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

“TASDIQLAYMAN”
Chirchiq davlat pedagogika
universiteti rektori
G.I.Muxamedov
_____
2024 yil “__” _____

KIBERXAVFSIZLIK ASOSLARI
O‘QUV DASTURI

Bilim sohasi:	600000 – Axborot-kommunikatsiya texnologiyalari
Ta’lim sohasi:	610000 – Axborot-kommunikatsiya texnologiyalari
Ta’lim yo‘nalishi:	60610100 –Axborot tizimlari va texnologiyalari

Chirchiq – 2024

Fan/modul kodi KIA1406	O‘quv yili 2025-2026	Semestr 4	ECTS - Kreditlar 6	
Fan/modul turi Majburiy	Ta’lim tili O‘zbek/rus		Haftadagi dars soatlari 6	
1.	Fanning nomi	Auditoriya mashg‘ulotlari (soat)	Mustaqil ta’lim (soat)	Jami yuklama (soat)
	Kiberxavfsizlik asoslari	90	90	180

2.

I. Fanning mazmuni.

Fanni o‘qitishdan maqsad – Kiberxavfsizlik asoslari fani kasbiy faoliyatda axborot tizimlari va axborot resurslarining axborot xavfsizligini ta’minlash bo’yicha masalalarni yechishda bilim, ko’nikma va malaka shakllantirishdan iborat.

Fanning vazifasi – talabalarga kiberxavfsizlikning asosiy tizimlari bilan tanishtirish va kriptografiya asoslari, foydalaishni nazoratlash, tarmoq va kompyuter xavfsizligini ta’minlashning hamda axborot xavfsizligini ta\minlashga oid dasturlar yaratish, mavjudlarini takomillashtirish.

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

II.I. Fan tarkibiga quyidagi mavzular kiradi:

1-mavzu. Kiberxavfsizlikning umumiy asoslari

Kursning qisqacha mazmuni va tarkibi, baholash mezonlari; axborot xavfsizligining asosiy tushunchalari; axboroat xavfsizligini ta’minlash darajalari(huquqiy, tashkiliy, tehnik), konteksga bog’liq holda tizim tushunchasi; tizimni tahlillashga yaxlitli yondashuv

2-mavzu. Kriptografiyaning asosiy tushunchasi va tarixi.

Shifrlash/deshifrlash; shifrlarga hujumlarning turkumlanishi; simmetrik va assimmetrik kriptografiya, kriptografiyaning tarixi, klassik shifrlar, bir martalik bloknot, stenografiya

3-mavzu. Simmetrik shifrlash.

Haqiqiy ma‘nosini inson tushunmaydigan belgilar ko‘rinishiga o‘tkazish. Blokli shifrlash. oqimli shifrlash ko’llanilishi

4-mavzu. Assimmetrik shifrlar.

Tushuncha, namuna, qo’llanilishi. assimmetrik shifrlash tizimlari hamda ularning matematik asoslari.

5-mavzu. Autentifikatsiya.

Identifikatsiya, autentufukatsiya va avtorizatsiya tushunchalari, turkumlanishi, ko’p oqimli autentifikatsiya, kriptografik tokenlar, kriptografik kurilmalar,

biometrik autentifikatsiya, bir martalik parollar, bilishga asoslangan autentifikatsiya, parolli avtorizatsiya.

6-mavzu. Parollarga hujumlar va parollarni saqlash.

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.

7-mavzu. Ma'lumotlar butunligi.
Elektron raqamli imzo, ko'llanilishi. Muammo hal etish uchun ma'lumotlar etarlilik darajasini bildiradi o'lchovlar.

8-mavzu. Ma'luomtlarning fizik xavfsizligi.
Ma'lumotlarni ishlash markazining xavsizligi, foydalaish kaliti, odamlarning xarakatlanishi, foydalanish kartasi va videokuzatuv.

9-mavzu. Ma'lumotlardan foydalanishning mantiqiy nazorati. Formal modellar.
Ma'lumotlarning turkumlanishi; himoya domenlari, ACL, C-list. Guruhli siyosat, parol, DAC, MAC, RBAC, ABAC, Bella-LaPadulla, Biba modellari.

10-mavzu. Diskli va faylli shifrash. Ma'lumotlarni xavfsiz chiqarib tashlash.
Apparatli va dasturli shifrlash, afzalliklariva kamchiliklari; qayta yozish, magnitsizlantirish, fizik yo' qqilish usullari, xotirani qoldiq magnitlanganligi.

11-mavzu. Kompyuter tarmoqlarining asoslari
Asosiy tushunchalar, topologiyalari, TCP/IP modeli.

12-mavzu. Tarmoq xavfsizligining tahdid va zaifliklari.
Tarmoq hujumlari, tahdid va zaifliklar, turkumlanishi.

13-mavzu. Tarmoqlararo ekran va virtual xususiy tarmoqlar.
Turkumlanishi, qo'llanislishi.

14-mavzu. Simsiz tarmoq xavfsizligi.
Simsiz tarmoqlarda tahdid va zaifliklar, turkumlanishi, qarshi choralar

15-mavzu. Loglash.
Loglash, loglarni tahlillash, suquluib kirishlarni aniqlashning loglar bilan bog'liqligi.

III. Seminar mashg‘ulotlar bo‘yicha ko‘rsatma va tavsiyalar

Seminar mashg‘ulotlar uchun quyidagi mavzular tavsiya etiladi:

1. Axborot xavfsizligining asosiy tushunchalari.
2. Axboroat xavfsizligini ta’minlash darajalari(huquqiy, tashkiliy, tehnik)
3. Shifrlash va deshifrlash
4. Kriptografiyaning tarixi, klassik shifrlar, bir martalik bloknot, stenografiya.
5. Blokli shifrlashning qo’llanilishi.
6. Oqimli shifrlashning qo’llanilishi.
7. Assimmetrik shifrlash usullari.
8. Assimmetrik shifrlash usullari va ularning qo’llanilishi.
9. Identifikatsiya, autentufukatsiya va avtorizatsiya tushunchalari.
10. Kriptografik kurilmalar. Biometrik autentifikatsiya
11. Lug’at bo’yicha hujum, kombinatsiyalarni to’liq ko’rib chiqish.
12. Fishing va ijtimoiy injineriya. Parollarni buzish vositalari.
13. Elektron raqamli imzo va uni qo’llanilishi.
14. Imzo qo’yish va uni tekshirish.
15. Ma’lumotlarni ishlash markazining xavsizligi. Foydalanish kaliti.
16. Odamlarning xarakatlanishi, foydalanish kartasi va videokuzatuv.
17. Himoya domenlari, ACL, C-list. Guruhli siyosat.
18. DAC, MAC, RBAC, ABAC, Bella-LaPadulla, Biba modellari.
19. Apparatli va dasturli shifrlash, afzalliklari va kamchiliklari.
20. Fizik yo’ qqilish usullari. Qayta yozish va magnitsizlantirish.
21. Kompyuter tarmoqlarining asosiy tushunchalari.
22. Tarmoq topologiyalari. TCP/IP modeli.
23. Tarmoq hujumlari.
24. Tahdid va zaifliklarning turkumlanishi.
25. Tarmoqlararo ekran qo’llanilishi.
26. VPN (Virtual xususiy tarmoq).
27. Simsiz tarmoqlarda tahdid va zaifliklar.
28. Tahdid va zaifliklarga qarshi choralar.
29. Loglash, loglarni tahlillash.
30. Suquluib kirishlarni aniqlashning loglar bilan bog’liqligi.

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.

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 va kiberxavfsizlikda uning ahamiyati.
5. Kiberxavfsizlikda inson omilining roli va ijtimoiy injiniring usullari.
6. Ransomware dasturlarining rivoji va ularning oldini olish choralari.
7. Ma'lumotlar bazalarining xavfsizligi: zaifliklar va himoya choralar.
8. Web-sayt xavfsizligi: Cross-site scripting (XSS) hujumlari va himoya choralari.
9. Denial of Service (DoS) va Distributed Denial of Service (DDoS) hujumlari.
10. Zero-day hujumlar: kiberxavfsizlikdagi xavf va javob choralari.
11. Ma'lumotlarni zaif joylardan o'g'irlash va uning oldini olish yo'llari.
12. Botnetlar: ularning ishlash prinsiplari va zararli dastur sifatida roli.
13. Kompyuter viruslari va troyanlar: turlari, tarixi va qarshi choralar.
14. Kiberjinoyatchilikka qarshi xalqaro qonunchilik.
15. Zararkunanda dasturlarning asosiy turlari va ularni aniqlash usullari.
16. Blockchain texnologiyasining kiberxavfsizlikdagi o'rni.
17. Kiberxavfsizlikda mashinaviy o'rganish (machine learning) va sun'iy intellektning roli.
18. Sim kartalarning klonlanishi va mobil qurilmalarning xavfsizligi.
19. Ma'lumotlarning zaxira nusxalarini yaratish va tiklash texnologiyalari.
20. Cloud Computing xavfsizligi: tarmoq xavfsizligi, ma'lumotlarning zaifliklari.
21. Phishing hujumlari: usullari va foydalanuvchilarni himoya qilish choralari.
22. Internet-of-Things (IoT) qurilmalarining xavfsizligi.
23. Kiberjinoyatlarning iqtisodiy zararlari va tahlili.
24. Kiberhujumlarga javob berish va xavfiylikni tiklash rejalari.
25. DNS hijacking hujumlari va ularning oldini olish.
26. USB qurilmalar orqali kiberhujumlar va ularning oldini olish choralari.
27. Simsiz tarmoqlar uchun WPA3 protokolining xavfsizlik yaxshilanishlari.
28. BYOD (Bring Your Own Device) siyosatining kiberxavfsizlikka ta'siri.
29. Kiberxavfsizlikda ommaviy ma'lumotlarning himoyasi.
30. Kiberxavfsizlikda blockchain va kriptografik tokenlarining ishlatilishi.

VII. Ta'lim natijalari (shakllanadigan kompetensiyalar)

Fanni o'zlashtirish natijasida talaba:

- "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‘lishi; (bilim)** Ma’lumotlarni himoyalash uchun kriptografik usullarni qo‘llash va ularni samarali boshqarish ko‘nikmalarini o‘zlashtiradi. Hujumlarni aniqlash va ularga qarshi choralar ko‘rish: Xavfsizlik tizimlarida hujumlarni aniqlash, ularga qarshi choralar ko‘rish va himoya mexanizmlarini sinovdan o‘tkazish imkoniyatiga ega bo‘ladi. Qonunchilik va axborot xavfsizligi siyosatlari: Kiber xavfsizlik sohasidagi qonunchilik, standartlar va siyosatlarni tushunish hamda ularga rioya qilish. Voqealar monitoringi va tahlili: Axborot xavfsizligi voqealarini kuzatish, tahlil qilish va ularga javob berish imkoniyatidan **foydalana olishi; (ko‘nikma).** Xavfsizlik tahlili va auditi: Axborot tizimlari xavfsizligini muntazam ravishda baholash va audit o‘tkazish. Etik xakerlik (penetrening 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 choralarni tushunish. 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.**
4.	**VIII. 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.	**IX. 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.	**X. Asosiy adabiyotlar:** 1. S.K.Ganiyev, A.A. Ganiyev, Z.T. Xudoyqulov. Kiberxavfsizlik asoslari, o'quv qo'llanma, 2020 yil. Elektron. 2. Jo'rayev G.U., Alayev R.H, Muxamadiyev F.R, Kompyuter tarmoqlari xavfsizligi, Axborot xavfsizligi, o’quv qo’llanma, Innovatsiya-Ziyo. 2022-yil. 3. S.K.Ganiyev, M.M. Karimov, K.A. Tashayev, Axborot xavfsizligi, “TOSHKENT” darslik, 2017-yil, Elektron

	XI. Qo‘shimcha adabiyotlar 1. . “Axborot texnologiyasi. Axborotlarni kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi” O’zbekiston Davlat standarti. O’zDSt 1105:2009. 2. Хилл Б. “Полный спровочник по Cisco” Пер. с англ. М.:Изд. Дом Вильямсю 2008г. 3. Шнайер Б. Прикладная криптография. Протоколы, алгоримт, исходные тексты на языке Си.- М.: ИздательстваТРИУМФ, 2003г-816. 4. Mirziyoyev Sh.M. Buyuk kelajakimizni mard va olijanob xalqimiz bilan birga quramiz. 2017 **Axborot manbalari** 1. www.lib.cspi.uz 2. www.denemetr.com 3. www.security.uz 4. www.uzinfocom.uz 5. www.unilibrary.uz
7.	**Chirchiq davlat pedagogika universiteti tomonidan ishlab chiqilgan va universitet Kengashining 2024 yil “** 29 **”** 08 **1-sonli dagi qarori bilan tasdiqlangan**
8.	**Fan/modul uchun ma’sul:** D.K.Ibadullayev CHDPU, “Informatika va axborot texnologiyalari” kafedrasi o’qituvchisi.
9.	**Taqrizchilar:** **M.U.Maxkamova** - CHDPU “Informatika o‘qitish metodikasi” kafedrasi v.v.b. dots, p.f.f.d.(PhD) **I.X.Normatov** - O’zbekiston milliy universiteti “Axborot xavfsizligi kafedrasi” f-m.f.d. professor.