OLIY TA'LIM, FAN VA INNOVATSIYALAR VAZIRLIGI
ZAHIRIDDIN MUHAMMAD BOBUR NOMIDAGI
ANDIJON DAVLAT UNIVERSITETI

"TASDIQLAYMAN"
O'quv ishlari bo'yicha prorektor
B. Axmedov
_____2025-yil

Dasturiy injiniringi kafedrasi

KIBERXAVFSIZLIK ASOSLARI
FAN SILLABUSI
(KIA1406)

Bilim sohasi: - 600 000 Axborot-kommunikatsiya texnologiyalari

Ta'lim sohasi: - 610 000 Axborot-kommunikatsiya texnologiyalari

Ta'lim yo'nalishi: - 60610500 Kompyuter injiniringi

Andijon – 2025

CamScanner yordamida skanerlangan

© Ushbu hujjat Andijon davlat universiteti mulki hisoblanadi va uni oluvchilar uchun maxfiy bo'lib, to'liq yoki qisman nusxa ko'chirilishi, tarqatilishi yoki ko'paytirilmasligi yoki uchinchi shaxslarga berilmasligi kerak. Ushbu materialni ko'paytirish, tarqatish, nusxalash, oshkor qilish, o'zgartirish, tarqatish yoki nashr etishning har qanday shakli qat'iyan man etiladi.

Kun	
Avgust 2025	Ushbu sillabus Andijon davlat universiteti kengashining 2025-yil "28"-avgustdagi 1-sonli bayonnomasi bilan ma'qullangan.
	Tuzuvchi: **N.O'rinov** – AndDU "Axborot texnologiyalari" kafedrasi dotsenti.
	Taqrizchilar: **Sh.Umarov** – FDTU O'quv uslubiy bo'lim boshlig'i o'rinbosari, PhD **J.R.Azimjonov** – AndDU Dasturiy injiniringi kafedrasi mudiri, PhD

CamScanner yordamida skanerlangan

Mundarija

KIA1406: Kiberxavfsizlik asoslari 4
1. Fan tavsifi..... 4
2. Fanning dastlabki rekvizitlari..... 4
3. Fanning maqsadi..... 4
4. Ta'lim berish natijalari 4
5. Ta'lim berish usullari 5
6. Mustaqil ta'lim va mustaqil ishlar 5
7. Adabiyotlar..... 6
8. Soatlar/Kreditlar..... 8
9. Fanning tarkibiy tuzilishi..... 8
10. Talabalar bilimini baholash 10
11. Akademik talablar 11

CamScanner yordamida skanerlangan

KIBERXAVFSIZLIK ASOSLARI (KIA1406)

1. Fan tavsifi

"Kiberxavfsizlik asoslari" fanida axborot tizimlari va tarmoqlarida yuzaga keladigan xavf-xatarlar, ularning oldini olish mexanizmlari, shuningdek, shaxs, tashkilot va jamiyat xavfsizligini ta'minlashga qaratilgan zamonaviy yondashuvlar o'rganiladi. Ushbu fan birinchi kursning ikkinchi semestrida o'qitilishi rejalashtirilgan.

Fan mazmunini anglab yetish — talabalar uchun axborot xavfsizligining asosiy tushunchalari, kompyuter tarmoqlarida xavfsizlikni ta'minlash prinsiplari, shaxsiy ma'lumotlarni himoya qilish yo'llari, zararli dasturlar va kiberhujumlarning oldini olish, autentifikatsiya va avtorizatsiya mexanizmlari, shuningdek, xalqaro va milliy kiberxavfsizlik standartlari haqida bilimlarni egallashda muhimdir.

Fanning asosiy jihati — talabalarga axborot xavfsizligini ta'minlash jarayonida zarur bo'lgan nazariy-metodologik va amaliy bazani shakllantirish, zamonaviy kiberxavfsizlik vositalaridan foydalanish, axborot tizimlarini tahlil qilish va ulardagi xavf-xatarlarni baholash ko'nikmalarini hosil qilishdan iboratdir. Fanda, shuningdek, quyidagi masalalar yoritiladi:

- kiberxavfsizlikning asosiy tushunchalari va tamoyillari;
- axborot xavfsizligi siyosati va boshqaruvi;
- tarmoq xavfsizligi va himoya vositalari;
- zararli dasturlar va ularning turlari;
- kriptografiya asoslari va ma'lumotlarni himoyalash usullari;
- hujumlarni aniqlash va oldini olish tizimlari (IDS/IPS);
- kiberxavfsizlikda inson omili va xavfsizlik madaniyati.

2. Fanning dastlabki rekvizitlari

Ushbu fan uchun oldindan bilim (prerekvizitlar) talab etilmaydi.

3. Fanning maqsadi

"Kiberxavfsizlik asoslari" fanining maqsadi talabalarga axborot tizimlari va kompyuter tarmoqlarida yuzaga kelishi mumkin bo'lgan xavf-xatarlarni anglash, ularni aniqlash, oldini olish va bartaraf etishning nazariy hamda amaliy bilimlarini berish, shuningdek, axborot resurslarini himoya qilishning tashkiliy, texnik va kriptografik usullari bo'yicha zarur ko'nikmalarni shakllantirishdan iborat.

- talabalarda kiberxavfsizlik sohasida zarur bo'lgan nazariy-metodologik va amaliy bazani hosil qilish,

CamScanner yordamida skanerlangan

- zamonaviy kiberxavfsizlikning tadqiqot va tahlil metodlarini axborot tizimlari va tarmoqlarni himoyalash jarayonida qo'llay bilish,
- kiberxavfsizlik shug'ullanadigan fundamental masalalar — axborot xavfsizligi tushunchalari va tamoyillari,
- tarmoq xavfsizligi va himoya texnologiyalari,
- zararli dasturlar va kiberhujumlar turlari,
- shaxsiy ma'lumotlarni himoya qilish va axborot maxfiyligini ta'minlash,
- kriptografik usullar va ma'lumotlarni shifrlash asoslari,
- autentifikatsiya va avtorizatsiya mexanizmlari,
- hujumlarni aniqlash va oldini olish tizimlari (IDS/IPS),
- axborot xavfsizligi siyosati va boshqaruvi,
- kiberxavfsizlikda inson omili, ijtimoiy muhit va xavfsizlik madaniyati,
- xalqaro va milliy standartlar asosida xavfsizlikni tashkil etish jarayonlari bilan tanishtirish orqali amaliy bilim va ko'nikmalarni hosil qilishdir.

4. Ta'lim berish natijalari

Ushbu fanni muvaffaqiyatli tugatib, talabalar quyidagi bilim, ko'nikma va malakalarga ega bo'ladilar:

1. Axborot xavfsizligi tushunchalari, kiberxavfsizlik tamoyillari va kiberxavflarning oldini olish mexanizmlari bo'yicha nazariy bilimlarni egallaydi.
2. Kompyuter tarmoqlari va axborot tizimlarida xavfsizlikni ta'minlash usullarini, xavf-xatarlarni aniqlash va ularni tahlil qilish mexanizmlarini tushunadi.
3. Zararli dasturlar, kiberhujum turlari va ularning oqibatlarini tahlil qila oladi hamda ularni bartaraf etish bo'yicha xulosalar chiqara oladi.
4. Kriptografiya asoslarini, autentifikatsiya va avtorizatsiya mexanizmlarini qo'llay oladi, shaxsiy ma'lumotlarni himoya qilish ko'nikmalariga ega bo'ladi.
5. Kiberxavfsizlik muammolarini tahlil qilishda zamonaviy metodlardan samarali foydalana oladi, axborot xavfsizligi siyosati va boshqaruv tamoyillarini amalda qo'llay oladi.
6. Hujumlarni aniqlash va oldini olish tizimlari (IDS/IPS), xavfsizlik devorlari (firewall) va boshqa himoya texnologiyalaridan foydalana oladi.
7. Axborot xavfsizligi bo'yicha xalqaro va milliy standartlarni (ISO/IEC 27001 va boshqalar) tushunadi va amaliyotda qo'llashni o'rganadi.

CamScanner yordamida skanerlangan

8. Tarmoq trafigini kuzatish, tahlil qilish va zarur hollarda xavfsizlik choralarini ko'ra olish ko'nikmalariga ega bo'ladi.
9. Inson omili bilan bog'liq xavfsizlik muammolarini anglaydi va kiberxavfsizlik madaniyatini shakllantirishga hissa qo'sha oladi.
10. Amaliy laboratoriya mashg'ulotlari orqali xavfsizlik vositalarini sozlash, xavf-xatarlarni modellashtirish va ularni bartaraf etish bo'yicha tajribaga ega bo'ladi.
11. Kiberxavfsizlikdagi yangi tendensiyalar, texnologiyalar va hujum uslublarini muntazam o'rganish va yangiliklardan xabardor bo'lib borish ko'nikmasini rivojlantiradi.

5. Ta'lim berish usullari

- **real vaziyatlarga asoslangan amaliy ishlarni bajarish** (masalan, kiberhujum stsenariylarini tahlil qilish, hujumlarni aniqlash va himoya choralarini ishlab chiqish);
- **esse, tezis va maqolalar yozish** (kiberxavfsizlikning dolzarb muammolari va yechimlari bo'yicha ilmiy yozuvlar tayyorlash);
- **vaziyatli topshiriqlarni (keys-stadi) yechish** (tarmoqdagi buzilish, zararli dastur tarqalishi yoki phishing hujumi kabi vaziyatlarni yechish);
- **jarayonli-yo'naltirilgan ta'lim** (axborot xavfsizligini ta'minlash jarayonlarini bosqichma-bosqich o'rgatish);
- **muhokamalarda ishtirok etish** (axborot xavfsizligi siyosati, xalqaro standartlar va huquqiy me'yorlarni muhokama qilish);
- **kichik guruhlarda ishlashni tashkil etish** (penetratsion test, tarmoq monitoringi va xavfsizlik siyosati ishlab chiqishda guruh bo'lib ishlash);
- **loyiha ishini bajarish** (tarmoq xavfsizlik modeli, antivirus himoya tizimi yoki IDS/IPS loyihasini ishlab chiqish);
- **mustaqil ishlarni bajarish** (adabiyotlarni o'qish, yangi tahdid va hujumlar bo'yicha tahliliy materiallar tayyorlash);
- **taqdimot tayyorlash** (kiberxavfsizlik texnologiyalari, hujum turlari va himoya vositalari haqida chiqish qilish);
- **turli darajadagi testlarni yechish** (asosiy tushunchalar, xavfsizlik vositalari va kiberxavfsizlik standartlari bo'yicha bilimlarni baholash);
- **so'rov o'tkazish** (talabalar orasida xavfsizlik madaniyati, shaxsiy ma'lumotlarni himoya qilish bo'yicha bilim darajasini aniqlash);
- **muammoni hal qilish** (real kiberxavfsizlik muammolarini aniqlash, ularni bartaraf etish va profilaktika choralarini ishlab chiqish).

CamScanner yordamida skanerlangan

6. Mustaqil ta'lim va mustaqil ishlar

1. Axborot xavfsizligi tushunchalari va tamoyillari.
2. Tahdidlar va zaifliklar.
3. Zararli dasturlar: turlari va ta'siri.
4. Kriptografiya: asosiy tushunchalar va algoritmlar.
5. Simmetrik kriptografiya va uning amaliyoti.
6. Asimmetrik kriptografiya va RSA algoritmi.
7. Autentifikatsiya va avtentifikatsiya usullari.
8. Parol xavfsizligi va parol boshqaruv dasturlari.
9. Biometrik autentifikatsiya: turlari va xavfsizligi.
10. Multi-faktorli autentifikatsiya va uning afzalliklari.
11. Tarmoq xavfsizligi asoslari.
12. Firewalls: turlari va ishlash prinsiplari.
13. IDS/IPS tizimlari va ularning roli.
14. VPN: ishlash prinsipi va xavfsizlik.
15. Wi-Fi xavfsizligi: WPA2 va boshqa choralar.
16. Veb xavfsizligi: asosiy tahdidlar va himoya usullari.
17. SQL Injection hujumlari va ularning oldini olish.
18. Cross-Site Scripting (XSS) hujumlari va himoya.
19. Cross-Site Request Forgery (CSRF) hujumlari va himoya.
20. E-mail xavfsizligi: phishing va spam hujumlari.
21. Bulutli xizmatlar xavfsizligi.
22. Mobil qurilmalar xavfsizligi.
23. Ransomware: tahdidi va himoyalanish usullari.
24. DoS va DDoS hujumlari: turlari va oldini olish.
25. Axborot xavfsizligi siyosati va boshqaruvi.
26. ISO/IEC 27001 standarti: asosiy tushunchalar.
27. Xavfsizlik hodisalarini aniqlash va javob choralarini ko'rish.
28. Ijtimoiy muhandislik hujumlari: turlari va oldini olish.
29. Axborot xavfsizligida inson omili va madaniyatini shakllantirish.
30. Kelajakdagi xavfsizlik tahdidlari va tendensiyalari.

7. ADABIYOTLAR

CamScanner yordamida skanerlangan

Asosiy adabiyotlar

1. Joseph Steinberg, Kevin Beaver, Ted Coombs and IRA Winkler Cybersecurity All-in-One For Dummies. manual Canada 2023.
2. Mark Stamp. Information sesurity. Prinsiples and Prastise. Sesond edition. A John Wiley& Sons, Ins., publisation. Printed in the United States of Amerisa. 2011 y. 584p.
3. O'rinov N.T., "Kiberxavfsizlik asoslari" darslik, Toshkent 2022.
4. O'rinov N.T., "Axborot xavfsizligi" o'quv qo'llanma, Andijon 2023.
5. David Wong., "Real-World Cryptography", Printed in the United States of America 2021.

Qo'shimcha adabiyotlar

1. Mirziyoev SH.M. "Niyati ulug' xalqning ishi ham ulug', hayoti yorug' va kelajagi farovon bo'ladi" - Toshkent.; O'zbekistan nashriyoti. 2019 yil
2. Mirziyoev SH.M. Buyuk kelajagimizni mard va oliyjanob xalqimiz bilan birga quramiz - Toshkent.; O'zbekistan nashriyoti. 2017
3. Mirziyoev SH.M. Qonun ustuvorligi va inson manfaatlarni ta'minlash yurt taraqqiyoti va xalq farovonligining garovi. - Toshkent.;O'zbekistan nashriyoti. 2017 yil
4. Mirziyoev SH.M. Erkin va farovon demokratik O'zbekistan davlatini birgalikda barpo etamiz. - Toshkent.; O'zbekistan nashriyoti.2017 yil
5. Mirziyoev SH.M. Tanqidiy taxlil qat'iy tartib intizom va shaxsiy javobgarlik har bir rahbar faoliyatining kundalik qoidasi Bo'lishi kerak.-Toskent .; O'zbekistan nashriyoti. 2017 iil

Axborot manbalari

1. https://prezident.uz
2. https://www.gov.uz
3. http://lex.uz
4. http://uza.uz
5. http://ziyonet.uz
6. https://edu.uz

8. Soatlar/Kreditlar

Ikkinchi semestr kredit modul miqdori – 6 ECTS

Ta'lim turi	Ma'ruza	Amaliy mashg'ulot	Laboratoriya	Mustaqil ta'lim	Jami
Kunduzgi	30	42	0	108	180
Yillik, jami	**30**	42	**0**	**108**	**180**

CamScanner yordamida skanerlangan

9. Fanning tarkibiy tuzilishi

Kunduzgi:

T/r	Mavzular	Ma'ruza, amaliy va seminar mashg'ulotlar rejasi	Soatlar		
			Ma'ruza mashg'ulotlari	Amaliy mashg'ulotlari	Mustaqil ta'lim
1.	Kirish va kiberxavfsizlik asoslari.	1. Axborot xavfsizligini tahlil qilish: zaifliklarni aniqlash bo'yicha keys-stadi. 2. Real voqealar asosida axborot xavfsizligi buzilishlarini muhokama qilish.	2	2	8
2.	Kriptografiyaning asosiy tushunchalari va tarixi.	1. Shifrlash va deshifrlash bo'yicha oddiy amaliy mashqlar. 2. Klassik shifrlash usullari (Sezar, Vigenere)ni dasturiy tarzda amalga oshirish.	2	2	8
3.	Simmetrik shifrlar.	1. AES, DES shifrlash algoritmlarini amalda ishlatish. 2. Simmetrik shifrlash orqali faylni himoyalash va tiklash.	2	6	8
4.	Assimmetrik shifrlar.	1. RSA algoritmini dasturiy amalga oshirish. 2. Assimmetrik shifrlash orqali kalit almashinuvini modellashtirish.	2	6	8
5.	Autentifikatsiya.	1. Parol asosidagi autentifikatsiya tizimlarini amalda qo'llash. 2. Biometrik autentifikatsiya ishlash tamoyillarini tahlil qilish.	2	2	8
6.	Parollarga xujumlar va parollarni saqlash.	1. Parol mustahkamligini tekshirish (hash funksiyalar). 2. Lug'at bo'yicha hujum (dictionary attack) va rainbow table misollarini ko'rsatish.	2	2	8
7.	Ma'lumotlarni butunligi.	1. Elektron raqamli imzo yaratish va tekshirish. 2. Fayl yaxlitligini tekshirish (hashing – SHA256, MD5).	2	2	8

CamScanner yordamida skanerlangan

8.	Ma'lumotlarning fizik xavfsizligi.	1. Videokuzatuv tizimlari bo'yicha keys tahlili. 2. Foydalanuvchi kartalari va kalitlar bilan ishlash tajribasi.	2	2	8
9.	Diskh va faylli shifrlash. Malumotlarni xavfsiz chiqarib tashlash.	1. TrueCrypt/VeraCrypt yordamida diskni shifrlash. 2. Fayllarni GPG/PGP orqali shifrlash va ochish.	2	2	8
10.	Kompuyuter tarmoqlarining asoslari.	1. TCP/IP tarmoq modeli bo'yicha paketlarni kuzatish (Wireshark amaliyoti).	2	2	6
11.	Tarmoq havfsizligining tahdid va zaifliklari.	1. Tarmoq hujumlarini (DoS, sniffing) amaliy misollar orqali ko'rib chiqish.	2	2	6
12.	Tarmoqlararo ekran va virtual hususiy tarmoqlar.	1. Firewall sozlash va tarmoqlararo ekran imkoniyatlarini sinash. 2. VPN orqali xavfsiz ulanishni tashkil etish.	2	2	6
13.	Zararkunanda dasturiy ta'minot.	1. Antivirüs vositalari yordamida viruslarni aniqlash amaliyoti. 2. Virtual mashinada zararli dastur xatti-harakatini kuzatish.	2	2	6
14.	Axborot xavfsizligida inson omili.	1. Ijtimoiy muhandislik hujumlari bo'yicha keys-stadi. 2. Xodimlar uchun xavfsizlik bo'yicha trening mashqlari.	2	2	6
15.	Kelajakdagi xavfsizlik tahdidlari va tendensiyalari.	1. IoT qurilmalarida xavfsizlik zaifliklarini amaliy tahlil qilish. 2. Sun'iy intellekt yordamida hujumlarni aniqlashga oid keyslar.	2	2	6
Jami soat			**30**	**42**	**108**

10. Talabalar bilimini baholash

Maksimal va	Ma'ruza mashg'ulotlarida 30 ball	Amaliyot mashg'ulotlarida 30 ball	Jami	Yakuniy nazorat	Jami

CamScanner yordamida skanerlangan

<table>
<tr><td>saralash ballari</td><td>Oraliq nazoat uchun</td><td>Mustaqil ta'lim</td><td>Joriy nazorat uchun</td><td>Mustaqil ta'lim</td><td rowspan="4">60</td><td rowspan="3">40</td><td rowspan="4">100</td></tr>
<tr><td>Maksimal bal 100%</td><td>15</td><td>15</td><td>15</td><td>15</td></tr>
<tr><td>Saralash bali 60%</td><td colspan="4">Saralash bali 36 ball</td></tr>
<tr><td>Nazoratni o'tkazish muddati va shakli</td><td colspan="2">Fanning 70 foiz o'zlashtirilganda (yozma, amaliy ish, og'zaki)</td><td colspan="2">Amaliyot mashg'ulotlar davomida</td><td>YN test shaklida o'tkaziladi</td></tr>
</table>

Talabaning semestr davomida fan bo'yicha to'plagan umumiy bali har bir nazorat turidan belgilangan qoidalarga muvofiq quyidagi formula orqali hisoblanadi:

YaB=JN+MI1+ON+MI2+YaN

Bu yerda:

JN — joriy nazorat; MI1 — Mustaqil ish -1;

ON — oraliq nazorat; MI2 — Mustaqil ish -2;

YaN — yakuniy nazorat

Eslatma: dars mashg'ulotlaridagi ishtiroki, mustaqil ta'lim, joriy va oraliq nazoratlar uchun ajratilgan jami ballar (60 ball)ning kamida 60 foizi (36 ball)ni to'play olmagan talabaning yakuniy nazoratga kirishiga ruxsat berilmaydi.

11. Akademik talablar

O'qituvchi va talaba o'rtasidagi o'zaro munosabat samimiy va beg'araz bo'lishi lozim, Talaba(lar) tomonidan bajarilgan va topshirilgan mustaqil ta'lim mavzu/topshiriqlarini elektron ta'lim platformasi **(HEMIS) orqali yuboradi** va **javobni ham shu tartibda oladi.** Belgilangan muddatda bajarilmagan topshiriqlar qayta qabul qilinmaydi.

CamScanner yordamida skanerlangan

Talaba fan uchun ajratilgan kreditni fanning o'zlashtirish darajasi, olgan bahosiga proporsional tarzda oladi. Fan uchun ajratilgan soat bo'yicha talaba maksimal ball to'plashi kerak bo'lgan kredit miqdori 6 kreditni tashkil etadi.

O'quv-uslubiy boshqarma boshlig'i: **F.U.Odilov**

Fakultet dekani: **A.Y.Boboyev**

Kafedra mudiri: **J.R.Azimjonov**

Tuzuvchi: **N.T.O'rinov**

CamScanner yordamida skanerlangan