O‘ZBEKISTON RESPUBLIKASI
OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI
NAMANGAN MUHANDISLIK-QURILISH INSTITUTI

“TASDIQLAYMAN”
Namangan muhandislik-qurilish
instituti rektori
_____SH.T. Ergashev
«__» _____2024 y

KIBERXAVFSIZLIK ASOSLARI FANINING

O‘QUV DASTURI

Bilim sohasi:	600 000 – Ishlab chiqarish-texnik soha
Ta’lim sohasi:	610 000 – Ishlab chiqarish texnologiyalari
Ta’lim yo‘nalishi:	60610400 – Dasturiy injiniring

Namangan – 2024 y.

Fam/modul kodi KYSF16MBK	O‘quv yili 2024-2025	Semestr 3	Kreditlar 6
Fan moduli turi Asosiy	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	46 m / 44 a	90	180

2.

I. Fanning mazmuni

Fanni o‘qitishdan maqsad – fanni o‘qitishdan maqsad - talabalarda kasbiy faoliyatda axborot tizimlari va axborot resurslarining kiberxavfsizligini ta'minlash bo‘yicha masalalarni echishda bilim, kunikma va malaka shakllantirishdan iborat.

Fanning vazifasi - talabalarni kiberxavfsizlikning asosiy tushunchalari bilan tanishtirish, kriptografiya asoslari, foydalanishni nazoratlash, tarmoq va kompyuter xavfsizligini ta'minlashning xamda axborot xavfsizligiga taxdidlar va ularga karshi kurashishni samarali usul va vositalarini o‘rgatishdan iborat.

II. Asosiy nazariy qism (maruza mashg‘ulotlari)

II.I. Fan tarkibiga quyidagi mavzular kiradi:

1-mavzu: Kiberxavfsizlikning asosiy tushunchalari: Axborot xavfsizligining xayotdagi timsollari, kiberxavfsizlik, axborot xavfsizligi, konfidensiallik, yaxlitlik, foydadanuvchanlik, risk, xujumchi kabi fikrlash, tizimli fikrlash, aktiv, taxdid, zaiflik, boshqarish vositasi, kiberxavfsizlikning bilim soxalari.

2-mavzu: Kiberjinoyatchilik, kiberqonunlar va kiberataka: Ichki kiberjinoyatlar, tashki kiberjinoyatlar, kiberqonunlar, milliy qonunlar, xalqaro kiberqonunlar, kiberataka.

3-mavzu: Inson faoliyati xavfsizligi: Kiberxavfsizlikda inson omili, ijtimoiy (sosial) injineriya, Fishing, Sosial injineriyadan ximoyalanish choralari.

4-mavzu: Kiberxavfsizlik arxitekturasi, strategiyasi va siyosati: Kiberxavfsizlik arxitekturasi, strategiya. Kiberxavfsizlik siyosati va uni amalga oshirish: axborot xavfsizligi siyosati, xavfsizlik siyosatining zaruriyati, xavfsizlik siyosatining afzalliklari, xavfsizlik siyosatining ierarxiyasi, xavfsizlik siyosati

xususiyatlari, axborot xavfsizligi siyosatining turlari.

5-mavzu: Kriptografiyaning asosiy tushunchalari: Asosiy terminlar, kriptografiya bo‘limlari, kriptotizim, Kerkxofs prinsipi, Kriptografiya tarixi, kriptografik akslantiishlar, bir martali bloknot.

6-mavzu: Simmetrik kriptografik algoritmlar: Oqimli simmetrik shifrlash algoritmlari, A5/1 oqimli shifrlash algoritmi, blokli simmetrik shifrlash algoritmlari, simmetrik kriptotizimlardagi muammolar, simmetrik kriptotizimlarda kalit uzunligi.

7-mavzu: Ochik kalitli kriptotizimlar: bir tomonlama funksiya, faktorlash muammosi, modul arifmetikasi, RSA algoritmi, ochik kalitli kriptotizimlardan foydalanish, ochik kalitli kriptotizimlarda kalit uzunligi.

8-mavzu: Ma’lumotlar yaxlitligini ta’minlash usullari: Xesh funksiya, xabarlarni autentifikasiyalash kodi, xesh - funksiyalar asosida ma'lumot yaxlitligini tekshirish, ochik kalitli shifrlash algoritmlari asosida ma'lumot yaxlitligini tekshirish va rad-etishdan ximoyalash, ERIni shakllantirish jarayoni, ERIni tekshirish jarayoni, ochik kalitlar infrastrukturasi.

9-mavzu: Disklarni va fayllarni shifrlash. Ma’lumotlarni xavfsiz o‘chirish usullari. Apparat-dasturiy shifrlash, apparat shifrlash, dasturiy shifrlash, disk va fayl tizim satxida shifrlash. Qogoz kurinishdagi xujjatlarni yo‘q qilish usullari, elektron xujjatlarni yo‘q qilish.

10-mavzu: Identifikasiya va autentifikasiya vositalari: identifikasiya, autentifikasiya va avtorizasiya, bir tomonlama va ikki tomonlama autentifikasiya, ko‘p omilli autentifikasiya, parol tizimlari, elektron qurilmalar, biometrik tizimlar.

11-mavzu: Ma’lumotlardan foydalanishni mantikiy boshqarish: foydalanishni boshqarish, foydalanishni diskresion boshqarish usuli (Discretionary access control, DAC), foydalanishni mandatli boshqarish usuli (Mandatory access control, MAC), foydalanishni rollarga asoslangan boshqarish usuli (Role-based access control, RBAC), foydalanishni atributlarga asoslangan boshqarish usuli (Attribute-based access control, ABAC), foydalanishni boshqarish matrisasi, ACL yoki C-list.

12-mavzu: Ko‘p satxli xavfsizlik modellari: Bell-LaPadula modeli, Biba modeli, mantikiy va fizik foydalanishlarni boshqarish.

13-mavzu: Ma’lumotlarni fizik ximoyalash: Fizik xavfsizlik, uning zaruriyati, fizik xavfsizlikka ta'sir qiluvchi omillar, tab'iy taxdidlar, sun'iy taxdidlar, fizik xavfsizlikni nazoratlash, boshka fizik xavfsizlik choralari, ogoxlik / o‘qitish.

14-mavzu: Kompyuter tarmoqlari va tarmoq xavfsizligi muammolari. Tarmoq turlari, tarmoq topologiyalari, OSI modeli, tarmoqqa quyiladigan talablar, TCP/IP modeli, tarmoq vositalari. Zaiflik, taxdid, xujum, ichki taxdid, tashki taxdid, razvedka xujumlari, kirish xujumlari, zararli xujumlar, xizmatdan voz kechishga undash (Denial of service, DOS) xujumlari.

15-mavzu: Tarmoq xavfsizligini ta’minlovchi vositalar: tarmoqlararo ekranlash, virtual xususiy tarmoqlar, siqilib kirishlarni aniklash tizimlari (Intrusion Detection System, IDS), ma'lumotlarning sirkib| chikishini oldini olish tizimlari (Data Leakage Prevention, DLP), yolgon nishonlar yoki tuzoqlar (honeypot).

16-mavzu: Simsiz tarmoq xavfsizligi: Simsiz tarmoq turlari, simsiz tarmoqlardagi mavjud zaifliklar, nazoratlanmaydigan xudud, ruxsatsiz siqilib kirish, yashirincha eshitish, xizmat kursatishdan voz kechishga undash, tarmoq orqali uzatiluvchi ma'lumotni shifrlash.

17-mavzu. Risklarni boshqarish: risk, risk darajasi, risk chastotasi, risk matrisasi, risklarni boshqarish, muxim risk kursatkichlari, risklarni boshqarish boskichlari, tashkilotda risklarni boshqarishning freymvorki, risklarni boshqarishning axborot tizimlari (Risk Management Information Systems, RMIS).

18-mavzu. Foydalanuvchanlik tushunchasi: zaxira usxalash,ma'lumotlarni qayta tiklash va xodisalarni qaydlash: foydalanuvchanlik, zaxira nusxalash, zaxira nusxalash vositalari. RAID texnologiyasi, afzalliklari va kamchiliklari, zaxira nusxalash usullari, zaxiralash turlari.

19-mavzu. Ma'lumotlarni qayta tiklash, ma'lumotni yuqolish sabablari, ma'lumotlarni qayta tiklash vositalari, xodisalarni qaydlash.

20-mavzu. Dasturiy vositalardagi xavfsizlik muammolari: veb saytlar bilan bog‘liq xavfsizlik muammolari, keng tarkalgan veb zaifliklar, xavfsiz va xavfsiz bo‘lmagan dasturlar tillari, dasturiy vositalardagi zaifliklar bilan tushunchalar.

21-mavzu. Kompyuter viruslari va virusdan ximoyalanish muammolari:

zararli dasturlar turlari, viruslar va ularning kpassifikasiyasi, viruslarni amalga oshiruvchi vazifalari, zararli dasturiy vositalarni aniqlash usullari, vositalari.

22-mavzu. Qayd yozuvini ximoyalash: qayd yozuviga alokador ma'lumotlarni ximoyalash, siz bilan alokada bulgan tomon bilan ma'lumotlarni ximoyalash, siz bilan alokada bulmagan tomonlarda ma'lumotlarni ximoyalash. Parollar, parollarni generasiyalash, parollarni boshqarish, parollarni saqdash, parollarni uzatish, parolga alternativ usullarni aniqlash.

23-mavzu. Ijtimoiy injineriyaga qarshi ximoya: ijtimoiy injineriya turlari, ijtimoiy injineriya mutaxassislari foydalanadigan prinsiplar, ijtimoiy tarmoqlarda ma'lumotlarni bo'lishmaslik, qalbaki ijtimoiy media ulanishlarini aniqlash, xavfsiz dasturiy vositalardan foydalanish.

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

Amaliy mashg'ulotlari uchun quyidagi mavzular tavsiya etiladi:

1. Kiberxavfsizlikda risklarni baxolashni o'rganish.
2. Klassik shifrlash algoritmlarini ishlash tartibini o'rganish.
3. TrueCrypt dasturi yordamida ma'lumotlarni shifrlashni o'rganish.
4. Polialfavitli almashtirish algoritmi yordami shifrlashga misol
5. Vijiner jadvalini (matrisasini) qo'llagan holda shifrlash.
6. Gamil'ton marshrutlariga asoslangan shifrlashga misol.
7. Identifikasiyalash usullari.
8. Operasion tizimda (Windows OT) parolga asoslangan autentifikasiya mexanizmini o'rnatishva sozlashni o'rganish.
9. Parolga asoslangan autentifikatsiya usuli.
10. Disklarni va fayllarni shifrlash.
11. Razvedka xujumini amalga oshirishni o'rganish.
12. Tarmoq xavfsizligi zaifliklari.
13. Domenda guruhlar va foydalanuvchilarni boshqarish.
14. Tarmoqlararo ekran vositasi yordamida tarmoq ximoyasini qurish.
15. Xavfsiz Wi-Fi Simsiz tarmogini qurish.
16. Ma'lumotlarni zaxira nusxalash usullari.

17. Ma'lumotlarni qayta tiklash usullari.
18. Zararli dasturlar va ularning turlari, vazifalari.
19. Maxsus dasturiy vositalar yordamida ma'lumotlarni qayta tiklashni o'rganish.
20. Shaxsiy kompyuterlarda viruslarga qarshi ximoyani o'rnatish.
21. Parollardan foydalanishni boshqarishni o'rganish.
22. Ijtimoiy tarmoqlardan ma'lumotlarni tiklashni o'rganish.

IV. Mustaqil ta'lim va mustaqil ishlar

Mustaqil ta'lim uchun tavsiya etiladigan topshiriqlar:

1. Kiberxavfsizlikga oid milliy va xorijiy me'yoriy-xuquqiy xujjatlar taxlili.
2. Axborotni ximoyalashning kriptografik usullari.
3. Enigma shifrlash mashinasi va uning bardoshligi.
4. Axborotni foydalanuvchanligini ta'minlashda antivirus, IDS, IPS, TE vositalarining o'rni.
5. Zararli dasturiy vositalarni klassifikasiyasi va ximoya usullari.
6. Axborot-kommunikasiya texnologiyalari xavfsizligiga bo'ladigan taxdidlar.
7. Zararkunanda dasturlarning turlari.
8. Kompyuter viruslari va virusdan ximoyalanish usullari.
9. Xorijiy davlatlarning elektron raqamli imzo algoritmlari taxlili.
10. Identifikasiya va autentifikasiya tushunchasi va vazifalari.
11. Axborot tizimlari va resurslaridan ruxsatsiz foydalanishlarni aniqlash uslubiyati.
12. Simsiz aloka tizimlarida axborot resurslarini ximoyalash.
13. Axborotni ruxsatsiz foydalanishlardan ximoyalash.
14. Ijtimoiy injeneriyada xujumlar taxlili.
15. Zamonaviy antivirus dasturiy vositalari va ularning imkoniyatlari.
16. Kiberjinoyat va kiberxuquq.
17. Tarmoqda uzatiluvchi axborotni ximoyalashda kriptografiyaning o'rni.
18. Zararkunanda dasturlar va ulardan ximoyalanish (masalan, Malwarebytes misolida).
19. Kiberjinoyatchilik va uni keng tarqalishining sabablari.
20. Yuz tasviriga asoslangan autentifikasiya usuli va uning xususiyatlari.

	21. Barmoq iziga asoslangan autentifikasiya usuli va uning xususiyatlari. 22. Elektron raqamli imzo va uni resublikamizda tadbiq etilish xolati. 23. Kiberxavfsizlik soxasi bo'yicha mutaxassis toifalari. 24. Kiberxavfsizlik soxasida karrera yo'llarini o'rganish. 25. Axborot xavfsizligi soxasida ish boshlash. 26. Kiberxavfsizlik soxasida mashxur sertifikatlar. 27. Parollarni boshqarish tizimlari (masalan, LastPass) va ulardan foydalanish. 28. Virtual ximoyalangan tarmoq va undan amaliyotda foydalanish (masalan, CyberGhost yoki ExpressVPN misolida). 29. Sotsial injineriya nima va uning zamonaviy usullari. 30. Biror tarmoqlararo ekran vositasini (masalan, ZoneAlarm) o'rnatish va sozlash. 31. Virtual ximoyalangan tarmoq va undan amaliyotda foydalanish (masalan, CyberGhost yoki ExpressVPN misolida). 32. Windows OTda foydalanuvchi qayd yozuvini (xususan, paroldan foydalanish siyosatini) sozlash. 33. Windows OTda zaxira nusxalashni (Backup and Restore) amalga oshirish. 34. Windows OTda imtiyozlar turlari, fayl va kataloglar uchun foydalanishni boshqarish tartibi. 35. Linux OTda imtiyozlar turlari, fayl va kataloglar uchun foydalanishni boshqarish tartibi. 36. Ma'lumotlarni qayta tiklash vositalari (masalan, Recuva yoki EaseUS Data Recovery Wizard Pro) va ular yordamida ma'lumotlarni qayta tiklash. 37. VeraCrypt dasturiy vositasi yordamida ma'lumotlarni ximoyalash. Mustaqil o'zlashtiriladigan mavzular bo'yicha talabalar tomonidan mustaqil ishlar tayyorlash, uni taqdimot qilish va amalda bajarish tavsiya etiladi
3.	**V. Fanni o'qitilish natijalari (shakllanadigan kompetentsiyalar)** Fanni o'zlashtirish natijasida talaba: – kiberxavfsizlikni ta'minlash aspektlarini xuquqiy, tashkiliy va texnik satxlari; – kiberxavfsizlik tamoyillari xaqida tasavvurga ega bo'lishi; – kiberxavfsizlikning asosiy tushunchalarining ta'riflarini;

	– kiberxavfsizlikning xuquqiy-me'yoriy bazasini; – kiberxavfsizlik soxasida xalqaro, milliy va idoraviy me'yoriy-xuquqiy bazani; – axborotning konfidensialligi, butunliligi va foydalanuvchanligi tushunchalarini bilishi va ulardan foydalana olishi; – kiberxavfsizlikka taxdidlarning asosiy turlari xamda ularga qarshi kurashish metod va usullarini tushuntirib berishi; – axborotning maxfiyligi, butunligi va foydalanuvchanligining buzilishi (usullarini taxlil qilish; – axborotning yuqolishi va buzilishi sabablari, turlari, kanallarini taxlil qilish; – axborotni ximoyalash usullari va vositalarini qo'llash; – kriptografiya, foydalanishni boshqarish, tarmoq va kompyuter xavfsizligini ta'minlash ko'nikmalariga ega bo'lishi kerak.
4.	**VI. Ta'lim texnologiyasi va metodlari.** – ma'ruzalar; – amaliy ishlarini bajarish va hulosalash; – interfaol keys-stadilar; – mantiqiy fikrlash, tezkor savol-javoblar; – guruhlarda ishlash; – taqdimotlarni qilish; – indivual (yakka tartibdagi) loyihalar; – jamoa bo'lib ishlash va himoya qilish uchun loyihalar.
5.	**VII. Kreditlarni olish uchun talablar:** Fanga oid nazariy va uslubiy tushunchalarni to'la o'zlashtirish, tahlil natijalarini to'g'ri aks ettira olish, o'rganilayotgan jarayonlar haqida mustaqil mushohada yuritish, berilgan kurs loyihasini bajarib uni himoya qilish, nazorat uchun berilgan vazifa va topshiriqlarni bajarish, yakuniy nazorat bo'yicha test topshrish.
6.	**Asosiy adabiyotlar** 1. S.K. Ganiev, A.A. Ganiev, Z.T. Xudoykulov. Kiberxafsizlik asoslari: o'quv qo'llanma, -T.: "Nihol print" OK, 2021. - 224 b. 2. С.К. Ганиев, З.Т. Худойкулов, Н.Б. Насруллаев. Основи кибербезопасности:

	учебное пособие, -T.: «Mahalla va oila nashriyoti», 2021. -240 c. **Qo‘shimcha adabiyotlar** 1. В.Ф.Шангин, Информасионная безопасност компютерних систем и сетей: учебное пособие - М. : ФОРУМ : ИНФРА-М, 2019. - 416 с. 2. S.K. Ganiev, M.M. Karimov, K. A. Tashev; Axborot xavfsizligi: darslik; Uzb. aloqa va axborotlashtirish agentligi. - T.: Alooqachi, 2008. - 383 b. 3. S.K. Ganiyev, M.M. Karimov, K.A. Tashev; Axborot xavfsizligi: darslik/ O‘z. Res. Oliy va o‘rta maxsus ta’lim vazirligi, TATU. - Qayta nashr. - T.: Fan va Texnologiya, 2017. - 372 b. **Internet saytlari** 1. httDs://csec.uz/uz/ 2. httns://unicon.uz/ 3. httns://lex.uz/ru/docs/-5960604 - 0‘zbekiston Respublikasining kiberxavfsizlik to‘g‘risida qonuni, 15.04.2022 yildagi O‘RQ-764-son **Axborot manbaalari** 1. www.ziyonet.uz 2. www.informika.ru 3. www.bilim.uz 4. www.euroleather.com
7.	Fanning o‘quv dasturi Namangan muhandislik - qurilish instituti Kengashining “____” _____2024 yildagi №_____ - sonli bayoni bilan tasdiqlangan.
8.	**Fan / modul uchun mas’ullar:** Xaydarov K. – NamMQI, “Axborot tizimlari va texnologiyalari” kafedrasi katta o‘qituvchisi. Anvarov A. – NamMQI, “Axborot tizimlari va texnologiyalari” kafedrasi kata o‘qituvchisi.
9.	**Taqrizchi:** Xasanov A. – NamMQI “Texnik tizimlarda AT” kafedrasi mudiri, dotsent, texnika fanlari nomzodi. Boltibayev SH. – Namangan Davlat Univesiteti “Informatika” kafedrasi dotsenti, f-m.f.n.