

**O'ZBEKISTON RESPUBLIKASI
OLIY TA'LIM, FAN VA
INNOVATSIYALAR VAZIRLIGI
SHAROF RASHIDOV NOMIDAGI
SAMARQAND DAVLAT
UNIVERSITETI
INTELLEKTUAL TIZIMLAR VA
KOMPYUTER
TEXNOLOGIYALARI FAKULTETI**



Ro'yxatga olindi:
№ 58-60610-200
2024 yil "10" 16



"TASDIQLAYMAN"

SamDU rektori:

R.I.Xalmuradov

2024 yil " " "

**TARMOQ XAVFSIZLIGI
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 TAXI506		O'quv yili 2026 -2027	Semestr 5	ECTS – Kreditlar 6	
Fan/modul turi Majburiy		Ta'lim tili O'zbek		Haftadagi dars soatlari 8	
1.	Fan nomi	Auditoriya mashg'ulotlari (soat)		Mustaqil ta'lim (soat)	Umumiy (soat)
	Tarmoq xavfsizligi	78		102	180

Fanning maqsadi (FM)

FM1	I. FANNING MAZMUNI Fanni o'qitishdan maqsad – talabalarda bu fandagi asosiy maqsad talabalarga axborot tizimlari va tarmoqlarni turli xavflardan himoya qilish uchun zarur bo'lgan bilim va ko'nikmalarni shakllantirishdir. Bu fan orqali o'quvchilarga tarmoq xavfsizligining muhim tushunchalari, himoya usullari, texnologiyalari va hujumlardan saqlanish usullari o'rgatiladi. Fanning vazifasi – talabalarda fanning nazariy va amaliy masalalarini shuningdek, Tarmoqlarga bo'ladigan turli xil hujumlarni va xavf-xatarlarni tushuntirish, ularni oldindan aniqlash va tahlil qilish ko'nikmalarini shakllantirish.
	Fan mazmuni II. Asosiy nazariy qism (ma'ruza mashg'ulotlari) II.1. Fan tarkibiga quyidagi mavzular kiradi: Mashg'ulotlar shakli: ma'ruza (M)
M1	Fanning asosiy tushunchalari. "Tarmoq xavfsizligi" fanining maqsadi va vazifasi. Xavfsizlikning asosiy tushunchalarini o'rgatish: Tarmoq xavfsizligi, axborot xavfsizligi, maxfiylik, butunlik va mavjudlik kabi asosiy tushunchalarni tushuntirish. Xavf turlarini tahlil qilish: Xakerlik, tarmoq hujumlari, viruslar, troyanlar, DDoS hujumlari kabi xavf va hujum turlarini tahlil qilish va ularga qarshi himoya choralarini ishlab chiqish. Kriptografiya va shifrlash texnologiyalari: Ma'lumotlarni shifrlash, autentifikatsiya, elektron imzo kabi texnologiyalardan foydalanish ko'nikmalarini shakllantirish. Tarmoq monitoringi va kuzatuv: Tarmoqlarni monitoring qilish, kiruvchi hujumlarni aniqlash va ularga javob berish usullarini o'rgatish. Tarmoq xavfsizligini ta'minlovchi vositalar: Firewall, IDS (hujumni aniqlash tizimlari), IPS (hujumning oldini olish tizimlari) kabi himoya vositalari bilan ishlash ko'nikmalarini rivojlantirish. Tarmoqlarga bo'ladigan turli xil hujumlarni va xavf-xatarlarni tushuntirish, ularni oldindan aniqlash va tahlil qilish ko'nikmalarini shakllantirish
M2	Tarmoq arxitekturasini va xavfsizlik tizimining tarmoqqa ta'siri: Dizayn va xavfsizlik tamoyillari Tarmoq xavfsizligining zarurati, uning asosiy tamoyillari va dasturiy ta'minot xavfsizligi. Xavfsizlik siyosati, xavfsizlik hujumlari va himoya strategiyalari
M3	Tarmoq xavf-xatarlari va kiberhujum turlari: Huquqbuzarliklarning oldini olish Tarmoq arxitekturasini infratuzilmasiga qanday ta'sir qilishini tahlil

	qilish. Tarmoq hujumlari turlari, ularning oldini olish usullari va xavfsizlikni ta'minlash strategiyalari
M4	Kriptografik tizimlar va shifrlash algoritmlari: Shifrlashning asosiy tamoyillari va xavfsizlikka ta'siri Tarmoq xavfsizlik infratuzilmasi: Huquqbuzarliklar va himoya qilish strategiyalari Tarmoqning tuzilishi va uning xavfsizlik infratuzilmasiga qanday ta'sir qilishini tahlil qilish. Tarmoq hujumlari turlari, ularning oldini olish usullari va xavfsizlikni ta'minlash strategiyalari
M5	Autentifikatsiya tizimlari va ruxsat berish: Tarmoq foydalanuvchilari uchun xavfsiz kirish texnologiyalari Kriptografik tizimlar va ma'lumotlarni himoya qilish: Asosiy algoritmlar va ularning amaliy qo'llanilishi Kriptografiya haqida asosiy tushunchalar, asosiy shifrlash algoritmlari (AES, RSA, DES) va ularning zamonaviy tarmoq xavfsizligidagi roli.
M6	Tarmoq xavfsizligini infratuzilmasi: Firewall va IDS/IPS tizimlari Kriptografik tizimlar va ma'lumotlarni himoya qilish: Asosiy algoritmlar va ularning amaliy qo'llanilishi Ma'lumotlar maxfiyligi va yaxlitligini ta'minlashda shifrlashning o'rni
M7	Virtual xususiy tarmoqlar (VPN): Ma'lumotlarni xavfsiz uzatish vositalari Autentifikatsiya va ruxsat berish mexanizmlari: Identifikatsiya tizimlari va xavfsiz kirish protokollari Autentifikatsiya tizimlari, identifikatsiya va ruxsat berishning asosiy tamoyillari hamda xavfsiz kirish uchun ishlatiladigan protokollar (Kerberos, OAuth, SAML)
M8	Wi-Fi tarmoqlarining xavfsizligi: Simsiz tarmoqlarning himoya usullari va tahdidlari Autentifikatsiya va ruxsat berish mexanizmlari: Identifikatsiya tizimlari va xavfsiz kirish protokollari Autentifikatsiya tizimlari, identifikatsiya va ruxsat berishning asosiy tamoyillari hamda xavfsiz kirish uchun ishlatiladigan protokollar (Kerberos, OAuth, SAML)
M9	Kiberhujumlar va ulardan himoyalash: Zamonaviy kiberhujumlar va ularga qarshi choralar Tarmoqlarni himoya qilish: Firewall va IDS/IPS tizimlarining roli va amaliy qo'llanilishi Tarmoq xavfsizligini ta'minlashda firewall va Intrusion Detection/Prevention tizimlarining ahamiyati, ularning ishlash tamoyillari va konfiguratsiyasi.
M10	Tarmoq xavfsizligi va qonunchilik: Qonun va xalqaro standartlarga rioya qilish Tarmoqlarni himoya qilish: Firewall va IDS/IPS tizimlarining roli va amaliy qo'llanilishi Tarmoq xavfsizligini ta'minlashda firewall va Intrusion Detection/Prevention tizimlarining ahamiyati, ularning ishlash tamoyillari va konfiguratsiyasi. Ushbu tizimlar yordamida xavfsizlik siyosatini qanday amalga oshirish
M11	Bulutli hisoblash xavfsizligi: Bulutli xizmatlarda ma'lumotlar xavfsizligini ta'minlash Tarmoq xavfsizligi muammolari: Amaliy tavsiyalar va standartlar Tarmoq xavfsizligi bo'yicha keng tarqalgan muammolar, kiberhujumlar turlari va hujumlardan himoyalash bo'yicha amaliy tavsiyalar. Tarmoq xavfsizligi bo'yicha xalqaro standartlar
M12	IoT qurilmalar xavfsizligi: Internetda ishlaydigan narsalarning himoya usullari Tarmoq xavfsizligi muammolari va hujumlarga qarshi himoya: Amaliy tavsiyalar va standartlar

	Tarmoq xavfsizligi bo'yicha keng tarqalgan muammolar, kiberhujumlar turlari va hujumlardan himoyalalanish bo'yicha amaliy tavsiyalar. Tarmoq xavfsizligi bo'yicha xalqaro standartlar
III.Mashg'ulotlar shakli: amaliy mashg'ulot (AM)	
A1	Tarmoq xavfsizligi vositalari va ularni sozlash
A2	Hujumlarni aniqlash tizimlari va firewall konfiguratsiyasi
A3	VPN xizmatlarini sozlash va xavfsiz uzatish usullari
A4	Tarmoq sniflash vositalari bilan ishlash (Wireshark)
A5	Wi-Fi tarmoqlarining xavfsizligini sinovdan o'tkazish
A6	Shifrlash algoritmlarini amaliy qo'llash
A7	Autentifikatsiya tizimlarini yaratish va ruxsat berish jarayonini boshqarish
A8	Kriptografik tizimlarni tekshirish va ularning ishlashini baholash
A9	IDS/IPS tizimlari bilan ishlash va tahlil qilish
A10	Tarmoq hujumlarini oldini olish strategiyalari va vositalari
A11	Bulutli hisoblash muhitida xavfsizlikni ta'minlash
A12	IoT tarmoqlari xavfsizligini sinovdan o'tkazish va himoya qilish
A13	Ma'lumotlarni xavfsiz uzatish texnologiyalari (SSL/TLS protokollari)
A14	Zamonaviy xavfsizlik texnologiyalari va ularning tarmoqlarga qo'llanilishi
III.Mashg'ulotlar shakli: laboratoriya mashg'ulot (LM)	
A1	Tarmoq paketlarini tahlil qilish va sniffing hujumlarini aniqlash (Wireshark)
A2	Tarmoq xavfsizligi vositalarini o'rganish (Firewall, IDS/IPS)
A3	VPN o'rnatish va himoyalangan tarmoq ulanishini ta'minlash
A4	Wi-Fi xavfsizligi: WPA2, WPA3 sozlamalari va sinovdan o'tkazish
A5	Kriptografik usullarni amaliy qo'llash
A6	Tarmoqda autentifikatsiya tizimlarini sozlash va sinash

A7	IDS/IPS tizimlari yordamida hujumlarni aniqlash
A8	Bulutli hisoblashda ma'lumotlarni shifrlash va himoya qilish
A9	Tarmoq xavfsizligi hujumlarini simulyatsiya qilish
A10	IoT xavfsizligini ta'minlash usullari va amaliy qo'llanilishi
A11	Kiberhujumlardan himoyalalanish texnologiyalari sinovi
A12	SSL/TLS protokollarining amaliy qo'llanilishi
A13	Bulutli xavfsizlik va IoT infratuzilmasini himoya qilish bo'yicha amaliy ishlar
A14	Zamonaviy xavfsizlik texnologiyalari va ularning tarmoqlarga qo'llanilishi

IV. Mustaqil ta'lim va mustaqil ishlar

Mustaqil ta'lim uchun tavsiya etiladigan mavzular

“Tarmoq xavfsizligi” fani bo'yicha mustaqil ta'lim va ishlarning kalendar tematik rejai

№	Mustaqil ta'lim mavzulari
1	Kirishni boshqarish tizimlari (Authentication va Authorization)
2	Tarmoqda shifrlash (Encryption)
3	Xavfsizlik devorlari (Firewalls) va virtual xavfsizlik devorlari
4	VPN texnologiyalari va xavfsizlik
5	Intruziyani aniqlash va oldini olish tizimlari (IDS/IPS)
6	Tarmoq segmentatsiyasi va VLAN xavfsizligi
7	DDoS hujumlari va himoya choralarini ishlab chiqish
8	Xavfsiz kodlash va dasturlash tamoyillari
9	Tarmoq monitoringi va xavfsizlik auditlari
10	Xavfsizlik siyosati va qoidalarini ishlab chiqish

“Tarmoq xavfsizligi” fani bo'yicha mustaqil ta'lim mavzulari uning mazmunini yoritish maqsadida tanlangan va talabada shu haqida bilim ko'nikmasini shakllantirish nazarda tutilgan. Jumladan, Tarmoq xavfsizligi fani bo'yicha mustaqil ta'lim olish uchun quyidagi muhim mavzularni tanlab olish mumkin. Bu mavzular tarmoq xavfsizligi tamoyillari, texnologiyalari va amaliyotlarini qamrab oladi va talabalarning chuqurroq tushunishiga yordam beradi. Bu mavzularni o'rganish orqali tarmoq xavfsizligi tamoyillarini tushunish va amaliyotda qo'llash imkoniyati kengayadi. Har bir mavzu uchun amaliy mashg'ulotlar va misollar o'rganishni yanada chuqurlashtiradi. 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.

3.	V. Fan o'qitilishining natijalari (shakllanadigan kompetensiyalar) Fanni o'zlashtirish natijasida talaba:
-----------	---

	Tarmoq xavfsizligi asoslarini tushunadi Talaba tarmoq xavfsizligiga tahdid qiluvchi asosiy xatarlar, xavf omillari va tahdid turlari haqida aniq bilimga ega bo'ladi. Shuningdek, tarmoq himoyasi uchun zarur bo'lgan xavfsizlik tamoyillarini tushunadi. Xavfsizlik hujumlariga qarshi chora ko'rishni biladi Talaba tarmoqda yuz berishi mumkin bo'lgan turli xavfsizlik hujumlarini, jumladan, DDoS, man-in-the-middle, phishing, ma'lumot o'g'irlanishi kabi hujumlarni aniqlash va ularga qarshi texnikalar qo'llash ko'nikmalariga ega bo'ladi. Shifrlash usullarini amaliyotda qo'llay oladi Talaba ma'lumotlarni himoyalash uchun shifrlash va dekodlash texnologiyalarini, jumladan, simmetrik va assimetrik shifrlash algoritmlarini, SSL/TLS protokollarini qo'llay oladi. Ma'lumotlarning xavfsiz uzatilishini ta'minlash ko'nikmasiga ega bo'ladi.
4.	VI. Ta'lim texnologiyalari va metodlari: • ma'ruzalar; • interfaol keys-stadilar; • munozara, • o'z-o'zini nazorat. • "Aqliy hujum", • "Muammo"; • Krossvord • Annogrammalar • Ko'chma dars mashg'ulotlari
5.	VII. Kreditni olish uchun talablar: Fanga oid nazariy va uslubiy tushunchalarni to'liq o'zlashtirish, tahlil natijalarini to'g'ri aks ettira olish, o'rganilayotgan jarayonlar haqida mustaqil mushohada yuritish va joriy, oraliq nazorat shakllarida berilgan vazifa topshiriqlarni bajarish, yakuniy nazorat ishini topshirish

6. Asosiy adabiyotlar:

1. M.M.Musayev Kompyuter tizimlari va tarmoqlari. – T.: «Aloqachi», 2013 - 395 bet.
2. Djumanov O. Kompyuter tarmoqlari fanidan O'quv qo'llanma, SamDU, 2022 yil.

Qo'shimcha adabiyotlar:

3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие / А.П. Алферов и др. — М.: Гелиос АРВ, 2005. — 480 с.
4. William Stallings "Network Security Essentials: Applications and Standards", Pearson Education, Nyu-Jersi, AQSh, 2020
5. William Stallings "Cryptography and Network Security: Principles and Practice", Pearson Education, Nyu-Jersi, AQSh, 2021
6. Аскеров Т.М. и др. Защита информации и информационная безопасность: Учебное пособие / Под общей редакцией К.И. Курбакова / Т.М. Аскеров и др. — М.: Рос. экон. акад., 2001. — 387 с.
7. Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность: Лабораторный практикум / А.В. Бабаш и др. — М.: Кнорус, 2011. — 136 с.
8. Гагарина Л.Г., Кокорева Е.В., Виснадул Б.Д. Технология разработки программного обеспечения: Учебное пособие / под ред. - М.: ИД «ФОРУМ»: ИНФРА-М, 2008. - 400 стр.
9. Nazarov F., Yarmatov Sh. Sun'iy intellekt asoslari. Darslik –SamDU, 2024 –yil, 178- bet
10. Д. Расулев, Р.Ходиева, Т.Закирова. Компьютер тизимлари ва тармоqlari архитектураси. - ТДИУ, 2005, 151 бет.
11. Aminov I.B. Komputerning texnik va dasturiy ta'minoti. Darslik. SamDU, 2022 yil, 536 bet.
12. O.I.Djumanov, X.Bustonov, Xolmonov S.M. Informatika va dasturlash asoslari - Uquv-uslubiy

ko'rsatma, SamDU nashri, 2009, 100 bet.

Axborot manbalari (saytlar):

	13. https://books.google.co.uz 14. https://oak.uz 15. https://www.academia.edu 16. https://www.amazon.com/Computer-Systems-Networks-Fastrack-Blundell/dp/1844806391 17. https://ecs-network.serv.pacific.edu/ecpe-170/slides/13-networking.pdf
7.	Fan dasturi Sh.Rashidov nomidagi Samarqand davlat universiteti Kengashining 2024 yil "24" avgustdagi 1-son bayonnomasi bilan ma'qullangan.
8.	Fan/modul uchun mas'ullar: Xolmonov S.M. – Sharof Rashidov nomidagi SamDU, "Sun'iy intellekt va axborot tizimlari" kafedrasida dotsenti.
9.	Taqrizchilar: Djumanov O.I. – Sam DU Sun'iy intellekt va axborot tizimlari kafedrasida dotsenti, (ichki) +998 91 532 65 74 Raximov S. – O'zbekiston-Finlandiya pedagogika institute Informatika kafedrasida dotsenti, PhD. (tashqi)

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

Rais – Axatqulov S.

Kafedra mudiri: **A.E.Rashidov**

Fakultet dekani: **F.M.Nazarov**

Sharof Rashidov nomidagi SamDU o'quv ishlari bo'yicha 1-proroktor: **A.S.Soleyev**

Sharof Rashidov nomidagi Samarqand davlat universiteti Intellektual tizimlar va kompyuter texnologiyalari fakulteti "Sun'iy intellekt va axborot tizimlari" kafedrasida o'qituvchilari tomonidan kredit-modul tizimiga moslashtirilgan 60610200 –Axborot xavfsizligi ta'lim yo'nalishi talabalari uchun tayyorlangan "Tarmoq xavfsizligi" fan dasturiga

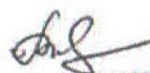
Taqriz

Mamlakatimizda jadal islohotlarni amalga oshirish bo'yicha butunlay yangicha g'oyalar, yondashuvlar, tamoyillar va yo'nalishlarga asoslangan bosqichga qadam qo'yimoqda. Shu boisdan Prezidentimiz Sh.M.Mirziyoyev tashabbuslari bilan yoshlarning bilim olishi uchun investitsiya kiritish orqali yurtimizda yangi Uyg'onish davri, ya'ni Uchinchi Renessans poydevorini yaratishni o'zimizga asosiy maqsad qilib belgilab oldik. Bugungi kunda zamonaviy kompyuter va axborot texnologiyalari bo'lajak mutaxassislardan muloqot uchun ma'lum bir darajadagi bilim, malaka va ko'nikmalarni talab qiladi. Bu bilim, malaka va ko'nikmalarni qay darajada mukammal bo'lishi muloqotning sifat darajasini belgilaydi. Mazkur muammoni hal qilish esa, boshlang'ich, o'rta maxsus va oliy ta'lim tizimidagi «Axborot texnologiyalari» fani oldida turgan eng dolzarb masalalardan biri bo'lib hisoblanadi. Ta'lim sohasidagi tub islohatlarning asosiy maqsadi jahon andozalari asosida bilimlar berish va raqobatlash kadrlar tayyorlashdir. Shuning uchun 60610200 – Axborot xavfsizligi ta'lim yo'nalishlarida o'qitiladigan fanlar ham zamonaviy fanlardan hisoblanadi. Ushbu namunaviy dastur bugungi kunning zamonaviy bilimlari bilan yangilangan va qayta ishlangan dastur bo'lib, unda fanning nazariy va amaliy jihatlariga alohida e'tibor qaratilgan. Mazkur fan dasturi texnologik jarayonlar va ishlab chiqarishni avtomatlashtirish yo'nalishlarida tahsil olayotgan talabalarining o'zlashtirishi lozim bo'lgan bilimlari va unga qo'yiladigan talablar asosida tuzilgan bo'lib, bo'lajak fan o'qituvchisi tayyorlangan "Tarmoq xavfsizligi" o'quv fanini o'zlashtirish jarayonida amalga oshiriladigan masalalar doirasida: kompyuter tarmoqlarini qurishda uchraydigan asosiy muammolardan biri, bu tarmoq tarkibiga kirgan qurilmalar - kompyuterlar, konsentratorlar, kommutatorlar, marshrutizatorlar o'rtasida axborot uzatishni amalga oshirish muammosi, bu yerda shu narsani ta'kidlab o'tish kerakki, bunda axborot uzatish (almashinish) asosan ketma-ket tarzda amalga oshirilishi. Axborot almashinish jarayonida qaysi qurilmalar ishtirok etayotganiga qarab: Ma'lumotlarning butunligini va maxfiyligini ta'minlash, tarmoqqa kirishni boshqarish va noqonuniy kirishlardan himoya qilish, tarmoq orqali uzatilayotgan ma'lumotlarning xavfsizligini ta'minlash, tarmoq faoliyatini kuzatish va tahdidlarni aniqlash, DDoS, phishing, malware va boshqa turdagi hujumlar, tarmoq uskunalaridagi yoki dasturiy ta'minotdagi zaifliklardan foydalanish, foydalanuvchilarni aldanish orqali ma'lumotlarga kirish.

Yuqoridagi fikrlardan kelib chiqqan holda, ushbu fan dasturi barcha qo'yilgan talablarga javob beradi deb hisoblayman.

O'zbekiston–Finlyandiya pedagogika
instituti "Informatika" kafedrasida

NING IMZOSINI
TASDIQLAYMAN
O'ZBEKISTON - FINLANDIYA
PEDAGOGIKA INSTITUTI
XODIMLAR BO'LIMI BOSHILIGI

 dots.S.Raximov



Sharof Rashidov nomidagi Samarqand davlat universiteti 2024-2025 o'quv yili uchun Intellektual tizimlar va kompyuter texnologiyalari fakulteti "Sun'iy intellekt va axborot tizimlari" kafedrasida o'qituvchilari tomonidan kredit-modul tizimiga moslashtirilgan 60610200 – Axborot xavfsizligi ta'lim yo'nalishi talabalari uchun tayyorlangan "Tarmoq xavfsizligi" fan dasturiga

TAQRIZ

Ta'lim sohasidagi tub islohatlarning asosiy maqsadi jahon andozalari asosida bilimlar berish va raqobatlash kadrlar tayyorlashdir. Shuning uchun 60610200 – Axborot xavfsizligi ta'lim yo'nalishlarida o'qitiladigan fanlar ham zamonaviy fanlardan hisoblanadi. Ushbu namunaviy dastur bugungi kunning zamonaviy bilimlari bilan yangilangan va qayta ishlangan dastur bo'lib, unda fanning nazariy va amaliy jihatlariga alohida e'tibor qaratilgan.

Mazkur fan dasturi texnologik jarayonlar va ishlab chiqarishni avtomatlashtirish yo'nalishlarida tahsil olayotgan talabalarining o'zlashtirishi lozim bo'lgan bilimlari va unga qo'yiladigan talablar asosida tuzilgan bo'lib, bo'lajak fan o'qituvchisi tayyorlangan "Tarmoq xavfsizligi" o'quv fanini o'zlashtirish jarayonida amalga oshiriladigan masalalar doirasida: kompyuter tarmoqlarini qurishda uchraydigan asosiy muammolardan biri, bu tarmoq tarkibiga kirgan qurilmalar - kompyuterlar, konsentratorlar, kommutatorlar, marshrutizatorlar o'rtasida axborot uzatishni amalga oshirish muammosi, bu yerda shu narsani ta'kidlab o'tish kerakki, bunda axborot uzatish (almashinish) asosan ketma-ket tarzda amalga oshirilishi. Axborot almashinish jarayonida qaysi qurilmalar ishtirok etayotganiga qarab: Ma'lumotlarning butunligini va maxfiyligini ta'minlash, tarmoqqa kirishni boshqarish va noqonuniy kirishlardan himoya qilish, tarmoq orqali uzatilayotgan ma'lumotlarning xavfsizligini ta'minlash, tarmoq faoliyatini kuzatish va tahdidlarni aniqlash, DDoS, phishing, malware va boshqa turdagi hujumlar, tarmoq uskunalaridagi yoki dasturiy ta'minotdagi zaifliklardan foydalanish, foydalanuvchilarni aldanish orqali ma'lumotlarga kirish.

Yuqoridagi fikrlardan kelib chiqqan holda, ushbu fan dasturi barcha qo'yilgan talablarga javob beradi deb hisoblayman.

Sharof Rashidov nomidagi Samarqand davlat universiteti
Sun'iy intellekt va axborot tizimlari kafedrasida dotsenti

Prof. n. Djumanov O.I.

