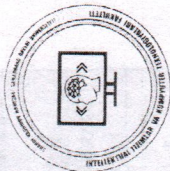


O'ZBEKISTON RESPUBLIKASI OLIY
TA'LIM, FAN VA INNOVATSIYALAR
VAZIRLIGI



SHAROF RASHIDOV NOMLI
SAMARQAND DAVLAT
UNIVERSITETI



Ro'yxatga olindi:

N^o 52-00610200

2024 yil "10" 02

Samarqand rektori

R.I.Xalmuradov

2024 yil " " "

RISKLARNI BOSHQARISH
FAN DASTURI

Bilim sohasi:

600000 – Axborot-kommunikatsiya texnologiyalari

Ta'lim sohasi:

610000 – Axborot-kommunikatsiya texnologiyalari

Ta'lim yo'nalishi:

60610200 – Axborot xavfsizligi

Fan/modul kodi	O'quv yili 2026-2027	Semestr 6	ECTS – Kreditlar 6
Fan/modul turi Tanlov fan	Ta'lim tili O'zbek	Haftadagi dars soatlari 4	
1.	Fan nomi	Auditoriya mashg'ulotlari (soat)	Jami (soat)
	Risklarni boshqarish	82	180
2.	I. Fanning mazmuni va maqsadi Fanni o'qitishdan maqsad – talabalarga axborot xavfsizligida risklarni boshqarishning nazariy va amaliy tamoyillarini o'rgatish, xalqaro standartlar, zamonaviy texnologiyalar, xavfsizlikni ta'minlash usullari bilan tanishtirishdan iborat. Fanning vazifasi – risklarni boshqarish fani talabalarining axborot xavfsizligi bo'yicha nazariy bilimlarini shakllantirish, xavflarni aniqlash va boshqarishning amaliy ko'nikmalarini rivojlantirish, xalqaro xavfsizlik standartlariga muvofiq xavfsizlik strategiyalarini ishlab chiqishni o'rgatishdir. Shuningdek, sun'iy intellekt, IDS tizimlari va xavfsizlik texnologiyalaridan foydalanish orqali axborot xavfsizligi muammolarini tahlil qilishni o'rgatish ham fanning asosiy vazifalari hisoblanadi. II. Asosiy nazariy qism (ma'ruza mashg'ulotlari) III.1. Fan tarkibiga quyidagi mavzular kiradi: Axborot xavfsizligida risklarni tahlil qilish, asosiy tamoyillar va yondashuvlar Axborot xavfsizligi xizmatining rivojlanishi va unda risklarni boshqarish tizimi Xalqaro axborot xavfsizligi standartlari va risklarni boshqarish Axborot xavfsizligidagi risklarni tahlil qilish texnologiyalari Axborot xavfsizligida risklarni aniqlash va baholash usullari Xatirlarni tahlil qilishning korporativ metodologiyasini ishlab chiqish Risklarni tahlil qilishda dasturiy vositalar Axborot xavfsizligini audit qilish COBIT standartiga muvofiq axborot xavfsizligi auditori: bosqichlar va usullar Axborot tizimlarining himoyalanganligini tahlil qilish Axborot tizimlarining tashqi perimetri himoyasi va uning tahlili Hujumlarni aniqlash va xavfsizlik tizimlari Tarmoq hujumlarini aniqlashning zamonaviy usullari va xavfsizlik boshqaruvi IDS tizimlari va ular orqali axborot xavfsizligi boshqaruvi Axborot xavfsizligi va risklarni boshqarishda sun'iy intellekt Axborot xavfsizligida bulutli texnologiyalarning roli		

Axborot xavfsizligini ta'minlashda kriptografik usullar Mobil qurilmalarda xavfsizlik risklarini boshqarish Axborot xavfsizligi infratuzilmasining himoyasi Tarmoq xavfsizligini ta'minlashning zamonaviy texnologiyalari va usullari Axborot xavfsizligida xavflarni prognozlash va ularni oldini olish strategiyalari III. Amaliy mashg'ulotlar bo'yicha ko'rsatma va tavsiyalar Amaliy mashg'ulotlari buyicha ko'rsatma va tavsiyalar Amaliy mashg'ulotlardan maqsad ma'ruza materiallari bo'yicha talabalarining bilim va ko'nikmalarini chuqurlashtirish va kengaytirishdan iborat. Risklarni boshqarish fani bo'yicha amaliy mashg'ulotlarning taxminiy tavsifi etiladigan mavzulari: Axborot xavfsizligidagi risklarni aniqlash: amaliy tadqiqot va tahlil Axborot xavfsizligi xizmatida xavflarni boshqarish jarayonini tashkil qilish Xalqaro standartlarga muvofiq xavfsizlik choralarini Axborot xavfsizligidagi risklarni tahlil qilishda amaliy texnologiyalarni qo'llash Risklarni baholashda statistik va ekspert baholash usullarini qo'llash Korporativ axborot xavfsizligi xatirlarini boshqarish strategiyalarini ishlab chiqish COBRA va CRAMM dasturlari yordamida xavfsizlik risklarini boshqarish Axborot xavfsizligi auditori bo'yicha amaliy audit jarayoni COBIT standartiga muvofiq audit amaliyoti tahlil qilish Axborot tizimlarining tashqi va ichki himoyasini baholash Tarmoq skanerlari yordamida xavfsizlikni baholash Tarmoq hujumlarini aniqlash va ular bilan bog'liq xavflarni boshqarish IDS tizimlarini sozlash va xavfsizlik boshqaruv tizimlarida ularni qo'llash Axborot xavfsizligida sun'iy intellektidan foydalangan holda xavf tahlili Sun'iy intellekt yordamida xatirlarni oldini olish usullari Axborot xavfsizligida raqamli imzo va sertifikatlarni qo'llash amaliyoti Axborot xavfsizligini ta'minlashda VPN texnologiyalarining amaliy qo'llanilishi Kriptografik vositalar yordamida axborot himoyasini ta'minlash: amaliy usullar Axborot xavfsizligida bulutli texnologiyalarning amaliy foydalanish yo'nalishlari Zaruriy xizmatlarni uzluksizligini ta'minlash va xatirlardan himoyalash usullari Mobil qurilmalarda xavfsizlik risklarini boshqarish va ularni amaliy baholash	3
--	---

Axborot xavfsizligi muammolarida muammolarni aniqlash va xavflarni boshqarish strategiyalari Amaliy mashg'ulotlar multimediy qurilmalari bilan jihozlangan auditoriyada bir akademik guruhga bir o'qituvchi tomonidan o'tkazilishi lozim. Mashg'ulotlar faol va interaktiv usullar yordamida o'tilishi, mos ravishda munosib pedagogik va axborot texnologiyalar qo'llanishi maqsadga muvofiq. Izoh: Ishchi dasturi shakllantirish jarayonida mazkur mashg'ulot turiga ishchi o'quv rejada ajratilgan soat hajmiga mos mavzular tanlab o'qitish tavsiya etiladi.	IV. Laboratoriya mashg'ulotlari bo'yicha ko'rsatma va tavsiyalar Laboratoriya mashg'ulotlardan maqsad talabalarining amaliyotda ko'rsatilgan va ishlangan dasturlarni o'zlarida amalda qo'llab ko'rish va bilim ko'nikmalarini chuqurlashtirish va kengaytirishdan iborat. IV.1. Risklarni boshqarish fani bo'yicha laboratoriya mashg'ulotlarining taxminiy tavsiya etiladigan mavzulari: Axborot xavfsizligi risklarini aniqlash va ularni dasturiy vositalar orqali tahlil qilish Risklarni baholashning korporativ tizimlarini qo'llanishini tahlil qilish COBRA dasturidan foydalangan holda xavf tahlil qilish va nazorat Axborot xavfsizligi auditing amaliy vositalarining imkoniyatlari Axborot tizimlari himoyasini audit qilish va ularning amaliy tahlili Skaner vositalari orqali axborot tizimlarining himoyasini tahlil qilish CRAMM metodologiyasi asosida xavfsizlikni boshqarish Tarmoq hujumlarini aniqlash va ularga qarshi chora ko'rish algoritmlarini yaratish IDS tizimlarini tarmoqda sozlash va ishlatish Sun'iy intellekt algoritmlaridan foydalangan holda tarmoq hujumlarini aniqlash Axborot xavfsizligi risklarini bashorat qilish va sun'iy intellekt yordamida boshqarish V. Mustaqil ta'lim va mustaqil ishlar Hozirgi davr mutaxassisidan yuqori darajadagi tayyorgarlik, mustaqil ravishda qarorlar qabul qila olish, belgilangan vazifalarni bajarish uchun ko'p ma'lumotlar orasidan kerakligini tanlab olish va bu ma'lumotlarni qayta ishlay olish talab qilinadi. Talabalarining mustaqil ta'limidan asosiy maqsadlar quyidagilardan iboratdir: • yangi bilim olish usullarini egallash, jarayonlarni mustaqil tahlil qila olish; • auditoriyadagi mashg'ulotlarda olgan bilimlarini mustahkamlash, chuqurlashtirish, kengaytirish va tartibga solish;
--	--

• ma'lumotlar va maxsus adabiyotlar bilan ishlashni o'rganish; • o'quv materiallarini mustaqil o'rganish. Mustaqil ta'lim uchun tavsiya etiladigan mavzular: Axborot xavfsizligida risklarni boshqarishning asosiy yondashuvlari Axborot xavfsizligini ta'minlashda zamonaviy hujumlarni aniqlash tizimlari Sun'iy intellektning axborot xavfsizligida qo'llanilishi va imkoniyatlari Axborot xavfsizligida xalqaro standartlar va ularning ahamiyati Korporativ axborot xavfsizligi tizimlari va ularni tahlil qilish Bulutli texnologiyalardagi xavfsizlik risklari va ularni boshqarish Mobil qurilmalarda axborot xavfsizligini ta'minlash usullari Kriptografiyaning axborot xavfsizligidagi roli va qo'llanilishi Tarmoq xavfsizligini ta'minlashda xavfsizlik devorlari va IDS tizimlari Axborot xavfsizligi infratuzilmasidagi yirik kompaniyalarning tajribasi Mustaqil o'zlashtiriladigan mavzular bo'yicha talabalar tomonidan referatlar tayyorlash va uni taqdimot qilish tavsiya etiladi.	3. VI. Fan o'qitilishining natijalari (shakllanadigan kompetensiyalar) Fanni o'zlashtirish natijasida talaba: • Axborot xavfsizligi bo'yicha nazariy bilimlar: Talabalar axborot xavfsizligining asosiy kontsepsiyalari va tamoyillarini chuqur o'rganib, xavflarni aniqlash va ularni boshqarishning nazariy asoslarini bilib olishadi. • Risklarni tahlil qilish va boshqarish kompetensiyasi: Axborot tizimlaridagi xavflarni aniqlash, ularni tahlil qilish va xavfsizlik choralarini ishlab chiqish ko'nikmalarini rivojlantiradilar. Talabalar xavfsizlik muammolarini aniqlash va ularga qarshi tegishli chora-tadbirlarni ishlab chiqishni o'rganadilar. • Axborot xavfsizligini ta'minlashning amaliy ko'nikmalari: Talabalar zamonaviy xavfsizlik texnologiyalari, kriptografiya usullari va tarmoq xavfsizligini ta'minlash bo'yicha amaliy bilim va ko'nikmalarga ega bo'lishadi. • Texnika va texnologik kompetensiyalar: Sun'iy intellekt, IDS tizimlari va boshqa zamonaviy texnologiyalar yordamida xavfsizlikni boshqarish bo'yicha texnik ko'nikmalarni shakllantiradilar. 4. VII. Ta'lim texnologiyalari va metodlari: • ma'ruzalar; • interfaol keys-stadilar; • seminarlar (mantiqiy fikrlash, tezkor savol-javoblar); • guruhlarda ishlash; • taqdimotlar qilish; 5.
---	--

	VIII. 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, oralik nazarot shakllarida berilgan vazifa va topshiriqlarni bajarish, yakuniy nazarot bo'yicha yozma ishini topshirish.
6.	IX. Asosiy adabiyotlar: 1. Peltier T. R. Information Security Risk Analysis / T. R. Peltier. – Second Edition. – Auerbach Publications, 2005. – 360 c. 2. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. - М.: Компания АйТи; ДМК Пресс, 2004. - 384 с.; ил. - (Информационные технологии для инженеров). 3. Abdullah Karasan. Machine Learning for Financial Risk Management with Python Algorithms for Modeling Risk. USA. 2022. -200p. 4. Варфоломеев А.А. Управление информационными рисками: Учеб. пособие. – М.: РУДН. 2008. – 158 с.; ил. Qo'shimcha adabiyotlar: 1. Melissa Jane Dark. Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives. Purdue University, USA. 2011. -307 p. 2. Р. А. Васильев. Управление информационной безопасностью. Нижегородский государственный лингвистический университет им. Н.А. Добролюбова (НГЛУ им. Н.А. Добролюбова), 2012. 3. Диогенес Ю., Озкая Э. "Кибербезопасность: стратегии атак и обороны" пер. с англ. Д. А. Беликова. - М.: ДМК Пресс, 2020. - 326 с.; ил. 4. S.K.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: o'quv qo'llanma. - T.: «Aloqachi», 2020, 303 bet. 5. Андреев Джейсон "Защита данных. От авторизации до аудита." — СПб.: Питер, 2021. — 272 с.; ил. Axborot manbalari (saytlar): 1. http://xaker.ru 2. https://www.gprc.ab.ca/files/coned/course/attachments 3. https://best-master.uz 4. https://www.cyberdegrees.org/resources/the-big-list/ 5. https://www.knowledgehut.com/blog/security/cyber-security-research-topics 6. https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them 7. https://us.norton.com/internetsecurity-how-to-7-most-important-cyber-security-topics-you-should-learn-about.html

	8. https://custom-writing.org/blog/cyber-security-topics-for-research 9. https://www.sciencedirect.com/topics/computer-science/cyber-security-research 10. https://www.elimucentre.com/cyber-security-research-topics/ 11. https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them 12. https://www.cyberdegrees.org/resources/the-big-list/ 13. https://cloudsecurityalliance.org/ 14. https://www.csiac.org/ 15. https://www.iotsecurityfoundation.org/
7.	Fan dasturi Samarqand davlat universiteti O'quv-uslubiy kengashining 2023 yil " " dagi -son bayonnomasi bilan ma'qullangan.
8.	Fan/modul uchun mas'ullar: M.R.Tojiyev – SamDU, "Kompyuter ilmlari va texnologiyalari fanlari" kafedrası dotsenti, texnika fanlari falsafa doktori
9.	Taqrizchilar: O. Yusupov – texnika fanlari falsafa doktori, (tel:(99)0636901) Z. Ibroximova – texnika fanlari falsafa doktori, PhD.

Rais:

S. Axatqulov

Kafedra mudiri:
Fakultet kengashi raisi:

M. Q. Nurmamatov

F.M.Nazarov

Kelishildi

O'quv ishlar bo'yicha prorektor:

A. Soliev



Sharof Rashidov nomidagi Samarqand davlat universiteti 60610200 –
Axborot xavfsizligi ishchi o'quv rejasidagi "Risklarni boshqarish" fanining
sillabusiga

TAQRIZ

Fanning maqsadi - talabalarga axborot xavfsizligida risklarni boshqarishning nazariy va amaliy tamoyillarini o'rgatish, xalqaro standartlar, zamonaviy texnologiyalar, xavfsizlikni ta'minlash usullari bilan tanishtirishdan iborat.

Ushbu ishchi o'quv dastur 60610200 – Axborot xavfsizligi yo'nalishining 3-bosqich kunduzgi ta'lim bakalavriat talabalari uchun "Risklarni boshqarish" fanining fan dasturi asosida ishlab chiqilgan.

Fan bo'yicha sillabusda o'quv fanining dolzarbligi va oliy kasbiy ta'limdagi o'rni, o'quv fanining maqsadi va vazifalari, ma'ruza, amaliy, laboratoriya va mustaqil ta'lim mavzulari, ularni tashkil etishning shakllari, fan bo'yicha talabalar bilimini baholash va nazorat qilish me'zonlari, foydalaniladigan asosiy va qo'shimcha o'quv adabiyotlar hamda axborot manbalari ro'yxati keltirilgan.

Fanning ma'ruza mashg'ulot mavzularida talabalar axborot xavfsizligi bo'yicha nazariy bilimlarini shakllantirish, xavflarni aniqlash va boshqarishning amaliy ko'nikmalarini rivojlantirish, xalqaro xavfsizlik standartlariga muvofiq xavfsizlik strategiyalarini ishlab chiqish tushuntirib o'tilgan.

Amaliyot qismida esa tibbiy axborotlarni uzatish standarti ISO 13606 asosida tibbiy statistik ma'lumotlarni yig'ish va taxlillash tizimlari.

Yuqorida keltirilganlarni hisobga olib, ushbu ishchi fan sillabusini o'quv jarayonida foydalanish uchun tavsiya qilaman.

Sharof Rashidov nomidagi
Samarqand davlat universiteti,
"Dasturiy injiniring" kafedrasi
mudiri PhD, dotsent



O.R. Yusupov

Sharof Rashidov nomidagi Samarqand davlat universiteti 60610200 –
Axborot xavfsizligi ishchi o'quv rejasidagi "Risklarni boshqarish" fanining
sillabusiga

TAQRIZ

Fanning maqsadi - talabalarga axborot xavfsizligida risklarni boshqarishning nazariy va amaliy tamoyillarini o'rgatish, xalqaro standartlar, zamonaviy texnologiyalar, xavfsizlikni ta'minlash usullari bilan tanishtirishdan iborat.

Ushbu ishchi o'quv dastur 60610200 – Axborot xavfsizligi yo'nalishining 3-bosqich kunduzgi ta'lim bakalavriat talabalari uchun "Risklarni boshqarish" fanining fan dasturi asosida ishlab chiqilgan.

Fan bo'yicha sillabusda o'quv fanining dolzarbligi va oliy kasbiy ta'limdagi o'rni, o'quv fanining maqsadi va vazifalari, ma'ruza, amaliy, laboratoriya va mustaqil ta'lim mavzulari, ularni tashkil etishning shakllari, fan bo'yicha talabalar bilimini baholash va nazorat qilish me'zonlari, foydalaniladigan asosiy va qo'shimcha o'quv adabiyotlar hamda axborot manbalari ro'yxati keltirilgan.

Fanning ma'ruza mashg'ulot mavzularida talabalar axborot xavfsizligi bo'yicha nazariy bilimlarini shakllantirish, xavflarni aniqlash va boshqarishning amaliy ko'nikmalarini rivojlantirish, xalqaro xavfsizlik standartlariga muvofiq xavfsizlik strategiyalarini ishlab chiqish tushuntirib o'tilgan.

Amaliyot qismida esa tibbiy axborotlarni uzatish standarti ISO 13606 asosida tibbiy statistik ma'lumotlarni yig'ish va taxlillash tizimlari.

Yuqorida keltirilganlarni hisobga olib, ushbu ishchi fan sillabusini o'quv jarayonida foydalanish uchun tavsiya qilaman.

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



Z. Ibrohimova