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

№ 1KO-70610302-39
2023-yil "5" 07

«TASDIQLANDI»
Filial Kengashi raisi
_____ O.X. Turakulov
2023-yil "___" _____

KIRISHGA RUXSATNI NAZORAT QILISHNING BIOMETRIK 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 MISC2215	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	
1	Fan nomi	Auditoriya mashg‘ulotlari soatlari	Mustaqil ta’lim soatlari	Jami
	Kirishga ruxsatni nazorat qilishning biometrik texnologiyalari	2-semestr – 60 soat	2-semestr – 90 soat	150
2	I. Fan mazmuni. **Fanni o`qitishdan maqsad** – kiberxavfsizlik usullari mazmunini, predmeti va metodi, uning maqsadi va vazifalari, kiberxavfsizlikni ta’minlashning asosiy tushunchalari, tahdidlari, hujum qilish usullari bilan tanishtirishdan iborat. II. Asosiy nazariy qism(Ma’ruza mashg‘ulotlari). **1-mavzu.** Kiberjinoyatchilik va kiberqonunlar **2-mavzu.** Kiberxavfsizlik arxitekturasi, strukturasi va siyosati. **3-mavzu.** Windows OT xavfsizligi. **4-mavzu.** Linux OT xavfsizligi **5-mavzu.** Kiberhujum turlari. **6-mavzu.** Kiberxavfsizlikning buzilishi. **7-mavzu.** Kritik kiberxavflar. **8-mavzu.** Zararli dasturlar turlari. **9-mavzu.** Social engineering. **10-mavzu.** Parollarga qarshi hujumlar va parollarni saqlash. **11-mavzu.** SQL injection. **12-mavzu.** XSS hujum **13-mavzu.** CSRF hujum **14-mavzu.** Web dasturlar xavfsizligi. **15-mavzu.** Bulutli texnologiyalar xavfsizligi. III. Amaliy mashg‘ulotlar. 1-amaliy mashg‘ulot. Kiberxavfsizlik asoslariga kirish Mamlakatimizda axborot xavfsizligiga oid qonunlar bilan tanishish. 2-amaliy mashg‘ulot. Kiberxavfsizlik arxitekturasi qurilishi, strukturasi tuzilishi va siyosati shakllantirilishi. Windows OT xavfsizligini ta’minlovchi prosessorlar bilan tanishish. 3-amaliy mashg‘ulot. Windows defender. Linux OT xavfsizligini taminlovchi skriptlar bilan ishlash. 4-amaliy mashg‘ulot. Windows va Linux OT xavfsizligini oshiruvchi kichik dasturlar. Password Attacks, Denial of Service Attacks, Passive Attack.			

	5-amaliy mashg‘ulot. Phishing, Identity Theft, Harassment, Cyberstalking. Kritik kiberxavflarni oldini olish. 6-amaliy mashg‘ulot. Social engineering. Hujum fazalari, odamlarni ishontirish, hujum turlarini oldindan olish. 7-amaliy mashg‘ulot. Lamport protokoli. SQL injection. XSS hujum 8-amaliy mashg‘ulot. CSRF hujum. SSL sertifikatlari. 9-amaliy mashg‘ulot. HTTP va HTTPS protokollari. Web brovzerlar xavfsizligi 10-amaliy mashg‘ulot. Xavfsizlik devorlari. Antivirus dasturlari. 11-amaliy mashg‘ulot. Kaspersky Security Cloud dasturi bilan ishlash. IoT texnologiyalari xavfsizligi. 12-amaliy mashg‘ulot. Ijtimoiy tarmoqda xavfsizlikni ta'minlash usullari. Mobil qurilmalar xavfsizligini taminlaydigan dasturlar. 13-amaliy mashg‘ulot. Ojizliklarni aniqlash. Umumiy zaifliklarni baholash tizimi. 14-amaliy mashg‘ulot. Zaiflikni skanerlash va sinovdan o‘tkazish. Kompyuter kriminalistikasi. 15-amaliy mashg‘ulot. Kompyuter kriminalistikasi uchun yo‘naltirilgan dasturlar. Kompyuter kriminalistikasi uchun vositalar va texnikalar. 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. API ga hujumlar. 2. Ma’lumotlar bazasiga hujum qilish. 3. Mobil ilovalarga hujumlar. 4. Kriptografiya. 5. Web serverlarga hujumlar.
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. S.K.Ganiyev A.A.Ganiyev, Z.T. Xudoyqulov: - “Kiberxavfsizlik asoslari” T-: “Iqtisod - Moliya”, 2020 y – 228 bet **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)