

Sharof Rashidov nomidagi Samarqand davlat universiteti intellektual tizimlar va kompyuter texnologiyalari fakulteti 70610202–Axborot xavfsizligi ta'lim yo'nalishlariga ishchi o'quv rejasidagi "Kiberhuquq va kiber etika" fanining sillabusiga

TAQRIZ

Ushbu fan sillabusi kiberhuquq va kiberetika sohasidagi talabalarni nazariy va amaliy bilimlar bilan ta'minlashga qaratilgan. Kiberhuquq — bu raqamli muhitda yuzaga keladigan huquqiy masalalarni tartibga soluvchi normativ-huquqiy me'yorlar to'plami, kiberetika esa axborot texnologiyalaridan foydalanishda axloqiy tamoyillarni o'rganadi. Ushbu fanni o'rganish, talabalarni zamonaviy kiber tahdidlarga, masalan, kiberhujumlar, ma'lumotlarni o'g'irlash va firibgarliklarga qarshi turishga tayyorlaydi.

Sillabusda belgilangan maqsadlar, talabalarni kiberhuquq va kiberetika asoslari bilan tanishtirib, ularni kiber muhitda xavfsizlikni ta'minlashga qaratilgan amaliy ko'nikmalar bilan qurollantirishdir. Talabalar shaxsiy va tijorat ma'lumotlarini himoya qilish, xavfsiz onlayn muhitda faoliyat yuritish va huquqiy me'yorlarga rioya qilishni o'rganadilar.

Fanning ma'ruzalarda tizimli tahlil, uning vazifalari, tamoyillari va tizimlar o'rtasidagi aloqalar o'rganiladi. Talabalar kiberhuquq va kiberetika doirasida turli tizimlar va ularning funktsiyalarini tahlil qilishni o'zlashtiradilar, bu esa ularning muammolarni hal etish qobiliyatini oshiradi.

Amaliy mashg'ulotlar davomida talabalar kiberhuquqiy standartlar, masalan, shaxsiy ma'lumotlarning himoyasi, mualliflik huquqi va kiberjinoychilikka qarshi qonunlarni o'rganadilar. Kiberetika doirasida esa axloqiy mas'uliyat, foydalanuvchi maxfiyligi va axloqiy qarorlar qabul qilishga e'tibor qaratiladi. Bu jarayonda xalqaro standartlar va amaliy vositalar o'rgatiladi.

Mustaqil ta'limning asosiy maqsadi talabalarni intellektual tahlil usullari bilan tanishtirish va ularni amaliy masalalarda qo'llashga tayyorlashdir. Talabalar o'qituvchining rahbarligi ostida nazariy bilimlarni mustaqil ravishda o'zlashtirish, intellektual tizimlarni loyihalash va amaliyotda qo'llash imkoniyatiga ega bo'ladilar.

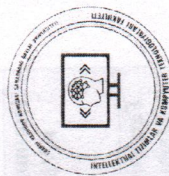
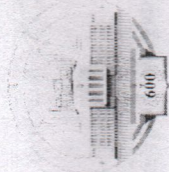
Ushbu fan sillabusi kiberhuquq va kiberetika sohasidagi muhim bilim va ko'nikmalarni o'z ichiga oladi. Talabalar nafaqat nazariy bilimlar, balki amaliy ko'nikmalarni ham o'zlashtirib, raqamli muhitda xavfsizlikni ta'minlashda o'zlarini tayyorlashlari mumkin. Shu sababli, ushbu ishchi fan sillabusini o'quv jarayonida foydalanish tavsiya etiladi.

TATU Samarqand filiali,
"Axborot texnologiyalari"
kafedrasining PhD, dotsenti

Z. Ibrohimova



O'ZBEKISTON RESPUBLIKASI OLIY
TA'LIM, FAN VA INNOVATSIYALAR
VAZIRLIGI



SHAROF RASHIDOV NOMLI

SAMARQAND DAVLAT

UNIVERSITETI

"FAN VA INNOVATSIYALAR"

KAFEDRASI

Ro'yxatga olindi:

№ DD-60610200

2024 yil "10" 02

2024 yil " "

R.I.Xalmuradov

Samarqand rektori

"FAN VA INNOVATSIYALAR"

KIBERHUQUQ VA KIBERETIKA

FAN DASTURI

Bilim sohasi:	600000 – Axborot kommunikatsion texnologiyalar
Ta'lim sohasi:	610 000 – Axborot kommunikatsion texnologiyalar
Ta'lim mutaxassisligi:	60610200 – Axborot xavfsizligi

Fan/modul kodlari	O'quv yili	Semestr	ECTS – Kreditlar
KVK1704	2027-2028	7	4
Fan/modul turi	Ta'lim tili	Haftadagi dars soatlari	
Majburiy fan	O'zbek	4	
1.	Fan nomi	Auditoriya mashg'ulotlari (soat)	Mustaqil ta'lim (soat)
	Innovatsiya va loyihalarni boshqarish	52	68
			120

Fanning maqsadi (FM)
1. Fanning mazmuni Kurs bakalavr darajasi uchun mo'ljallangan bo'lib, Fanni o'qitishdan maqsad talabalarga kiberxavfsizlikni ta'minlash sohasidagi xalqaro va milliy me'yoriy, nazariy va amaliy izlanishlar natijalari bilan tanishtirish hamda axborot tizimlarini, resurslarini himoyalangan texnologiya asosida qurish, himoyalagan axborotga nisbatan bo'ladigan taxdidlarga nisbatan zamonaviy yondashuvlarni hisobga olgan holda huquqiy tahlil qilishga doir bilimlar va ko'nikmalar hosil qilishdan iborat. Fanning vazifasi talabalarga nazariy bilimlar, amaliy ko'nikmalar, hamda kibermakonda huquq normalariga va kiberetikaning qoidalariga rioya qilgan holda axborotni himoyalashning ahamiyatini ochib berish.
2. FM

Fan mazmuni
II. Asosiy nazariy qism (ma'ruza mashg'ulotlari) II.1. Fan tarkibiga quyidagi mavzular kiradi: Mashg'ulotlar shakli: ma'ruza (M)
Kirish. Kiberhuquq va kiberetika fanining maqsadi va vazifalari. Kiberjinoyatchilik, kiberjinoyatchilik turlari, kiberetika, axborot erkinligi prinsiplari va kafolatlari. Axborotdan oqilona foydalanish kodeksi. Kiberhuquq va kiberetika. O'zbekiston Respublikasida kiberxavfsizlikni ta'minlashning asosiy yo'nalishlari. Kiberxavfsizlikni ta'minlash sohasidagi davlat siyosati. Axborotni himoyalash usullari. Huquqiy himoya. Tashkiliy himoya. Injener-texnik himoya.
Intelektual mulkga bo'lgan egalik huquqlari himoyasi. Intelektual mulk tushunchasi. Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma'lumotlar bazalarining huquqiy himoyasi to'g'risidagi qonunning mohiyati. Kompyuter dasturlariga mualliflik huquqlari. Xizmat faoliyatida yaratilgan asarlarga nisbatan mualliflik huquqi qoidalari. Kompyuter dasturlarini ro'yxatga olish. Dasturiy ta'minotga bo'lgan mualliflik
M1
M2

	huquqlarini himoya qilishning umumijahon konversiyasi va uning asosiy qoidalari
M3	Kompyuter xavfsizligi bilan bog'liq ahloqiy muammolar: hakerlik, haktivizm va konturhaking. Kompyuter xavfsizligini ta'minlashda bilan axloqiy muammolar va ularning yechimlari. Zamonaviy kiberjinoyatlarining ko'rinishlari va ularni kelib chiqish sabablari. Kiberxavfsizlikdagi yangi yo'nalishlar: haktivizm va konturhaking. Internet tarmog'ida siyosiy g'oyalarni tarqatish usullari. So'z erkinligi, internetdan foydalanishda inson huquqlari va axborot erkinligini himoya qilish, noqonuniy usullar yordamida kompyuter tarmoqlaridan foydalanish Ochiq kodli va bepul dasturiy vositalardan foydalanishdagi etik masalalar Internet tarmoqlari orqali ochiq dasturiy ta'minotlardan foydalanishning afzalliklari va kamchiliklari. Ochiq kodli dasturlar bilan bepul dasturiy vositalarning bir-biridan farqi. Ochiq kodli dasturiy vositalarning himoyalashning huquqiy asoslari. Kiberhuquqni ta'minlashda tashkilotlar faoliyatida foydalaniladigan ochiq kodli dasturlarni litsenziyalash tizimi, axborotni himoya qilish vositalarini sertifikatlash va axborot xavfsizligi talablari bo'yicha axborotlashtirish obektlarini attestatsiyasi, kadrlarni tayyorlash, maxsus aloqa tizimlari, ilmiy-tadqiqot va tajriba-konstruktorlik ishlarini tashkillashtirish tizimlari.
M4	Internet tadqiqotlar etikasi va uning muhim masalalari Internet tadqiqotlar etikasining kelib chiqish sabablari, asosiy tashkil etuvchilari va ularni ijtimoiy tarmoq foydalanuvchilari orasida ommalashtirish usullari. Internet etikasining rivojlanishida jamiyatda mintalitetlar turlicha ekanligi sababli yuzaga keladigan muammolari. Internen etikasining muhim masalalari.
M5	
M6	Kompyuter etikasi kodeksi. Axborotlashtirish subyektlari, axborot etikasi, kompyuter etikasi kodeksi, zamonaviy jamiyatda axborot munosabatlarning axloqiy me'yorlarga mosligi nuqtai nazaridan axborot xavfsizligini ta'minlash vazifalariga mosligi nuqtai nazaridan holati. Kibermojaro etikasi Raqamli oldini olish. Mutaxassislar o'rtasida kiberjang terminiga turlicha yondashishlar mavjudligi sabablari. Kibermojaro etikasining paydo bo'lishi va hozirda foydalanish omillari. AQSH, Buyuk Britaniya, Rossiya, Xitoy, Isroil, Eron, Shimoliy Koreya kabi bir qancha mamlakatlardagi mavjud kibermojarolar. Halqaro va mahalliy kibermojarolarning kelib ko'rinishdagi hujum turlaridan foydalanib jamiyatga zarar etkazishlarni chiqish sabablari.
M7	
M8	Kibermakonda axborot xavfsizligini ta'minlashda risklarni baxolash Kibermakonda axborot xavfsizligini ta'minlashda risk tushunchasi. ISO/IEC 27005:2008 «Information technology – Security techniques Information security risk management») xalkaro standarti. Menedjment jarayonida AX riski IB. Kontekstni belgilash, riskni baxolash, riskni kayta

	ishlash. Riskni kamaytirish. Riskni koldirish. Riskni oldini olish. Riskni ko'chirish. Risklarni qabul qilish
M9	Konfidensial axborotning turlari va darajalari bo'yicha klassifikatsiyasi Axborot tizimi, elektron resurs tushunchalari. Elektron resurslari kategoriyalari. Elektron resurslari va tizimlarini muxofaza qilish tartiblari. Davlat sirlari, tijorat sirlari muhofazasi, hujjatlarni maxfiylik darajasini belgilash va yuritish qoidalarini Kiberxavfsizlik buzg'unchisining gipotetik modeli. Buzg'unchining gipotetik modeli tushunchasi. Axborotni qayta ishlash texnologiyasidan foydalanadigan buzg'unchi modeli. Ichki va tashqi buzg'unchi. Buzg'unchini motivatsiyasi. Ma'suliyatsizlik, shaxsiy manfaatdorlik, yuqori malakaga ega ekanligini tasdiqlash. Axborot tizimiga oid bilimlari darajasiga ko'ra, imkoniyatlari qullaydigan usullari va vositalari bo'yicha. Sodir etish vaqi bo'yicha. Kiberxavfsizlikni ta'minlashning normativ-huquqiy asoslari. ISO / IEC 27001:2005 va ISO/IEC 17799:2005, ISO / IEC 15408-1-2005. "Axborot texnologiyalari. Xavfsizlikni ta'minlash metodlari. Axborot xavfsizligini boshqarish tizimlari. Talablar. Axborot xavfsizligini boshqarishning amaliy qoidalar. Axborot texnologiyalari xavfsizligini baholash mezonlari. AQSH Mudofaa Vazirligi (MV) kompyuter xavfsizligi "Ishonchli tizimlarning himoyalanganligini baholash mezonlari" standarti. Xavfsizlik darajalari, kafolatli himoya; ruxsatni tulq boshqarish; ruxsatni tanlash orqali boshqarish; minimal xavfsizlik tushunchalari. AQShning FIPS (Federal Information Processing Standards) standarti. Yevropa davlatlarining axborot xavfsizligini ta'minlashning uyg'unlashtirilgan mezonlari. Mezonlarda tizim va mahsulot tushunchasi. Umumiy mezonlarning yaratilishi.
M10	Kiberbulling (Cyber Bullying) Kiberbulling tushunchasi. Kiberbulling turlari. O'smir yoshdagilar paydo bo'lgan kiberbullingni zamonaviy ko'rinishlari. Kiberbullinga qarshi kurashish usullari va vositalari. Kiberbullingni jamiyatga ta'siri. Yoshlar ongini buzishdan himoyalash usullari. Internet foydalanuvchilarida milliy-madaniy etika koidalarni shakllantirish mexanizmlari.
M11	Kiber-texnologiyalar va ulardagi kiber etika masalalari Suniy intellekt va undagi kiber etika masalalari. Etika tamoyillariga bo'ysonuvchi suniy intellekt tushunchasi. Blokcheyn etikasi va uning mohiyati. Saylov tizimlaridagi blokcheyn texnologiyalari va undagi etika yondashuvlari. Blokcheyndagi anonimlik va xavfsizlik.
M12	Kiberbulling (Cyber Bullying) Kiberbulling tushunchasi. Kiberbulling turlari. O'smir yoshdagilar paydo bo'lgan kiberbullingni zamonaviy ko'rinishlari. Kiberbullinga qarshi kurashish usullari va vositalari. Kiberbullingni jamiyatga ta'siri. Yoshlar ongini buzishdan himoyalash usullari. Internet foydalanuvchilarida milliy-madaniy etika koidalarni shakllantirish mexanizmlari.
M13	Kiber-texnologiyalar va ulardagi kiber etika masalalari Suniy intellekt va undagi kiber etika masalalari. Etika tamoyillariga bo'ysonuvchi suniy intellekt tushunchasi. Blokcheyn etikasi va uning mohiyati. Saylov tizimlaridagi blokcheyn texnologiyalari va undagi etika yondashuvlari. Blokcheyndagi anonimlik va xavfsizlik.
III.	Amaliy mashg'ulotlar bo'yicha ko'rsatma va tavsiyalar: Amaliy (A) Amaliy mashg'ulotlar uchun quyidagi mavzular tavsiya etiladi.

A1.	O'zbekiston Respublikasida axborotlashtirish sohasidagi siyosatining asosiy yo'nalishlari
A2.	Kiberhuquq va kiberetika sohasida halqaro qonunchilik Kiberhuquq va kiberetika sohalari, internet va raqamli texnologiyalar rivojlanishi bilan birga o'sib bormoqda. Ushbu sohalar, axborot xavfsizligi, ma'lumotlarni himoya qilish, foydalanuvchi maxfiyligi va raqamli huquqlarni ta'minlashga qaratilgan xalqaro qonunchilikni o'z ichiga oladi
A3.	Intellectual mulk himoyasi. Elektron hisoblash mashinalari uchun yaratilgan dasturlarning mualliflik xuquqlarini himoya qilish aspektlari Intellectual mulk himoyasi, mualliflarning ijodiy ishlari, ixtirolari va innovatsiyalarini himoya qilish maqsadida tuzilgan qonunlar va qoidalar to'plamidir. Elektron hisoblash mashinalari uchun yaratilgan dasturlar, bu sohada muhim o'rin tutadi va ularga nisbatan mualliflik huquqlarini himoya qilish alohida e'tiborga molikdir
	Intellectual mulk himoyasi. Elektron hisoblash mashinalari uchun yaratilgan dasturlarning mualliflik xuquqlarini himoya qilish aspektlari Intellectual mulk himoyasi, ijodiy asarlarni va ixtirolarni himoya qilish maqsadida tuzilgan qonunlar va qoidalar to'plamidir. Elektron hisoblash mashinalari uchun yaratilgan dasturlar, bu sohada muhim o'rin tutadi va ularga nisbatan mualliflik huquqlarini himoya qilish bir qator jihatlarni o'z ichiga oladi
A4.	Kompyuter xavfsizligi bilan bog'liq ahloqiy muammolar va ularning turlari Kompyuter xavfsizligi bugungi kunda har qanday tashkilot va shaxs uchun muhim ahamiyatga ega. Ushbu sohada axloqiy muammolar ko'plab muammolarni keltirib chiqarishi mumkin. Quyida kompyuter xavfsizligi bilan bog'liq asosiy ahloqiy muammolar va ularning turlari keltirilgan
A5.	Windows operatsion tizimida tizim fayllari yaxlitligini tekshirish Windows operatsion tizimida tizim fayllarining yaxlitligini tekshirish, tizimning barqarorligini va xavfsizligini ta'minlash uchun muhimdir. Tizim fayllari, Windows tizimining normal ishlashi uchun zarur bo'lgan asosiy fayllardir. Ularning o'zgarishi yoki buzilishi tizimning ishlashiga salbiy ta'sir ko'rsatishi mumkin
A6.	Axborot kommunikatsion tizimlarda spamlar va ulardan himoyalash Spam — bu foydalanuvchilarga ruxsatsiz yuborilgan, ko'pincha reklamaviy yoki zararli bo'lgan xabarlar. Spam, asosan, elektron pochta,
A7.	

A8.	ijtimoiy tarmoqlar va boshqa axborot kommunikatsion tizimlarida uchraydi. Spam xabarlarining asosiy maqsadi foydalanuvchilarning e'tiborini jalb qilish, firibgarlik qilish yoki zararli dasturlarni tarqatishdir Axborot kommunikatsion tizimlarda spamlar va ulardan himoyalash Spam — bu foydalanuvchilarga ruxsatsiz yuborilgan, ko'pincha reklamaviy yoki zararli bo'lgan xabarlar. Spam, asosan, elektron pochta, ijtimoiy tarmoqlar va boshqa axborot kommunikatsion tizimlarida uchrab, foydalanuvchilarning e'tiborini jalb qilish yoki firibgarlik qilish maqsadida yuboriladi
A9.	Dasturiy ta'minot xavfsizligini ta'minlashda zaifliklar turlari Dasturiy ta'minot xavfsizligini ta'minlash uchun zaifliklarni aniqlash va ularni bartaraf etish muhimdir. Zaifliklar dasturiy ta'minotning ishlashida xavfsizlikka tahdid solishi mumkin Shadow Defender dasturini ishlash prinsiplarini o'rganish, dasturiy ta'minot xavfsizligini bajarish prinsiplari Dasturiy ta'minot xavfsizligini ta'minlash uchun zaifliklarni aniqlash va ularni bartaraf etish juda muhimdir. Zaifliklar dasturiy ta'minotning ishlashida xavfsizlikka tahdid solishi mumkin, bu esa ma'lumotlar o'g'irlanishi, tizimlar buzilishi yoki boshqa zararli harakatlarga olib kelishi mumkin. Quyida bu jarayonning ahamiyati va asosiy bosqichlari haqida ma'lumot berilgan
A10.	Ruxsatsiz nusxa ko'chirishdan himoya qilish dasturlari. Kompyuterning apparat vositalariga bog'lash dasturlari. Dasturiy yechimlar Ruxsatsiz nusxa ko'chirishdan himoya qilish dasturlari (DRM - Digital Rights Management) mualliflik huquqlarini himoya qilish va dasturiy ta'minotning noqonuniy tarqatilishining oldini olish uchun ishlatiladi.
A11.	Kiberbullinga qarshi kurashish usullari Kiberbullying — bu onlayn muhitda, masalan, ijtimoiy tarmoqlar, forumlar yoki boshqa raqamli platformalarda, boshqalarni haqorat qilish, ta'qib qilish yoki izza qilishdir. Kiberbullinga qarshi kurashish juda muhim va quyidagi usullarni o'z ichiga oladi
A12.	Shadow Defender dasturini ishlash prinsiplarini o'rganish, dasturiy ta'minot xavfsizligini bajarish prinsiplari Shadow Defender — bu kompyuter xavfsizligini ta'minlash va tizimni himoya qilish uchun mo'ljallangan dasturiy ta'minot. U foydalanuvchilarga xususiy va korporativ tizimlarni zararli dasturlardan, viruslardan va boshqa tahdidlardan himoya qilish imkonini beradi

IV. Mustaqil ta'lim va mustaqil ishlar

Mustaqil ta'lim uchun tavsiya etiladigan mavzular
“Innovatsiya va loyihalarni boshqarish” fani bo'yicha mustaqil ta'lim va ishlarining kalendar tematik rejas

N ^o	Mustaqil ta'lim mavzulari
1.	Kiberhuquq va kiberetika sohasida halqaro qonunchilik.
2.	Kiberhuquq va kiberetika sohasida Uzbekistan Respublikasi qonunchiligi
3.	Konfidensial axborotni himoyalashning huquqiy asoslari.
4.	Axborotlashtirish qoidalarini buzganlik uchun javobgarlik.
5.	Intelektual mulk himoyasi.
6.	Dasturiy ta'minot(DT) ishlab chiqaruvchilarning himoya turlari.
7.	Axborotni himoya qilish nazariyasining umummetodologik prinsiplari.
8.	Axborotni maxfiylik darajasiga qarab toifalash.
9.	Himoya usullarining, algoritmilarining, mexanizmlarining mustaxkamligi.
10.	Kiberxavfsizlikni huquqiy aspektlari.
11.	Dasturiy ta'minot xavfsizligini ta'minlashda zaifliklar turlari.
12.	DTni xavfsizligini ta'minlashning prinsiplari va taxdidlar modellari.
13.	DTni tarqatishda lisenziyalash va sertifikatlash.
14.	DTni ruxsat etilmagan o'zgartirishlardan himoyalash.
15.	Dasturlarni ishonchligini va butunligini ta'minlash kriptografik vositalari.
16.	Shartli bepul bo'lgan DT ni himoyalash usullari.
17.	Kiberhuquq sohasiga oid halqaro standartlar.
18.	Kiberhuquq sohasiga oid yevropa standartlari.
19.	Kiberhuquq sohasiga oid AQSh standartlari.
20.	Kiberhuquq sohasiga oid milliy standartlar.
21.	Kiberetikaning asosiy qoidalari va uning ahamiyati.
22.	Bulutli tizimlarda axborotni himoyalashning huquqiy ta'minlanganligi.
23.	Elektron to'lovlarini amalga oshirishning huquqiy asoslari.
24.	Texnik kanallarni kompleks himoya qilish tizimlari.

“Kiberhuquq va kibertika” fani bo'yicha mustaqil ta'lim mavzulari uning mazmunini yoritish maqsadida tanlangan va talabada shu haqida bilim ko'nikmasini shakllantirish nazarda tutilgan. Jumladan, innovatsiya va investitsiyalarni shakllantirish va yo'naltirish usullari va manbalarini, qishloqxo'jalik korxonalarining ichki xo'jalik faoliyati, ishlab chiqarishni va biznesini rejalashtirish; rejalashtirish tizimi, tamoyillari va tuzilish uslubini, investitsion loyihalarni ishlab chiqish, loyihaviy tahlil mohiyatini va usullarini; mahsulot (ishlar, xizmatlar)ni ishlab chiqarish va sotish xarajatlarini tarkibi hamda moliyaviy natijalarni shakllantirish tartibini; loyiha hujjatlarini ishlab chiqish, ekspertizadan o'tkazish va tasdiqlash tartibini; korxonalarida loyihaviy tahlil usullarini va xususiyatlarini, shuningdek kelajakda sarflanadigan investitsiyaning samaradorligini oshirish.

- Shu mazmunda MT da nazarda tutilgan mavzular haqida talabalar ish olib borishadi. Barcha keltirilgan mavzularni har biri to'g'risida talabalar qay tarzda

o'zlashtirish, bilim ko'nikmasiga ega bo'lish mexanizmi fanning sillabusida ochib beriladi.

-o'z ilmiy va amaliy faoliyatida mos tizimlardan foydalanish va rivojlantirishni;

- boshqaruv nazariyasi va amaliyotining so'ngi yutuqlarini qo'llagan holda korxona faoliyati va personalni boshqarish

3.	VI. Fan kompetensiyalar) Kiberjinoatchilik, kiberjinoatchilik turlari, kibernetika, axborot erkinligi prinsiplari va kafolatlari haqida tushunchaga ega bo'lishi kerak; Axborot urushining milliy xavfsizlikka tahdidi. Axborot urushi konsepsiyasi. Axborotli urush xususiyatlari. Axborot qurolini qo'llashning asosiy obyektlari haqida bilim ko'nikmalarga ega bo'lishi kerak; loyihalar xavfsizligi modellari qiyosiy tahlili qilish to'g'risida aniq malakalariga ega bo'lishi kerak. -o'z ilmiy va amaliy faoliyatida mos tizimlardan foydalanish va rivojlantirishni; - boshqaruv nazariyasi va amaliyotining so'ngi yutuqlarini qo'llagan holda korxona faoliyati va personalni boshqarish - zamonaviy axborot texnologiyalari tizimlarini yaratish va ulardan foydalanish bilan bog'liq ishlab chiqarish jarayonlari sifatini baholash va monitoringini o'tkazish usullari va mexanizmini ishlab chiqishni; - faoliyatni amalga oshirish, nazorat va uning bajarilish natijasi bo'yicha xulosa qila olish bo'yicha ish rejasini tuzish va bajarishni; - moddiy-texnik resurslarni yetkazib berish, servis xizmatlari ko'rsatish, ishlab chiqarilgan mahsulotlarni sotish bo'yicha shartnomalar tuzish va bajarilishini nazorat qilishni;	o'qitilishining natijalari (shakllanadigan)
4.	VII. Ta'lim texnologiyalari va metodlari: - ma'ruzalar; - interfaol keys-stadilar; - seminarlar (mantiqiy fikrlash, tezkor savol-javoblar); - guruhlarda ishlash; - taqdimotlar qilish; - individual loyihalar; - jamoa bo'lib ishlash va ximoya qilish uchun loyihalar. VII. Kreditni olish uchun talablar: Fanga oid nazariy va uslubiy tushunchalarni to'la o'zlashtirish, tahlil natijalarini tegishli to'g'ri aks ettira olish, o'rganilayotgan jarayonlar haqida mustaqil mushohada yuritish, amaliy mashg'ulotlarda berilgan masalalar dasturini tuzish va joriy, oraliq nazorat shakllarida berilgan vazifa va topshiriqlarni bajarish, yakuniy nazorat bo'yicha yozma ishini topshirish.	

6

Asosiy adabiyotlar:

1. M.Grabowski, E. Robinson, Cyber law and ethics, Taylor & Francis, 2022, London.

2. Ch. Stückelberger, P.Duggal, Cyber Ethics 4.0, Globethics.net, 2018, Geneva

Qo'shimcha adabiyotlar: 1. Stückelberger, Christoph, and Pavan Duggal. Cyber ethics 4.0: serving humanity 2. Kenneth Einar Himma and Herman T. Tavani, The Handbook of Information and Computer Ethics, 2017, P 706. 3. Шаныгин, В.Ф. Информационная безопасность и защита информации / М.: ДМК, 2014. - 702 с. Common Criteria for Information Technology Security Evaluation. Part III: Security Assurance Components [V Internet] // Common Criteria Portal.-2012 4. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013.-474 с. O'zbekiston Respublikasi Prezidentining 2002 yil 20 fevralda "Ilmiy tadqiqot faoliyatini tashkil etishni takomillashtirish to'g'risida"gi PF-3029-son Farmoni. Manba: www.lex.uz. 5. O'zbekiston Respublikasi Prezidentining 2006 yil 7 avgustdagi "Fan va texnologiyalar rivojlanishini muvofiqlashtirish va boshqarishni takomillashtirish chora-tadbirlari to'g'risida"gi PQ-436-son Qarori. Manba: www.lex.uz. 6. O'zbekiston Respublikasi Prezidentining 2008 yil 15 iyuldagi "Innovatsion loyihalar va texnologiyalarni ishlab chiqarishga" tatbiq etishni rag'batlantirish borasidagi qo'shimcha choratadbirlar to'g'risida"gi 916-Qarori. Manba: www.lex.uz. 7. http://vwm-help.net/lib/b/book/4177904444/19 8. http://www.pearsonitcertification.com/articles/article.aspx?p=1998558&seqNum=4 9. www.lex.uz – O'zbekiston Respublikasi Qonun xujjatlari ma'lumotlari milliy bazasi 10. www.library.tuit.uz – информационный портал ТУИТ 11. www.intuit.ru – основы информационной безопасности 12. www.gov.uz.- Hukumat portali.	Axborot manbalari (saytlar):
Fan dasturi Samarqand davlat universiteti O'quv-uslubiy kengashining 2024 yil " " dagi -son bayonnomasi bilan ma'qullangan.	Fan/modul uchun mas'ullar: J.S. Jabbarov – SamDU, "Boshqaruv nazariyasi va axborot xavfsizligi" kafedras mudiri, texnik fanlari bo'yicha falsafa doktori, PhD

A.A. Omonov – SamDU, “Boshqaruv nazariyasi va axborot xavfsizligi” kafedrası assistenti
Taqrizchilar:
O.Yusupov – texnika fanlari falsafa doktori, kafedra mudiri (tel:(97) 4412979)
Z. Ibroximova – TATU SF, texnika fanlari falsafa doktori, PhD.

Universitetning 2024-yil 16- avgustdagi 301-ij buyrug‘i asosida
Fan dasturlari va mustaqil ta‘lim topshiriqlarini ishlab chiqishga ma’sul ishchi
guruhi:

Rais

AP

Axatqulov S.

Kafedra mudiri

M.K.

M.K. Nurmatov

Fakultet dekani

F.M.

F.M. Nazarov

Sh. Rashidov nomidagi Samarqand davlat universiteti
O‘quv ishlariga mas’ul bo‘lgan yuqori prorektor:

A.S. Soliev



APB

Sharof Rashidov nomidagi Samarqand davlat universiteti Intellektual tizimlar va kompyuter texnologiyalari fakulteti 70610202–Axborot xavfsizligi ta’lim yo’nalishlariga ishchi o’quv rejasidagi “Kiberhuquq va kiber etika” fanining sillabusiga

TAQRIZ

Ushbu fan sillabusi kiberhuquq va kiberetika sohalarida talabalarni nazariy va amaliy bilimlar bilan ta'minlashga qaratilgan. Kiberhuquq — bu raqamli muhitda yuzaga keladigan huquqiy masalalarni tartibga soluvchi normativ-huquqiy me'yorlar to'plami, kiberetika esa axborot texnologiyalaridan foydalanishda axloqiy tamoyillarni o'rganadi. Ushbu fanni o'rganish, talabalarni zamonaviy kiber tahdidlarga, masalan, kiberhujumlar, ma'lumotlarni o'g'irlash va firtbgartiklarga qarshi turishga tayyorlaydi.

Sillabusda belgilangan maqsadlar, talabalarni kiberhuquq va kiberetika asoslari bilan tanishtirib, ularni kiber muhitda xavfsizlikni ta'minlashga qaratilgan amaliy ko'nikmalar bilan qurollantirishdir. Talabalar shaxsiy va tijorat ma'lumotlarini himoya qilish, xavfsiz onlayn muhitda faoliyat yuritish va huquqiy me'yorlarga rioya qilishni o'rganadilar.

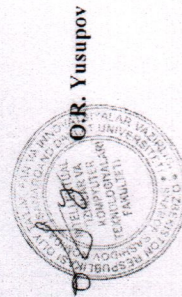
Fanning ma'ruzalari tizimli tahlil, uning vazifalari, tamoyillari va tizimlar o'rtasidagi aloqalar o'rganiladi. Talabalar kiberhuquq va kiberetika doirasida turli tizimlar va ularning funktsiyalarini tahlil qilishni o'zlashtiradilar, bu esa ularning muammolarni hal etish qobiliyatini oshiradi.

Amaliy mashg'ulotlar davomida talabalar kiberhuquqiy standartlar, masalan, shaxsiy ma'lumotlarning himoyasi, mualliflik huquqi va kiberjinoiyatchilikka qarshi qonunlarni o'rganadilar. Kiberetika doirasida esa axloqiy mas'uliyat, foydalanuvchi maxfiyligi va axloqiy qarorlar qabul qilishga e'tibor qaratiladi. Bu jarayonda xalqaro standartlar va amaliy vositalar o'rganiladi.

Mustaqil ta'limning asosiy maqsadi talabalarni intellektual tahlil usullari bilan tanishtirish va ularni amaliy masalalarda qo'llashga tayyorlashdir. Talabalar o'qituvchining rahbarligi ostida nazariy bilimlarni mustaqil ravishda o'zlashtirish, intellektual tizimlarni loyihalash va amaliyotda qo'llash imkoniyatiga ega bo'ladilar.

Ushbu fan sillabusi kiberhuquq va kiberetika sohalarida muhim bilim va ko'nikmalarni o'z ichiga oladi. Talabalar nafaqat nazariy bilimlar, balki amaliy ko'nikmalarni ham o'zlashtirib, raqamli muhitda xavfsizlikni ta'minlashda o'zlarini tayyorlashlari mumkin. Shu sababli, ushbu ishchi fan sillabusini o'quv jarayonida foydalanish tavsiya etiladi.

Sharof Rashidov nomidagi
Samarqand davlat universiteti,
“Dasturiy injiniring” kafedrası
mudiri PhD, dotsent



O.R. Yusupov