O‘ZBEKISTON RESPUBLIKASI

OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

O‘quv-uslubiy bo‘lim tomonidan ro‘yxatga olindi

№ MD-70610302-3.04

2023-yil "5" 07

«TASDIQLANDI»

O‘quv ishlari bo‘yicha direktor Kengashi raisi

_____ O.X. Turakulov

2023 yil "__" _____

FAOLIYATNING TURLI TARMOQLARIDA AXBOROTNI HIMOYALASH TEXNOLOGIYALARI FAN DASTURI

Bilim sohasi:	**600000** – Axborot-kommunikatsiya texnologiyalari
Ta’lim sohasi:	**610000** – Axborot-kommunikasiya texnologiyalari
Ta’lim yo‘nalishi:	**70610302** – Axborot xavfsizligi (yo‘nalishlar bo‘yicha)

Fan dasturi O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligining 2021 yil 25-avgustdagi 365-sonli buyrug‘i bilan tasdiqlangan 70610302 – Axborot xavfsizligi (yo‘nalishlar bo‘yicha) ta’lim yo‘nalishi malaka talablari va ishchi o‘quv rejasiga muvofiq tayyorlandi.

Tuzuvchilar:

A.A.Abdumalikov — O‘zMUJF, “Kompyuter ilmlari va dasturlashtirish” kafedrasi v.b dotsenti.

Fan dasturi filial ilmiy-uslubiy Kengashida muhokama etildi va filial Kengashida muhokama etishga tavsiya qilindi (2023 - yil “21” iyundagi 11 - sonli bayonnoma).

O‘quv-ishlari bo‘yicha direktor o‘rinbosari: R.Abduraxmanov

Fan dasturi filial Kengashida muhokama etildi va foydalanishga tavsiya qilindi (2023 - yil “5” iyuldagi 11 - sonli bayonnoma).

Kengash kotibi: D. Soatova

Fan/modul kodi MISC2125	O‘quv yili 2023/2024	Semestr 2-semestr	ECTS Kreditlari 2-semestr - 5
Fan modul turi Tanlov	Ta’lim tili O‘zbek		Haftadagi dars soatlari 2-semestr - 4

	Fan nomi	Auditoriya mashg‘ulotlari soatlari	Mustaqil ta’lim soatlari	Jami
1	Faoliyatning turli tarmoqlarida axborotni himoyalash texnologiyalari	2-semestr – 60 soat	2-semestr – 90 soat	150

2 I. Fan mazmuni.

Fanni o‘qitishdan maqsad – talabalarda tashkilotning maxfiy ma'lumotlarini, muhim ma'lumotlarini va IT aktivlarini ruxsatsiz kirish, oshkor qilish, buzish, o'zgartirish yoki yo'q qilishdan himoya qilish haqida tushuncha hosil qilish, u ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlash uchun strategiyalar, protseduralar va ta’limdagi imkoniyatlari va amaliyotda qo‘llash usullari haqida nazariy va amaliy bilimlarni, ko‘nikma va malakalarni shakllantirishdan iborat.

II. Asosiy nazariy qism(Ma’ruza mashg‘ulotlari).

1-mavzu. Sog'liqni saqlashda kiberxavfsizlik: bemorlarning yozuvlari, tibbiy asboblar va nozik sog'liq ma'lumotlarini kiber tahdidlardan himoya qilish uchun texnologiyalarni o'rganish.

2-mavzu. Moliyaviy ma'lumotlarining xavfsizligi: bank va moliya sohasida moliyaviy operatsiyalar va mijozlar ma'lumotlarini himoya qilish uchun so'nggi shifrlash va autentifikatsiya usullarini tahlil qilish.

3-mavzu. Elektron tijorat maxfiylik yechimlari: Onlayn xaridorlarning maxfiyligini ta'minlash uchun xavfsiz to'lov shlyuzlari va ma'lumotlarni anonimlashtirish kabi strategiyalarni o'rganish.

4-mavzu. Sanoat nazorati tizimlari xavfsizligi: tajovuzni aniqlash tizimlari kabi texnologiyalardan foydalangan holda muhim infratuzilma va ishlab chiqarish jarayonlarini kiberhujumlardan himoya qilish choralarini o'rganish.

5-mavzu. Hukumat va mudofaa ma'lumotlarini himoya qilish: maxfiy ma'lumotlar va harbiy aloqalar uchun shifrlash, xavfsiz aloqa kanallari va tahdidlarni aniqlashni o'rganish.

6-mavzu. Ta'lim ma'lumotlarining maxfiyligi: talabalar ma'lumotlarini himoya qilish, xavfsiz onlayn ta'lim muhiti va ta'lim yozuvlariga ruxsatsiz kirishni oldini olish texnologiyalarini muhokama qilish.

7-mavzu. Chakana savdo sanoatida ma'lumotlar buzilishining oldini olish: chakana ma'lumotlar buzilishining oldini olish uchun savdo nuqtalari xavfsizligini, inventarizatsiyani boshqarish tizimlarini va mijozlar ma'lumotlarini himoya qilish mexanizmlarini tahlil qilish.

8-mavzu. Telekommunikatsiya tarmog'i xavfsizligi: Aloqa tarmoqlarini himoya qilish, tinglashning oldini olish va uzatilgan ma'lumotlarning

	yaxlitligini ta'minlash usullarini o'rganish. **9-mavzu.** Energiya infratuzilmasini himoya qilish: Elektr tarmoqlari va energetika ob'ektlarini kiber tahdidlardan himoya qilish uchun SCADA xavfsizligi va anomaliyalarni aniqlash kabi texnologiyalarni muhokama qilish. **10-mavzu.** Qishloq xo'jaligi texnologiyalari ma'lumotlar xavfsizligi: aniq qishloq xo'jaligi tizimlari, IoT qurilmalari va avtomatlashtirilgan qishloq xo'jaligi texnikasidan ma'lumotlarni himoya qilish choralarini o'rganish. **11-mavzu.** Transport tizimining kiberxavfsizligi: avtonom transport vositalarini, transport tarmoqlarini va harakatni boshqarish tizimlarini xakerlik va buzilishlardan himoya qilish uchun texnologiyalarni tahlil qilish. **12-mavzu.** Ko'ngilochar sanoat qaroqchiligining oldini olish: raqamli huquqlarni boshqarish (DRM) yechimlari va media kontentining ruxsatsiz tarqatilishining oldini olish uchun suv belgilarini qo'yish texnologiyalarini muhokama qilish. **13-mavzu.** Yuridik ma'lumotlarining maxfiyligi: mijoz va advokat o'rtasidagi xavfsiz aloqa platformalarini va yuridik hujjatlar va ish ma'lumotlari uchun ma'lumotlarni himoya qilish usullarini o'rganish. **14-mavzu.** Ko'chmas mulk tranzaksiyalari ma'lumotlarini himoya qilish: mulk operatsiyalari va nozik ko'chmas mulk ma'lumotlarining xavfsizligini ta'minlash uchun blokcheynga asoslangan echimlar va shifrlash usullarini tahlil qilish. **15-mavzu.** Notijorat tashkilot ma'lumotlarining maxfiyligi: donor ma'lumotlarini, benefitsiar ma'lumotlarini va notijorat tashkilotlarning operatsion ma'lumotlarini kiber tahdidlardan himoya qilish strategiyalarini muhokama qilish. III. Amaliy mashg‘ulotlar. 1-amaliy mashg‘ulot. Sog’liqni saqlashda kiberxavfsizlik. 2-amaliy mashg‘ulot. Moliyaviy ma'lumotlarining xavfsizligi. 3-amaliy mashg‘ulot. Elektron tijorat maxfiylik yechimlari. 4-amaliy mashg‘ulot. Sanoat nazorati tizimlari xavfsizligi. 5-amaliy mashg‘ulot. Hukumat va mudofaa ma'lumotlarini himoya qilish. 6-amaliy mashg‘ulot. Ta'lim ma'lumotlarining maxfiyligi. 7-amaliy mashg‘ulot. Chakana savdo sanoatida ma'lumotlar buzilishining oldini olish. 8-amaliy mashg‘ulot. Telekommunikatsiya tarmog'i xavfsizligi 9-amaliy mashg‘ulot. Energiya infratuzilmasini himoya qilish 10-amaliy mashg‘ulot. Qishloq xo'jaligi texnologiyalari ma'lumotlar xavfsizligi 11-amaliy mashg‘ulot. Transport tizimining kiberxavfsizligi. 12-amaliy mashg‘ulot. Ko'ngilochar sanoat qaroqchiligining oldini olish. 13-amaliy mashg‘ulot. Yuridik ma'lumotlarining maxfiyligi.

	14-amaliy mashg‘ulot. Ko'chmas mulk tranzaksiyalari ma'lumotlarini himoya qilish. 15-amaliy mashg‘ulot. Notijorat tashkilot ma'lumotlarining maxfiyligi. IV. Mustaqil ta’lim va mustaqil ishlar. Mustaqil ta’limining asosiy maqsadi – o‘qituvchining rahbarligi ostida berilganlarni intellektual tahlili sohasidagi an’anaviy va zamonaviy usullar haqida tasavvurga ega bo‘lishi, zarur holatlarda ularni qo‘llay olishi, turli sohaning amaliy masalalariga sun’iy intellekt usullarini, xususan berilganlarni intellektual tahlili usullarni qo‘llanishidan xabardor bo‘lishdan iborat. Magistrant mustaqil ishini tashkil etishda quyidagi shakllardan foydalaniladi: • ayrim nazariy mavzularni o‘quv adabiyotlari yordamida mustaqil o‘zlashtirish; • berilgan mavzular bo‘yicha intllektual tizimni bosqichma-bosqich loyihalash; • nazariy bilimlarni amaliyotda qo‘llash. Tavsiya etilayotgan mustaqil ishlarning mavzulari: 1. Ta'minot zanjiri xavfsizligi: soxtalashtirish va ruxsatsiz buzishning oldini olish uchun xom ashyo olishdan mahsulot yetkazib berishgacha bo'lgan ta'minot zanjirlarining yaxlitligi va xavfsizligini ta'minlaydigan texnologiyalarni o'rganish. 2. Media va jurnalistika kiberxavfsizlik: xakerlik va kuzatuvlar qarshisida jurnalistlar manbalari, raqamli kontent va aloqa kanallarini himoya qilish vositalari va texnologiyalarini muhokama qilish. 3. Atrof-muhit monitoringi ma'lumotlari xavfsizligi: iqlimni o'rganish va saqlash bo'yicha harakatlar uchun muhim ma'lumotlarni to'plash uchun ishlatiladigan atrof-muhit sensorlari va monitoring tizimlaridan ma'lumotlarni himoya qilish usullarini o'rganish. 4. Inson resurslari va xodimlar ma'lumotlarini himoya qilish: Shaxsiy ma'lumotlar o'g'irlanishi va ruxsatsiz kirishning oldini olish uchun xodimlarning yozuvlari, ish haqi ma'lumotlari va boshqa nozik HR ma'lumotlarini himoya qiluvchi texnologiyalarni tahlil qilish.
3	V. Fan o‘qitilishining natijalari. Mazkur fan bo‘yicha quyidagi o‘qitish shakllaridan foydalaniladi: - ma’ruzalar, amaliy mashg‘ulotlar (ma’lumotlar va texnologiyalarni anglab olish, aqliy qiziqishni rivojlantirish, nazariy bilimlarni mustahkamlash); - davra suhbatlari (ko‘rilayotgan loyiha yechimlari bo‘yicha taklif berish qobiliyatini oshirish, eshitish, idrok qilish va mantiqiy xulosalar chiqarish); - bahs va munozaralar (loyihalar yechimi bo‘yicha dalillar va asosli argumentlarni taqdim qilish, eshitish va muammolar yechimini topish qobiliyatini rivojlantirish)
4	VI. Ta’lim texnologiyalari va metodlari. - Ma’ruzalar;

	- Individual topshiriqlar; - Guruhlarda ishlash;
5	VII. Kredit olish uchun talablar. Fanga oid nazariy va uslubiy tushunchalarni to'la o'zlashtirish, kichik amaliy masalalarni yecha olish, mustaqil ravishda metodlar, strukturalar yarata olishi va joriy, oraliq nazorati shakllarida berilgan vazifa va topshiriqlarni bajarishi, yakuniy nazorat bo'yicha test/yozma ishlarni topshirish.
6	**Foydalangan adabiyotlar** 1.Диогенес Ю., Озкайя Э. Кибербезопасност: стратегии атак и оборони / пер. с анг. Д.А.Беликова. – М.: ДМК Пресс, 2020. – 326 с 2.Джеймс Куроуз, Кит Росс. Компьютерные сети: Нисходящий подход. -6-изд. – Москва: Издательсьтво "Э", 2016. **Internet saytlar** 1. http://edu.uz – O'zbekiston Respublikasi Oliy va o'rta maxsus ta'lim vazirligi 2. http:// www.mitc.uz - O'zbekiston Respublikasi axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi 3. http://lex.uz – O'zbekiston Respublikasi Qonun hujjatlari ma'lumotlari milliy bazasi 4. http://bimm.uz – Oliy ta'lim tizimi pedagog va rahbar kadrlarini qayta tayyorlash va ularning malakasini oshirishni tashkil etish bosh ilmiy-metodik markazi 5. http://ziyonet.uz – Ta'lim portali ZiyoNET
7	**Fan/modul uchun mas'ullar:** A.A.Abdumalikov – O'zMU Jizzax filiali, "Kompyuter ilmlari va dasturlashtirish" kafedrasi v.b. dotsenti
8	**Taqrizchilar:** Yusupov R.M. – JDPU, "Informatika va raqamli ta'lim texnologiyalari" kafedrasi mudiri, dotsent, t.f.n. Begbo'tayev A. – JDPU, "Informatika va raqamli ta'lim texnologiyalari" kafedrasi dotsenti, p.f.f.d. (PhD)