

41147  
200

**O'ZBEKISTON RESPUBLIKASI  
OLIY TA'LIM, FAN VA INNOVATSIYALAR VAZIRLIGI  
MAKTABGACHA VA MAKTAB TA'LIM VAZIRLIGI  
SAMARQAND DAVLAT PEDAGOGIKA INSTITUTI**

Ro'yxatga olindi:  
№ BD 29  
2025-yil "29" avgust



**AXBOROT XAVFSIZLIGI  
FANINING O'QUV DASTURI**

<b>Bilim sohasi:</b>	<b>100000 - Ta'lim</b>
<b>Ta'lim sohasi:</b>	<b>110000 – Ta'lim</b>
<b>Ta'lim yo'nalishi:</b>	<b>60110600 – Matematika va informatika</b>

Samarqand – 2025





Kalitni xavfsiz uzatish muammosi – kalitni ishonchli tarzda uzatish zarurati. Nosimmetrik kriptografiya odatda autentifikatsiya va raqamli imzolarni yaratishda qo'llaniladi.

### III. Amaliy Laboratoriya mashg'ulotlari

1. Axborot xavfsizligiga kirish
  - o Axborot xavfsizligini ta'minlash asoslari.
  - o Xavfsizlikni ta'minlashda foydalaniladigan umumiy metodlar.
2. Axborot xavfsizligi siyosati va huquqiy asoslari
  - o Axborot xavfsizligini ta'minlashga oid qonunlar va me'yorlar.
  - o Axborot xavfsizligi siyosatini ishlab chiqish.
3. Axborot urushi: mohiyati, turlari va usullari
  - o Axborot urushining turli shakllari va xavfsizlikka ta'siri.
  - o Axborot urushi vositalarini aniqlash va ulardan himoya qilish.
4. Kompyuter tarmoqlarini himoya qilish asoslari
  - o Tarmoqni himoya qilish texnologiyalari (firewall, antiviruslar).
  - o Tarmoq xavfsizligini baholash va xavfsizlik tizimlarini sozlash.
5. Internet xavfsizligi
  - o Internetda xavfsizlikni ta'minlashning asosiy qoidalari.
  - o Onlayn hujumlardan himoya qilish (phishing, malware, DDoS).
6. Ma'lumotlarni shifrlash asoslari
  - o Shifrlash algoritmilarini qo'llash va ularning xavfsizlikni ta'minlashdagi roli.
  - o Simmetrik va nosimmetrik shifrlashni o'rganish va qo'llash.
7. Kriptografik protokollar va autentifikatsiya usullari
  - o SSL/TLS va boshqa kriptografik protokollarni o'rnatish va qo'llash.
  - o Identifikatsiya va autentifikatsiyani amalga oshirish (parol, biometrik, ikki faktorli autentifikatsiya).
8. Axborotlarni texnik vositalar orqali himoyalash
  - o Antivirus va antimalware vositalarini o'rnatish va ishlatish.
  - o Kibernetik hujumlardan himoya qilish va tizimlarni tahlil qilish.
9. Shaxsiy kompyuterda ma'lumotlarni himoya qilish
  - o Shaxsiy kompyuterlarda xavfsizlikni ta'minlash: antivirus dasturlari, foydalanuvchi huquqlari.
  - o Parollar va ma'lumotlarni shifrlash bo'yicha amaliyot.
10. Axborot tizimlarini himoya qilish: Xavfsiz tizimlarni yaratish
  - o Avtomatlashtirilgan axborot tizimlarida xavfsizlikni ta'minlash.
  - o Tizimni xavfsizlashtirishda ishlatiladigan vositalar (firewall, IDS/IPS).
11. Ma'lumotlarni zaxiralash va tiklash usullari.
12. Xavfsizlikni yaratish va ulardan tiklash usullari.
13. Kriptografik shifrlash algoritmilarini o'rganish va amaliyotda qo'llash.
14. Shifrlash tizimlarini tuzish va analiz qilish.
15. Axborot xavfsizligi huquqiy muammolarini hal etish
16. Axborot xavfsizligi va huquqiy javobgarlik.
17. Axborotlar buzilishi holatlarida huquqiy choralar va jazolar.

### IV. Laboratoriya mashg'ulotlari

1. Axborot xavfsizligining asosiy tahdidlarini aniqlash va tasniflash
  - o Kompyuter xavfsizligiga tahdid soluvchi omillarni o'rganish (viruslar, fishing, rootkitlar).
  - o Ochiq manbalardan real tahdidlar misollarini tahlil qilish.
2. Operatsion tizimda foydalanuvchi huquqlarini boshqarish va xavfsizligini ta'minlash
  - o Windows/Linux tizimlarida foydalanuvchi rollarini sozlash, guruhlarini boshqarish.
  - o Mahalliy va tarmoq kirishini cheklash amaliyoti.
3. Firewall va NAT orqali tarmoq xavfsizligini ta'minlash
  - o Windows Defender Firewall yoki piSense orqali xavfsizlik devorini sozlash.
  - o NAT (Network Address Translation) orqali tarmoqdagi qurilmalarni yashirish.
4. Brauzerlar xavfsizlik sozlamalari va xavfli saytlarni aniqlash
  - o Chrome, Firefox kabi brauzerlarda xavfsizlik funksiyalarini tekshirish va sozlash.
  - o Simulyatsiya qilingan phishing sahifalariga kirishda brauzer reaksiyasini o'rganish.
5. Kompyuter tarmoqlarida portlarni aniqlash va filtrlash
  - o Nmap yordamida ochiq portlarni aniqlash.
  - o Xavfli portlar orqali tahdidlarni tahlil qilish va bloklash.
6. Elektron raqamli imzo yaratish va hujjatni imzolash amaliyoti
  - o E-imzo modullaridan foydalanib PDF yoki DOC fayllarni raqamli imzolash.
  - o Imzoni verifikatsiya qilish (haqiqiyligini tekshirish).
7. Rasmlar orqali maxfiy ma'lumotlarni yashirish (steganografiya)
  - o Steghide yoki boshqa vositalar bilan jpg, wav fayllarga xabar yashirish.
  - o Yashirilgan xabarlarini tiklash.
8. Disk va fayl shifrlash vositalari bilan ishlash: VeraCrypt / BitLocker
  - o Diskni to'liq shifrlash va parol bilan himoyalash.
  - o USB qurilmalarni shifrlash va test qilish.
9. Ma'lumotlarni zaxiralash va tiklash: tizim va fayl darajasida
  - o Windows'ning "Backup and Restore" va Linux'dagi rsync, tar vositalaridan foydalanish.
  - o Avto-backup sozlash va tiklashni bajarish.
10. Ikki bosqichli autentifikatsiya tizimini sozlash va sinovdan o'tkazish
  - o Google Authenticator, Authy orqali autentifikatsiya o'rnatish.
  - o Web-ilovalar yoki VPN kirishini ikki bosqichli autentifikatsiyaga ulash.
11. Identifikatsiya va foydalanuvchini tekshirish tizimlari
  - o Biometrik autentifikatsiya tushunchasi.
  - o Logon tizimlarida foydalanuvchini aniqlash amaliyoti (login, parol, captcha).
12. Xavfsiz tarmoq trafikini tahlil qilish: Wireshark orqali monitoring
  - o Tarmoq paketlarini real vaqt rejimida yozib olish.
  - o Tizimga qilingan kutilmagan so'rovlarini aniqlash va tahlil qilish.
13. Virtual tarmoq muhiti yaratish va xavfsizlikni sinash (VirtualBox/PiSense



asosida)

- Virtual tarmoqda NAT, DHCP, Firewall sozlash.
- Ichki tarmoqda test hujumlar o'tkazib xavfsizlik holatini baholash.

#### V. Mustaqil ta'lim va mustaqil ishlar

Auditoriyanidan tashqari vaqtda bajariladigan mustaqil ishlar quyidagi turlarda amalga oshirilishi tavsiya etiladi:

- Mavzuni og'zaki bayon qilish;
- 4 javobli test savoli tayyorlash;
- yozma savol tayyorlash;
- Taqdimot tayyorlash;
- Referat tayyorlash;
- Ma'lumotlarni jadval ko'rinishida ifodalash;
- Videorolik tayyorlash;
- Ko'rgazmali qurol tayyorlash;
- Bir soatlik dars ishanma tayyorlash;
- Krassvord tuzish;
- Xorijiy adabiyotlardan ma'lumotlarni to'plash, tarjima qilish va tahlil qilish;
- Ha, yo'q javobli test tuzish;
- Audio dars tayyorlash;
- Internet ma'lumotlarini to'plash va tahlil qilish;
- Adabiyotlar ro'yxatini tuzish;

#### VI. Mustaqil ta'lim uchun tavsiya etiladigan mavzulari:

1. Internetda xavfsiz harakatlanish: asosiy qoidalar va real tahdidlar
2. Axborot xavfsizligining asosiy tamoyillari: maxfiylik, yaxlitlik va mavjudlik
3. Himoya ob'ektlari: axborot, foydalanuvchi va texnik vositalar
4. Axborot turlari va tashuvchilari: matn, rasm, ovoz va ularning xavfsizligi
5. Axborot tizimlarida himoyalash strategiyalari va vositalari
6. Zararli dasturlar: turlari, tarqalish usullari va faoliyat prinsiplari
7. Zararli dasturlardan samarali himoyalash usullari
8. Kompyuter jinoyatlari: turlari, misollari va huquqiy oqibatlar
9. Axborotni yo'qotishdan himoyalash: backup va xavf strategiyalari
10. Dasturiy ta'minotga qarshi hujumlar va ularni rad etish choralari
11. Apparat vositalarni rad etish (DoS/DDoS) hujumlaridan himoyalash
12. Axborotni saqlash va taqdim etish shakllari: xavfsizlik nuqtayi nazaridan tahlil
13. Axborotni himoyalashning asosiy metodlari: texnik, dasturiy va tashkiliy
14. Axborot xavfsizligini ta'minlovchi xalqaro va milliy tashkilotlar
15. Tashkilotlarda axborot xavfsizligini boshqarish tizimi (ISMS)
16. Cisco xavfsizlik texnologiyalari: ilovalar, sozlash va nazorat
17. Axborot xavfsizligi tahdidlarini aniqlash va tahlil qilish
18. Kriptografik kalitlarni boshqarish vositalari va ularning muhimligi
19. Diskdagi ma'lumotlarni shifrlash: TrueCrypt, BitLocker va VeraCrypt misolida

21. Axborot xavfsizligining tarixiy rivojlanish bosqichlari va yutuqlari
22. Axborotni himoyalashning tashkiliy-texnik yondashuvlari
23. Kompyuter viruslaridan himoalanish: antivirus, sandbox, va monitoring vositalari
24. Axborotni viruslardan himoyalashda kompleks yondashuv
25. Axborotni himoyalashning zamonaviy texnologiyalari: AI, blokcheyn, Zero Trust
26. Axborotni himoyalashning innovatsion va yangi metodlari
27. Xodimlar uchun axborot xavfsizligi bo'yicha xavfsizlik madaniyatini shakllantirish
28. Mobil qurilmalarda axborot xavfsizligini ta'minlash: amaliy yondashuvlar

3.	<p><b>VII. Ta'lim natijalari (shakllanadigan kompetensiyalar)</b></p> <p><b>Talaba bilish kerak:</b></p> <ul style="list-style-type: none"><li>- Axborot xavfsizligi fanini o'zlashtirish uchun umumiy informatika, kompyuter savodxonligi va raqamli texnologiyalar bo'yicha boshlang'ich bilimlarga ega bo'lishi zarur. (<i>bilim</i>)</li><li>- Axborot xavfsizligining mazmuni, asosiy tushunchalari, maqsadi va vazifalarini bilish, himoya ob'ektlari, tahdidlar va ularni bartaraf etish usullari, shuningdek, tarmoq xavfsizligi, kriptografik asoslar, zararli dasturlar, autentifikatsiya vositalari haqida nazariy tushunchalarga ega bo'lish. (<i>bilim</i>)</li><li>- Zararli dasturlarni aniqlash va oldini olish, tarmoq xavfsizligi vositalaridan foydalanish, axborot tizimlarida ma'lumotlarni shifrlash, kriptografik kalitlar bilan ishlash, disk va tarmoq orqali uzatiladigan ma'lumotlarni himoyalash, shuningdek, axborot xavfsizligining tashkiliy-texnik chora-tadbirlarini amaliy qo'llay olish ko'nikmalariga ega bo'lish. (<i>ko'nikma</i>)</li><li>- Elektron darsliklar, video ma'ruzalar, simulyator dasturlar, internet resurslari, lokal tarmoqdagi virtual laboratoriyalar, axborot xavfsizligi bo'yicha onlayn testlar, case-study materiallaridan samarali foydalana olish. (<i>ko'nikma</i>)</li><li>- Mustaqil ta'lim, loyihaviy ishlar, tahdid tahlili, real holatlar asosida yechim ishlab chiqish, rolli o'yinlar, mini-debat, SWOT-tahlil, hamkorlikda o'rganish kabi interaktiv pedagogik yondashuvlardan foydalanish orqali axborot xavfsizligini baholash, tahdidlarni aniqlash va ularning oldini olish bo'yicha mustahkam amaliy malakaga ega bo'lish. (<i>malaka</i>)</li></ul>
4.	<p><b>VIII. Ta'lim texnologiyalari va metodlari:</b></p> <ul style="list-style-type: none"><li>• ma'ruzalar;</li><li>• interfaol keys-stadilar;</li><li>• dialogik yondoshuv</li><li>• SWOT tahlili</li><li>• Venn diagrammasi</li><li>• Blis so'rov</li><li>• nilufar guli</li><li>• baliq skeleti</li><li>• kim chaqqon</li><li>• blis test va boshqalar</li></ul>
5.	<p><b>IX. Kreditlarni olish uchun talablar:</b></p> <p>Fanga oid nazariy va amaliy tushunchalarni to'la o'zlashtirish, tahlil natijalarini to'g'ri aks ettira olish. o'reanilavotgan jarayonlar haqida mustaqil mushohada yuritish,</p>



	yakuniy nazorat bo'yicha amaliy ishini topshirish.
6.	<p><b>X. Asosiy adabiyotlar</b></p> <ol style="list-style-type: none"> <li>1. Aripov M., Matyakubov A.S. Axborotlarni himoyalash usullari. Toshkent "Universitet". 2014 yil.</li> <li>2. G'aniyev S.K. Karimov M.M. Tashev.K.A. Axborot xavfsizligi. T.: "Fan va texnologiya", 2017, 372 bet.</li> <li>3. M.M.Aripov, B.F.Abdurahimov, A.S.Matyakubov. Kriptografik usullar. Toshkent. 2020 yil. 213 bet.</li> <li>4. B.N.Tahirov. Axborot xavfsizligi asoslari. Buxoro: Fan va ta'lim, 2022.-156 b.</li> </ol> <p><b>XI. Qo'shimcha adabiyotlar</b></p> <ol style="list-style-type: none"> <li>1. I.X.Abdullayev, M.X.Aliyeva, D.A.Maxramova. Axborot xavfsizligi. O'quv qo'llanma. Samarqand 2025.</li> <li>2. Z.M.Raxmatullayev. Kompyuter texnikasidan samarali foydalanish bo'yicha uslubiy talablar va tavsiyalar. Toshkent. "O'qituvchi", 2012</li> <li>3. Charles P. Pfleeger, Shari Lawrence Pfleeger. Security in Computing, 4th Edition. Pearson Education, Inc.2007</li> <li>4. Michael E. Whitman. Herbert J. Mattord. Principles of Information Security, Fourth Edition. Course Technology, Cengage Learning. 2012</li> <li>5. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. –СПб.: БХВ-Петербург, 2009. – 576 с..</li> </ol> <p><b>Axborot manbalari</b></p> <ol style="list-style-type: none"> <li>1. <a href="http://www.gov.uz">www.gov.uz</a> – O'zbekiston Respublikasi hukumat portal.</li> <li>2. <a href="http://www.nuu.uz">www.nuu.uz</a></li> <li>3. <a href="http://www.ziyonet.uz">www.ziyonet.uz</a></li> <li>4. <a href="http://www.infomag.ru">www.infomag.ru</a></li> </ol>
7.	Fan dasturi Samarqand davlat pedagogika instituti o'quv-uslubiy kengashining 2025 yil "___" _____-son bayonnomasi bilan ma'qullangan
8.	<p><b>Fan/modul uchun mas'ullar va dastur mualliflari:</b></p> <p>I.X.Abdullayev – Samarqand davlat pedagogika instituti Informatika kafedrasida assistenti.</p> <p>O'M.Saidov – Samarqand davlat pedagogika instituti Informatika kafedrasida mudiri, informatika fanlari bo'yicha falsafa doktori (PhD).</p>
9.	<p><b>Taqrizchilar:</b></p> <p>S.Hasanova - Samarqand davlat pedagogika instituti Informatika kafedrasida dotsenti (ichki)</p> <p>A.J.Xurramov – Chirchiq davlat pedagogika instituti Informatika va axborot texnologiyalari kafedrasida dotsenti</p>

Oliy ta'lim, fan va innovatsiyalar vazirligi tomonidan 2025-yil uchun tasdiqlangan xalqaro e'tirof etilgan tashkilotlarning reytingida top 300 talikka kiruvchi Lomonosov nomidagi Moskva Davlat Universiteti(QS-93,THE-108, ARWU-115) ning "Axborot xavfsizligi asoslari" va Indian Institute of Science (QS-210, THE-261, ARWU-418) "Axborot xavfsizligi siyosati" fan dasturlari tahlil qilinib

ushbu asosda fan dastur ishlab chiqildi. "Axborot xavfsizligi" fanining dasturi tayyorlanib 6 ta mavzusi yangilandi.

[https://www.socio.msu.ru/documents/bpp3\\_200p.pdf](https://www.socio.msu.ru/documents/bpp3_200p.pdf)

<https://iisc.ac.in/wp-content/uploads/2025/01/Information-Security-Policy-IISc-signed.pdf>

Fan dastur Aniq va amaliy fanlar fakultetning 2025-yil 28-fevraldagi 10-sonli farmoyish bilan tuzulgan ishchi guruh tomonidan ma'qullangan.

Tuzuvchi:

Kafedra mudiri:

Fakultet dekani:

O'quv-ishlar bo'yicha prorektor:

I.X.Abdullayev  
O'M.Saidov  
A.N.Abdullayev  
S.H.Mushtamonov