

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



SHAROF RASHIDOV NOMLI
SAMARQAND DAVLAT
UNIVERSITETI



Ro'yxatga olindi:

№ DD-60610-2-4-5

2024 yil "10" 02

Samarqand rektori

R.I.Xalmuradov

2024 yil " " "

KIBERXAVFSIZLIK ASOSLARI

FAN DASTURI

Bilim sohasi:

600000 – Axborot-kommunikatsiya
texnologiyalari

Ta'lim sohasi:

610000 – Axborot-kommunikatsiya
texnologiyalari

Ta'lim yo'nalishi:

60610100 – Axborot tizimlar va
texnologiyalari

60610200 – Axborot xavfsizligi

60610400 – Daturiy injiniring

60610500 – Sun'iy intellekt

Fan/modul kodi	O'quv yili 2025-2026	Semestr 4	ECTS – Kreditlar 6
Fan/modul turi	Ta'lim tili O'zbek	Haftadagi dars soatlari 4	
1.	Fan nomi	Auditoriya mashg'ulotlari (soat)	Jami (soat)
	Kiberxavfsizlik asoslari	82	180
2.	I. Fanning mazmuni va maqsadi 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. Fanning vazifasi – Kiberxavfsizlik fanining maqsadi raqamli tizimlar, tarmoqlar va ma'lumotlarni ruxsatsiz kirish, kiberhujumlar va potentsial tahdidlardan himoya qilish uchun texnikalar, strategiyalar va texnologiyalarni o'rganish, ishlab chiqish va amalga oshirishdan iborat. U jismoniy shaxslarni, tashkilotlarni va jamiyatlarni turli kiberxavflardan himoya qilishga, raqamli sohadagi ma'lumotlar va resurslarning maxfiyligi, yaxlitligi va mavjudligini ta'minlashga qaratilgan. Kiberxavfsizliklar, zaifliklar va ularni yumshatish usullarini tushunish orqali kiberxavfsizlik fani barcha foydalanuvchilar uchun ishonchliroq va xavfsizroq onlayn muhitni yaratishga qaratilgan. II. Asosiy nazariy qism (ma'ruza mashg'ulotlari) II.1. Fan tarkibiga quyidagi mavzular kiradi: Kiberjinoatchilik va kiberqonunlar. Kiberxavfsizlik arxitekturasini, strategiyasi va siyosati. Kompyuter hodisalariga javob qaytarish jarayoni. Razvedka va ma'lumotlarni to'plash Tizimlarga bo'ladigan xujumlar Foydalanuvchi rekvizitlariga xujum qilish. Tizimga kirgandan keyingi xarakatlar. Xavfsizlik siyosati. Tarmoqni segmentlarga ajratish. Aktiv sensorlar. Kiberrazvedka. Ojizliklarni boshqarish. Jurnallar analizi. IoT qurilmalar havfsizligi. Mobil qurilmalar havfsizligi. 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 talabalarning bilim va ko'nikmalarini chuqurlashtirish va kengaytirishdan iborat. Kiberxavfsizlik asoslari fani bo'yicha amaliy mashg'ulotlarning taxminiy tavsiya etiladigan mavzulari: Virtual mashinada labalatoriyada ishlash muhitini yaratish. Windows OT jarayonlari bilan tanishish. Protoses Explorer. Linux OT jarayonlari bilan tanishish. Hodisalariga javob qaytarish jamoasini shakllantirish. Ro'y bergan hodisalarni o'rganish. Hujumlar senaryolarini o'rganish. CMD, Powershell bilan ishlash. Buryurlar bilan tanishish. Bash Nmap, Metasploit, John the Ripper, THC Hydra, Wireshark. dasturlari bioan tanishish. Aircrack-ng, Nikto, Kismet, Cain and Abel dasturlari bioan tanishish. Tashqi razvetka usullari. Ijtimoiy tarmoqlardan ma'lumotlar yig'ish usullari. Sotsial injinera usullari. Google dorks. Fishing. Ichki razvedka usullari. Prisdump, tepdump, Scanrand dasturlari bilan tanishish. Varddrayving metodi bilan tanishish. IDA PRO dasturi bilan ishlash. Kon-Bootv a Hiren's BootCD dasturini ishlatib korish. Nessus dasturi bilan oqizliklar qidirish. Virtual mashinada Cobalt Strike dasturini sinab ko'rish. Pass-The-Hash Toolkit dasturi bian ishlash. Social-Engineer Toolkit dasturi bian ishlash. Sysntemals paketidagi Psexec utilitasidan foydalanish. Tizimga kirgandan keyingi huqulami oshirish. Mimikatz dasturi bilan ishlash. Axborot xavfsizligi siyosatini tuzish. Windows 8 da Power Shell va Meterpreter orqali huqumi oshirish. Axborot xavfsizligi siyosatini tuzish. Axborot xavfsizligi siyosatini to'g'ri yo'lga qo'yish. Tashkilot foydalanuvchilariga treninglarni tashkil qilish. Fizik tarmoqni segmentlarga ajratish. Suricata tizimi bilan tanishish. Ochiq kodli kiberrazvedkani amalga oshiradigan dasturi ar. Belka Soft dasturi bilan tanishish. PassMark OSForensics dasturi bilan tanishish. Amaliy mashg'ulotlar multimeidiya 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.	3
---	---

IV. Laboratoriya mashg'ulotlari buyicha ko'rsatma va tavsiyalar Laboratoriya mashg'ulotlardan maqsad talabalarining amaliyotda ko'rsatilgan va ishlangan dasturlarni o'zlarida amalga qo'llab qo'yish va bilim ko'nikmalarini chuqurlashtirish va kengaytirishdan iborat. IV.1. Kiberxavfsizlik fani bo'yicha laboratoriya mashg'ulotlarining taxminiy tavsifiy etiladigan mavzulari: Virtual mashinada laboratoriyada ishlash muhitini yaratish. Windows OT jarayonlari bilan tanishish. Protoses Explorer. Linux OT jarayonlari bilan tanishish. Hodisalariga javob qaytarish jarayonini shakllantirish. Ro'y bergan hodisalarni o'rganish. Hujumlar senaryolarini o'rganish. CMD, Powershell bilan ishlash. Buryurlar bilan tanishish. Bash Nmap, Metasploit, John the Ripper, THC Hydra, Wireshark, dasturlari bilan tanishish. Aircrack-ng, Nikto, Kismet, Cain and Abel dasturlari bilan tanishish. Tashqi razvetka usullari. Ijtimoiy tarmoqlardan ma'lumotlar yig'ish usullari. Sotsial injinieriya usullari. Google dorks, Fishing. Ichki razvedka usullari. Prisdump, tcpdump, Scandump dasturlari bilan tanishish. Varddrayving metodi bilan tanishish. IDA PRO dasturi bilan ishlash. Kon-Boot va Hiren's BootCD dasturini ishlatib ko'rish. Nessus dasturi bilan o'qitilish. Virtual mashinada Cobalt Strike dasturini sinab ko'rish. Pass-The-Hash Toolkit dasturi bilan ishlash. Social-Engineer Toolkit dasturi bilan ishlash. Sysinternals paketidagi PsExec utilitasidan foydalanish. Tizimga kirgandan keyingi huquqlarni oshirish. Mimikatz dasturi bilan ishlash. Axborot xavfsizligi siyosatini tuzish. Windows 8 da Power Shell va Meterpreter orqali huquqlarni oshirish. Axborot xavfsizligi siyosatini tuzish. Axborot xavfsizligi siyosatini to'g'ri yo'lga qo'yish. Tashkilot foydalanuvchilariga treninglarni tashkil qilish. Fizik tarmoqni segmentlarga ajratish. Suricata tizimi bilan tanishish. Ochiq kodli kibernetika amaliyotiga oshiradigan dasturlar. Belka Soft dasturi bilan tanishish. PassMark OSForensics dasturi bilan tanishish. Tizimni qayta tiklash jarayoni rejasini tuzish qadamlari. Nessus va Secunia Personal Software Inspector dasturi bilan tanishish. Dump fayllar bilan ishlash. Jumallarni analiz qilishni o'rganish. Barmoq izlari orqali parollarni olish.	
---	--

UART va SWD orqali IoT ni buzish APK dasturlarini analiz qilish. Android XploitSpy dasturi bilan tanishish. 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 ishlash talab qilinadi. Talabalarining mustaqil ta'limdan 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: Tashqi resurslardan ma'lumotlar yig'ish; Kriptografiya; OWASP TOP 10 xujumlar bilan tanishish; Kodachi OT o'rganish; C2 platformalari bilan ishlash; Kali Linux OT o'rganish; API ga xujumlar; Malumotlar bazasiga xujum qilish; Ijtimoiy muhandislik; Veb serverlarga xujumlar; Intemetda anonimlikni ta'minlash. 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: • "Kiberxavfsizlik asoslari" fanini o'zlashtirish jarayonida amalga oshiriladigan masalalar doirasida kiberxavfsizlik haqida tasavvur va bilimga ega bo'lishi; • Axborot xavfsizligi sohasidagi tahdidlarni amalga oshirish, kiberhujum dasturlarini amalda qo'llash ko'nikmalariga ega bo'lishi; • Axborot tizimiga xujum qilish usul va yo'riqlaridan foydalanishni tadbir etib bilish va axborot tizimi himoyasini tashkil etish yo'llarini
--	---

	bilish va zarur xavfsizlik dasturlarni ishlatish malakasiga ega bo'lishi kerak.
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, oraliq nazarot shakllarida berilgan vazifa va topshiriqlarni bajarish, yakuniy nazarot bo'yicha yozma ishini topshirish.
6.	IX. Asosiy adabiyotlar: 1. Диогенес Ю., Озкая Э. "Кибербезопасность: стратегии атак и обороны" / пер. с англ. Д. А. Беликова. - М.: ДМК Пресс, 2020. - 326 с.: ил. 2. S.K. Ganiyev, A.A. Ganiyev, Z.T. Xudoyqulov. Kiberxavfsizlik asoslari: o'quv qo'llanma. - T.: «Aloqachi», 2020. 303 bet. 3. Андреев Джейсон "Защита данных. От авторизации до аудита." — СПб.: Питер, 2021. — 272 с.: ил. Qo'shimcha adabiyotlar: 4. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли "Kali Linux. Тестирование на проникновение и безопасность." - СПб.: Питер, 2020. 448 с.: ил. 5. Тронкон Пол, Олбинг Карл "Bash и кибербезопасность: атака, защита и анализ из командной строки Linux." С СПб.: Питер, 2020. — 288 с.: ил. 6. Эрикссон Д. Хакнинг: искусство эксплуатации. 2-е изд. - СПб.: Питер, 2018. - 496 с.: ил. 7. Джо Грей "Социальная инженерия и этичный хакинг на практике" / пер. с англ В. С. Яценкова. - М.: ДМК Пресс, 2023. - 226 с.: ил. 8. Python глазами хакера. - СПб.: БХВ-Петербург, 2022. - 176 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.esiac.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" kafedrasida dotsenti, texnika fanlari falsafa doktori
9.	Taqrizchilar: F.Nazarov – texnika fanlari falsafa doktori, fakultet dekani (tel:(99)0636901) Z. Ibroximova – TATU, texnika fanlari falsafa doktori, PhD.

Rais

Kafedra mudiri:

S. Axatqulov

Fakultet kengashi raisi:

Q.M. Nurmamatov

Kelishildi

O'quv ishlar bo'yicha prorektor:

F.M.Nazarov

A. Soleev



Sharof Rashidov nomidagi Samarqand davlat universiteti Intellektual tizimlar va kompyuter texnologiyalari fakulteti 60610100-Axb tiz va tex, 60610200-Axborot xavfsizligi, 60610400-Dasturiy injiniring, 60610500-Sun'iy intellekt ta'lim yo'nalishlariga ishchi o'quv rejasidagi "Elektron tijorat xavfsizligi" fanining sillabusiga

TAQRIZ

Ushbu fan sillabusi kibernetika sohasida talabalarni nazariy va amaliy bilimlar bilan ta'minlashga qaratilgan. Kibernetika — bu axborot tizimlari, ma'lumotlar va tarmoqlarni kiber tashvirlardan himoya qilish jarayonidir. Ushbu fanni o'rganish orqali talabalar zamonaviy kiber tashvirlarga, masalan, kibernetika, zararli dasturlar va ma'lumotlarni o'g'irlashga qarshi samarali choralarini qo'llashni o'rganadilar.

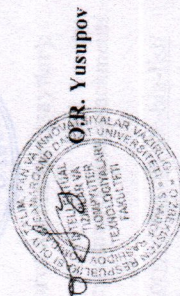
Sillabusda belgilangan maqsadlar, talabalarni kibernetika sohasidagi asosiy bilimlari, himoya usullari va kiber tashvirlarga qarshi kurashish strategiyalari bilan tanishtirishdan iborat. Talabalar kibernetika sohasidagi muhim jihatlarni, jumladan, shaxsiy va tijorat ma'lumotlarini himoya qilish, xavfsiz tarmoqlarni yaratish va xavfsizlik standartlariga rioya qilishni o'rganadilar. Fanning ma'lumotlarida tizimli tahlil, uning vazifalari, tamoyillari va tizimlar o'rtasidagi aloqalar o'rganiladi. Talabalar kibernetika sohasidagi doirasida turli tizimlar va ularning funktsiyalarini tahlil qilishni o'rganadilar, bu esa ularning muammolarni hal etish qobiliyatini oshiradi.

Amaliy mashg'ulotlar davomida talabalar kibernetika protokollari, xavfsiz to'lov tizimlari, shifrlash usullari va ma'lumotlar himoyasi haqida chuqur bilim olish imkoniyatiga ega bo'ladi. Ular kiber tashvirlarga qarshi real muammolarni hal qilishda amaliy ko'nikmalarni shakllantiradilar. Xavfsizlik standartlari va me'yorlarga rioya qilish jarayoni ham muvaffaqiyatli bo'ladi.

Mustaqil ta'limning asosiy maqsadi talabalarni zamonaviy kibernetika strategiyalari bo'yicha tadqiqotlar olib borishga va ulardan amaliy masalalarda foydalanishga tayyorlashdir. Talabalar o'qituvchining rahbarligi ostida nazariy bilimlarni mustaqil ravishda o'zlashtirish, kibernetika tizimlarini loyihalash va amaliyotda qo'llash imkoniyatiga ega bo'ladi.

Ushbu fan sillabusi kibernetika sohasida 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" kafedrasi
mudiri PhD, dotsent



Sharof Rashidov nomidagi Samarqand davlat universiteti Intellektual tizimlar va kompyuter texnologiyalari fakulteti 60610100-Axb tiz va tex, 60610200-Axborot xavfsizligi, 60610400-Dasturiy injiniring, 60610500-Sun'iy intellekt ta'lim yo'nalishlariga ishchi o'quv rejasidagi "Elektron tijorat xavfsizligi" fanining sillabusiga

TAQRIZ

Ushbu fan sillabusi kibernetika sohasida talabalarni nazariy va amaliy bilimlar bilan ta'minlashga qaratilgan. Kibernetika — bu axborot tizimlari, ma'lumotlar va tarmoqlarni kiber tashvirlardan himoya qilish jarayonidir. Ushbu fanni o'rganish orqali talabalar zamonaviy kiber tashvirlarga, masalan, kibernetika, zararli dasturlar va ma'lumotlarni o'g'irlashga qarshi samarali choralarini qo'llashni o'rganadilar.

Sillabusda belgilangan maqsadlar, talabalarni kibernetika sohasidagi asosiy bilimlari, himoya usullari va kiber tashvirlarga qarshi kurashish strategiyalari bilan tanishtirishdan iborat. Talabalar kibernetika sohasidagi muhim jihatlarni, jumladan, shaxsiy va tijorat ma'lumotlarini himoya qilish, xavfsiz tarmoqlarni yaratish va xavfsizlik standartlariga rioya qilishni o'rganadilar. Fanning ma'lumotlarida tizimli tahlil, uning vazifalari, tamoyillari va tizimlar o'rtasidagi aloqalar o'rganiladi. Talabalar kibernetika sohasidagi doirasida turli tizimlar va ularning funktsiyalarini tahlil qilishni o'rganadilar, bu esa ularning muammolarni hal etish qobiliyatini oshiradi.

Amaliy mashg'ulotlar davomida talabalar kibernetika protokollari, xavfsiz to'lov tizimlari, shifrlash usullari va ma'lumotlar himoyasi haqida chuqur bilim olish imkoniyatiga ega bo'ladi. Ular kiber tashvirlarga qarshi real muammolarni hal qilishda amaliy ko'nikmalarni shakllantiradilar. Xavfsizlik standartlari va me'yorlarga rioya qilish jarayoni ham muvaffaqiyatli bo'ladi.

Mustaqil ta'limning asosiy maqsadi talabalarni zamonaviy kibernetika strategiyalari bo'yicha tadqiqotlar olib borishga va ulardan amaliy masalalarda foydalanishga tayyorlashdir. Talabalar o'qituvchining rahbarligi ostida nazariy bilimlarni mustaqil ravishda o'zlashtirish, kibernetika tizimlarini loyihalash va amaliyotda qo'llash imkoniyatiga ega bo'ladi.

Ushbu fan sillabusi kibernetika sohasida 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"
kafedrasi PhD, dotsent



Z. Ibrohimova