O‘ZBEKISTON RESPUBLIKASI
OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI
CHIRCHIQ DAVLAT PEDAGOGIKA UNIVERSITETI

“TASDIQLAYMAN”
Chirchiq davlat pedagogika
universiteti rektori
O.A.Muxamedov
2023 yil “29” avgust

AXBOROT XAVFSIZLIGI O’QUV DASTURI

Bilim sohasi:	100000 – Ta’lim
Ta’lim sohasi:	110000 – Ta’lim
Ta’lim yo‘nalishi:	60110600 – Matematika va informatika

Chirchiq – 2023

Fan/modul kodi AXAM4804	O‘quv yili 2026-2027	Semestr 8	ECTS - Kreditlar 4	
Fan/modul turi Majburiy	Ta’lim tili O‘zbek		Haftadagi dars soatlari 4	
1.	Fanning nomi	Auditoriya mashg‘ulotlari (soat)	Mustaqil ta’lim (soat)	Jami yuklama (soat)
	Axborot xavfsiligi	60	60	120

2.

I. Fanning mazmuni.

Fanning maqsadi — bo‘lajak informatika o‘qituvchilariga zamonaviy axborot xavfsizligining eng muhim bo‘lgan ilmiy-nazariy asoslari va amaliy jihatlarini chuqur o‘rgatish, Davlat ta' lim standarti va malaka talabalariga javob beradigan bilimlar berish, zamonaviy axborot xavfsizligii yo‘nalishida innovatsion g‘oyalarni yaratishga bo‘lgan qiziqishlarini oshirish, informatika o‘qituvchisining zamonaviy dasturlashga oid kasbiy kompetensiyalarni shaklantirish hamda rivojlantirishdan iborat.

Fanning vazifalari - talabalardan Kadrlar tayyorlash milliy dasturi asosida shuningdek, mamlakatimizda axborot kommunikatsiya-texnqlogiyalari sohasini yanada rivojlantirish, talaba-yoshlarni zamonaviy axborot xavfsizligi, IT sohasida innovatsion g‘oyalarni yaratishga bo‘lgan qiziqishlarini oshirish, ob'yektga yo‘naltirilgan axborot xavfsizligining nazariy asoslarini bilish, ob'yektga yo‘naltirilgan muhitlarda xabarlarni uzatish, ularga ishlov berish, ob'yektlar iyerarxiyasi asosida dasturlarni loyihalash, muayyan ob'yektga yo‘naltirilgan muhitlarda chiziqli, tarmoqlanuvchi va takrorlanuvchi va modulli dasturlar tuza olish, loyihalash va ulardan foydalana olish, masalalarni tahlil qila lish, masalalarga mos tuzilgan dastur va natijalarni taqqoslay olish ko‘nikma va malakalariga ega bo‘lish talab etiladi.

II. Nazariy qism (ma’ruza mashg‘ulotlari)

II.I. Fan tarkibiga quyidagi mavzular kiradi:

1-mavzu: Axborot xavfsizligining asosiy tushunchalari

Axborot xavfsizligi faniga kirish. Xavfsizlik siyosati. Xavfsizlikni baxolash va hk o’rganish.

2-mavzu: Axborotlarni stenografik va kriptografik himoyalash

Axborotni ximoayida stenografik himoyalashni o’rganish. Kriptografik algoritmlar. Kriptografik himoyalash usullarini o’rganish.

3-mavzu: Simmetriyali va nosimmetriyali kriptotizim asoslari

Axborotlarni himoyalashda simmetrik va no simmetrik kriptotizimlarni o’rganish. Axborot xavfsizligida algoritmlarni tasfirlash.

4-mavzu: Axborotlarni himoyalashning klassik usullari. Sezar shifri, Affin

tizimi

Axborotni ximoyalashda klassik usllarni o'rganish hamda Sezar shifri usulida himoyalash. Affin usullarini analiz qilish va qo'llashni o'rganish.

5-mavzu: Kalit so`zli jadval almashtirishlar. Sehrli kvadrat usulida shifrlash

Axborotni kalitlar yordamida himoyalash. Axborotlarni tasimlash yordamida sehrli kvadratchalarga bo'lish usulida shifrlashni o'rganish.

6-mavzu: Identifikatsiya va autentifikatsiya vositalari

Axborotni himoyalashda Identifikatsiya jarayoni. Autentifikatsiya jarayonini o'tkazish. Identifikatsiya va autentifikatsiya vositalarini o'rganish.

7-mavzu: Ryukzak algoritmi

Axborot xavfsizligida ma'lumotlarni to'g'ri taksimlashni o'rganish. Ma'lumotlarni taksimlashda jadval usulini qo'llashni o'rganish.

8-mavzu: RSA algoritmi

Shifrlash algoritmlari bilan tanishish. RSA algoritmi bilan ishlash. RSA algoritmini masalalarda qo'llashni o'rganish.

9-mavzu: Rabin algoritmi

Rabin algoritmi bilan tanishish. Rabin algortimini bo'laklarga bo'lgan holda o'rganish. Rabin algoritmini masalalarda qo'llashni o'rganish.

10-mavzu: Elgamal shifrlash algoritmi

Elgamal algoritmi bilan tanishish. Elgomal algoritmini sintez va analiz qilish. Elgomal algoritmi bilan ma'lumotlarni shifrlash.

11-mavzu: Elektron raqamli imzo va uning turlari

(ERI)Elektron raqamli imzo bilan tanishish. ERI bo'laklarga bo'lgan holda xeshlash funksiyalari bilan tanishish. ERI ning turlari bilan tanishish. ERI real masalalarda qo'llashni o'rganish.

12-mavzu: DSA va GOST R 34.10-94 elektron raqamli imzo algoritmlari

DSA electron raqamli imzo algoritmini bilan tanishish. GOST R 34.10.-94 elektron raqamli imzo algoritmi bilan tanishish. ERI larning farqlari va qo'llash

mumkin bo'lgan sohalari bilan tanishish.

13-mavzu: Kompyuter tarmoqlari xavfsizligini ta'minlash

Tarmoq xavfsizligi bilan tanishish. Tarmoqdan kelishi mumkin bo'lgan xavflarni aniqlash. Xavfsizlikni ta'minlash dasturlari bilan ishlashni o'rganish.

14-mavzu: Axborotni himoyalashning huquqiy masalalari

Axborotlarni himoyalashning huquqiy normalari. Axborotning himoyalanganlik darajalari va uning xavfsizligi bilan tanishish.

15-mavzu: Tashkilot yoki korxonalarda axborot havfsizligini ta'minlash

Tashkilotlarda axborot xavfsizligi turlari. Tashkilot yoki korxonalarda axborot xavfsizligini ta'minlashning ishonchli usullari bilan tanishish.

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

Amaliy mashg'ulotlar uchun quyidagi mavzular tavsiya etiladi:

1. Axborot xavfsizligining asosiy tushunchalari
2. Axborotlarni stenografik va kriptografik himoyalash
3. Simmetriyali va nosimmetriyali kriptotizim asoslari
4. Axborotlarni himoyalashning klassik usullari. Sezar shifri, Affin tizimi
5. Kalit so`zli jadval almashtirishlar. Sehrli kvadrat usulida shifrlash
6. Identifikatsiya va autentifikatsiya vositalari
7. Ryukzak algoritmi
8. RSA algoritmi
9. Rabin algoritmi
10. Elgamal shifrlash algoritmi
11. Elektron raqamli imzo va uning turlari
12. DSA va GOST R 34.10-94 elektron raqamli imzo algoritmlari
13. Kompyuter tarmoqlari xavfsizligini ta'minlash
14. Axborotni himoyalashning huquqiy masalalari
15. Tashkilot yoki korxonalarda axborot havfsizligini ta'minlash

IV. Mustaqil ta'lim va mustaqil ishlar

Mustaqil ta'limni baholash – bu talabalarning jamoaviy tartibda va yakka tartibda berilgan amaliy loyihalarni bajarishlari orqali amalga oshiriladi. Bunda har bir talabaga bitta jamoaviy loyiha va ikkita yakka tartibda bajariladigan loyiha beriladi. Talaba berilgan loyihaning maqsad va vazifalarini, mohiyatini tushungan holda qo'yilgan masalani 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 to‘liq ochib beriladi. **V. Mustaqil ta’lim uchun tavsiya etiladigan mavzular:** 1. Internetda xavfsizlik 2. Axborot xavfsizligiiningasosiy tashkil etuvchilari 3. Himoya ob’ektlari 4. Axborotni toifalari va tashuvchilari 5. Axborot tizimlarida himoyalash 6. Zararli dasturlar 7. Zararli dasturlardan himoyalanish yo‘llari 8. Kompyuter jinoyatlari tahlili 9. Axborotni yo‘qotishdan himoyalash 10. Dasturiy vositalarni rad etishdan himoyalash 11. Apparatli vositalarni rad etishdan himoyalash 12. Axborotni taqdim qilish va saqlash shakllari 13. Axborotlarni himoyalashning metodlari 14. Axborot xavfsizligini ta’minlovchi organlar 15. Tashkilotning axborot xavfsizligi 16. Cisco maxsus ilovasi 17. Axborot xavfsizligi va tahdidlarni tahlil qilish 18. Kriptografik kalitni boshqarish vositasi 19. Diskdagi ma’lumotlarni shifrlash tizimlari 20. Tarmoqda uzatiladigan ma’lumotlarni shifrlash tizimlari 21. Axborot xavfsizligini rivojlanishining tarixiy jihatlari 22. Axborotlarnihimoyalashning tashkiliy-texnik usullari 23. Kompyuter viruslaridan himoyalanish 24. Axborotlarni viruslardan himoyalash 25. Axborotlarni himoyalashning zamonaviy yo‘llari 26. Axborotlarni himoyalashning yangi metodlari 27. Axborot xavfsizlik siyosati 28. Axborot xavfsizligining huquqiy meyorlari 29. Taqmoq xavfsizligi tushunchasi va turlari. 30. Tarmoq xavfsizligini tekshirish dasturlari va turlari
3.	**VI. Ta’lim natijalari (shakllanadigan kompetensiyalar)** **Fanni o‘zlashtirish natijasida talaba:** — ob'yektga yo'naltirilgan axborot xavfsiligining nazariy asoslari, ob'yektlarni loyihalash, matematik va interfeys ob'yektlari, voqealar va xabarlar, ob'yektga yo'naltirilgan muhitlarda xabarlami uzatish, ularga ishlov berish mexanizmlari, ob'yektlar iyerarxiyasi asosida dasturlarni loyihalash, muayyan ob'yektga

	yo'naltirilgan axborot xavfsiligi to'g'risida bilimga; — ob'yektga yo'naltirilgan axborot xavfsiligida chiziqli, tarmoqlanuvchi va takrorlanuvchi va modulli dasturlar tuza olishni, dasturlashning ob'yektga yo'naltirilgan paradigmasini, ob'yektga yo'naltirilgan muhitlarda dasturlarni loyihalash ko 'nikmasiga; — ob'yektga yo'naltirilgan axborot xavfsiligi muhitida ishlash, masalalarni tahlil qila olish, muayyan axborot xavfsiligi yordamida masalalarning dasturini tuzish va natijalarni taqqoslay olish malakalariga ega bo'lishi lozim.
4.	**VII. 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 hioya qilish uchun loyihalar
5.	**VIII. 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 bajarishi zarur.
6.	**IX. Asosiy adabiyotlar:** 1. Karimov I.M., Turg`unov N.A. Axborot xavfsizligi asoslari. T.: O'zbekiston Respublikasi IIV Akademiyasi, 2013. – 123 b. 2. Ganiyev S.K., Ganiyev A.A., Xudoyqulov Z.T. Kiberxavfsizlik asoslari T.: «Aloqachi», 2020, 303 bet. 3. G'aniyev S.K. Karimov M.M. Tashev.K.A. Axborot xafsizligi. T.: «Fan va texnologiya», 2017,372 bet. 4. Akbarov D.E. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanishi. – T.: «O'zbekiston markasi», 2009. –424 b. 5. Жданов О.Н., Золотарев В.В. Методы и средства криптографической защиты информаци. СибГАУ. –Красноярск, 2007. – 217 с. 6. Lai X., Massey J.L. A proposal for a new block encryption standard //Advances in Cryptology – Proc. Eurocrypt'90, LNCS 473, Springer-Verlag, 1991, pp. 389-404.

	X. Qo‘shimcha adabiyotlar 1. Aripov M., Matyakubov A.S. Axborotlarni himoyalash usullari. Toshkent “Universitet” 2014 2. Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014 3. Charles P. Pfleeger, Shari Lawrence Pfleeger. Security in Computing, 4th Edition. Pearson Education, Inc.2007 4. Michael E. Whitman. Herbert J. Mattord. Principles of Information Security, Fourth Edition. Course Technology, Cengage Learning. 2012 5. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с. **Axborot manbalari** 1. www.lex.uz - O‘zbekiston Respublikasi Qonun hujjatlari milliy bazasi 2. www.ziyonet.uz – Axborot ta’lim portali 3. www.edu.uz – Oliy va o‘rta maxsus ta’lim vazirligi portali 4. www.tdpu.uz – Nizomiy nomidagi TDPU rasmiy sayti 5. www.cspi.uz- Chirchiq davlat pedagogika universiteti
7.	**Chirchiq davlat pedagogika universiteti tomonidan ishlab chiqilgan va universitet Kengashining 2023 yil “** 29 **” avgust dagi qarori bilan tasdiqlangan**
8.	**Fan/modul uchun ma’sul:** **R.O.Sultanov** CHDPU, “Informatika va axborot texnologiyalari” kafedrasi katta o`qituvchisi.
9.	**Taqrizchilar:** **S.N.Tursunov** - TDPU “Informatika o’qitish metodikasi” kafedrasi mudiri **G.T.Yudasheva** – CHDPU “Informatika o’qitish metodikasi” kafedrasi v.v.b. dotsenti