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»

Filial Kengashi raisi

O.X. Turakulov

2023-yil "__" _____

AXBOROT XAVFSIZLIGINI BOSHQARISH 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 MISC2115	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	Axborot xavfsizligini boshqarish	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. Axborot xavfsizligini boshqarishga kirish: axborot xavfsizligini boshqarish asoslari, maqsadlari va ahamiyati.

2-mavzu. Xavfsizlik siyosati, standartlari va tartiblari: Tashkilot uchun samarali xavfsizlik siyosati, standartlari va protseduralarini ishlab chiqish va amalga oshirish.

3-mavzu. Risklarni boshqarish va baholash: axborot xavfsizligiga xavflarni aniqlash, baholash va boshqarish.

4-mavzu. Xavfsizlikni boshqarish va muvofiqlik: axborot xavfsizligini boshqarish uchun asos yaratish va tegishli qoidalarga rioya qilishni ta'minlash.

5-mavzu. Xavfsizlik bo'yicha xabardorlik va trening: xodimlarni xavfsizlik bo'yicha ilg'or tajribalar haqida o'rgatish va xavfsizlik bo'yicha xabardorlik madaniyatini oshirish.

6-mavzu. Obro'ni himoya qilish: ma'lumotlarning buzilishi, kiberhujumlar va boshqa xavfsizlik hodisalarining oldini olish orqali tashkilot obro'sini himoya qilish.

7-mavzu. Biznes uzluksizligini qo'llab-quvvatlash: muhim biznes jarayonlari xavfsizlik hodisalari yoki uzilishlar yuz berganda ham davom etishini ta'minlash.

8-mavzu. Xavfsiz hamkorlikni yoqish: tashkilot ichida ham, tashqi hamkorlar bilan ham xavfsiz muloqot va hamkorlikni ta'minlash.

9-mavzu. Ma'lumotlar yo'qotilishining oldini olish: Ma'lumotlarning tasodifiy yoki qasddan yo'qolishi, o'g'irlanishi yoki sizib chiqishining oldini olish uchun chora-tadbirlarni amalga oshirish.

10-mavzu. Ishonchni shakllantirish: mijozlar, mijozlar va manfaatdor tomonlarga ularning ma'lumotlari ehtiyotkorlik va xavfsizlik bilan ishlanishini ko'rsatish.

	11-mavzu. Innovatsiyalarni qo'llab-quvvatlash: xavfsizlikni buzmasdan yangi texnologiyalar va innovatsiyalarni o'zlashtirish imkonini beruvchi xavfsiz muhitni yaratish. **12-mavzu. Xarajatlarni kamaytirish:** Xavfsizlik buzilishi va hodisalarining oldini olish tashkilotlarga bunday hodisalardan tiklanish bilan bog'liq moliyaviy va operatsion xarajatlardan qochishga yordam beradi. **13-mavzu. Voqealarga javob berish:** Xavfsizlik hodisalarini aniqlash, ularga javob berish va ularni tiklash uchun tizimli yondashuvga ega bo'lish. **14-mavzu. Xodimlarni o'qitish:** xodimlarga axborot xavfsizligini ta'minlashda ularning roli va mas'uliyati haqida o'rgatish orqali xavfsizlikni anglash madaniyatini oshirish. **15-mavzu. Tegishli sinchkovlikni ko'rsatish:** Tashkilot huquqiy va tartibga solish masalalarida muhim bo'lishi mumkin bo'lgan ma'lumotlarni himoya qilish bo'yicha o'z majburiyatlarini jiddiy qabul qilishini ko'rsatish. III. Amaliy mashg'ulotlar. 1-amaliy mashg'ulot. Xavfsizlik, konfidensiallik, integritet va mavjudlik tushunchalari. 2-amaliy mashg'ulot. Xavfsizlik sozlamalari, standartlari va tartibotlarni qo'llashning ahamiyati. 3-amaliy mashg'ulot. Xavfsizlik risklarini aniqlash, baholash va ularga qarshi maslahatlar. 4-amaliy mashg'ulot. Viruslar, trojanlar, ransomware kabi malware turlari va ularga qarshi himoya. 5-amaliy mashg'ulot. Firewalls, IDS, IPS, VPN kabi vositalar orqali tarmoq xavfsizligini saqlash. 6-amaliy mashg'ulot. Xavfsizlik sozlamalari orqali ma'lumotni o'zgartirishsiz yuborish. 7-amaliy mashg'ulot. Vulnerability assessment, penetraziya testlari va xavfsizlik skanerlari. 8-amaliy mashg'ulot. Foydalanuvchi kirishini boshqarish, parol yaratish va 2-faktor autentifikatsiya. 9-amaliy mashg'ulot. Iqtidorli xakkerlik va insandagi xavfsizlik taktikalarini tushuntirish. 10-amaliy mashg'ulot. Xavfsizlik insidentlarini aniqlash, boshqarish va ulardan tiklanish. 11-amaliy mashg'ulot. Xavfsizlikni tizim va dasturlar dizayni bilan ta'minlash. 12-amaliy mashg'ulot. Xavfsizlik sozlamalarini tekshirish va holatni monitoring qilish. 13-amaliy mashg'ulot. Xavfsizlikga oid huquqiy masalalar va global qonunchilik. 14-amaliy mashg'ulot. Xavfsizlik xaqida ishtirokchilar va xodimlarni ta'lim

	berish. 15-amaliy mashg'ulot. So'nggi xavfsizlik tashkilotlarini monitoring qilish va tahlil qilish. 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.Tashkiliy xavfsizlik qonunchiligi va standartlari, xavfsizlik sozlamalari va ularni amalga oshirish. 2. Ma'lumotni shifrlash va endi-to-end xavfsizlik tizimlarini o'rganish. 3. Foydalanuvchilarni boshqarish, parol yaratish, biometrik identifikatsiya va 2-faktor autentifikatsiya. 4. Tizim va dasturlarni xavfsizlikning tamoyillariga muvofiq dizayn qilish. 5. Xavfsizlikning o'ziga xos ma'nosini tushunish, xavfsizlik ta'limi va ishtirokchilarga o'rgatish.
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)