
19. Е.К.Баранова. Информационная безопасность и защита информации. Учебное пособие. «Инфра-М». 2019 год. 336 стр.
20. Katz J., Lindell Y. Introduction to modern cryptography. – CRC press, 2014.
21. Stamp M. Information security: principles and practice. – New York : Wiley, 2011. – T. 2.
22. Akbarov D. Ye. "Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi" – Toshkent, 2008 – 394 bet.
23. Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Toshkent, 2021 – 206 bet.
24. Kiberxavfsizlik asoslari: O'quv qo'llanma / S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; - T.: "Iqtisod-Moliya", 2021. – 228 b.

QO'SHIMCHA ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasi Prezidentining 2017 yil 7 fevraldagi PF-4947-son «O'zbekiston Respublikasini yanada rivojlantirish bo'yicha Harakatlar strategiyasi to'g'risida» gi Farmoni.
2. O'zbekiston Respublikasi Prezidentining 2007 yil 3 apreldagi PQ-614-son «O'zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to'g'risida»gi Qarori.
3. Axborot texnologiyasi. Axborotlarni kriptofafik muhofazasi. Ma'lumotlarni shifrlash algoritmi" O'zbekiston Davlat standarti. O'zDSt 1105:2009.
4. F.M.Muxtorov. Kiberxavfsizlik asoslari. Darslik. Farg'ona. Classic. 2023 y. 338 b.
5. С.К. Ганиев, З.Т. Худойкулов, Н.Б. Насруллаев. Основы кибербезопасности: учебное пособие, -Т.: «Mahalla va oila nashriyoti», 2021. -240 c
6. В.А. Семенко. Информационная безопасность. Учебное пособие. «Форум-Инфа». 2019 год. 416стр.

7. Е.К.Баранова. Информационная безопасность и защита информации. Учебное пособие. «Инфра-М». 2019 год. 336 стр
8. Шелухин О.И., Канасев С.Д., Стеганография. Алгоритмы и программная реализация. Учебное пособие 2021г., 592стр
9. В.Г.Грибунин, И.Н.Оков, И.В.Турицев. Цифровая стеганография-М.: СОЛОН-Прес, 2017.-262с.
- 10.Шелухин О.И., Магомедова Д.И., Технологии стеганографии в системах инфокоммуникаций. Форматная стеганография. Практикум 2020г., 34стр
- 11.Грибунин, В. Г. Цифровая стеганография [Электронный ресурс] / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — Москва: СОЛОН-Пресс, 2018. — 262 с. — ISBN 978-5-91359-173-9
- 12.Z.Z.Miryusupov. Kompyuter tarmoqlari. O'quv qo'llanma. Toshkent. Aloqachi nashriyoti. 2020-y.144 b.
- 13.A.M.Eshmuradov va boshq. Internet tarmoqlari va xizmatlari. Darslik. Toshkent. Aloqachi nashriyoti. 2017-y. 476 b.
- 14.B.A.Turgunov. Kompyuter tarmoqlari loyihalash. O'quv qo'llanma. Farg'ona. Classic nashriyoti. 2021-yil. 172 b.
- 15.N.Jo'rayev va boshq. Kompyuter tizimlari va tarmoqlari. O'quv qo'llanma. Farg'ona. Farg'ona nashriyoti. 2009-y. 100 b.
- 16.Aumasson J. P. Serious cryptography: a practical introduction to modern encryption. – No Starch Press, 2017.
- 17.Sen J. Homomorphic encryption-Theory and Application //Theory and Practice of Cryptography and Network Security Protocols and Technologies. – 2013. – S. 1-21.

Internet saytlar

1. www.zivonet.uz
2. www.cert.uz
3. www.uzinfocom.uz
4. www.lex.uz