O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

“TASDIQLAYMAN”
Kiberxavfsizlik fakulteti dekani
Sh.G‘ulomov
2025-yil “26” 04

MOBIL XAVFSIZLIK

FANI BO‘YICHA

SILLABUS

Kunduzgi ta`lim uchun

Bilim sohasi:	600 000	– Axborot-kommunikatsiya texnologiyalari
Ta`lim sohasi:	610 000	– Axborot-kommunikatsiya texnologiyalari
Ta`lim yo‘nalishi:	60611200	– Kiberxavfsizlik injiniringi

Toshkent 2025

FAN SILLABUSI
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti bakalavriat

60611200 – Kiberxavfsizlik injiniringi yo'nalishlari

Fan nomi:	**Mobil xavfsizlik**
Fan turi:	Mutaxassislik tanlov fan
Fan kodi:	
Bosqich:	2
Semestr:	4
Ta'lim shakli:	Kunduzgi
Mashg'ulotlar shakli va semestrga ajratilgan soatlar:	180
Ma`ruza	42
Amaliy mashg`ulotlar	30
Laboratoriya mashg`ulotlari	-
Seminar	-
Mustaqil ta`lim	108
Sinov birligi miqdori:	6
Baholash shakli:	Imtixon
Fan tili:	O`zbek

Fan maqsadi (FM)	
FM1	Talabalarga kiberxavfsizlikni ta`minlash sohasida Mobil xavfsizlikning nazariy va amaliy izlanishlar orqali tanishtirish hisoblanadi. Mobil xavfsizlikni ta`minlashda foydalaniladigan turli zamonaviy yondashuvlar, usullar va vositalarni qo`llashga doir bilimlar va ko`nikmalar hosil qilishdan iborat.

Fanni o'zlashtirish uchun zarur boshlang'ich talablar	
1.	Yo`q

Ta'lim natijalari (TN)	
	Bilimlar jihatidan:
TN1	Mobil xavfsizlikning asosiy tushunchalarini aytib berish.
TN2	Mobil xavfsizlikning zaruriyatini asoslab berish.
TN3	Mobil xavfsizlikka tahdidlar tahlilini amalga oshirishni aytib berish.
TN4	Mobil xavfsizlikning universal usullarini tushuntira olish.
	Ko'nikmalar jihatidan:
TN5	Mobil xavfsizlik tahlilini amalga oshirish.
TN6	Mobil xavfsizlikning universal usullaridan foydalana olish.
TN7	GSM, UMTS, LTE kabi mobil tarmoqlar xavfsizligi tahlilini amalga oshirish.
TN8	Mobil tizimlar xavfsizligi tahlilini amalga oshirish.

Fan mazmuni	
Mashg'ulotlar shakli: ma'ruza (M)	
M1	Mobil xavfsizlikka kirish
M2	Asosiy xavfsizlik elementlari va kriptografik usullar (4 soat)
M3	GSM tarmoqlari xavfsizligi
M4	UMTS tarmoqlari xavfsizligi
M5	LTE tarmoq xavfsizligi
M6	WiFi va Bluetooth texnologiyalari xavfsizligi. (4 soat)
M7	SIM/UICC kartalari xavfsizligi (4 soat)
M8	Mobil ilovalar xavfsizligini ta'minlash usullari. (4 soat)
M9	Android operatsion tizimi xavfsizlik modeli
M10	iOS operatsion tizimi xavfsizlik modeli (4 soat)
M11	Windows Phone operatsion tizimi xavfsizlik modeli
M12	SMS/MMS, geolokatsiya va mobil veb tizimlari xavfsizligi (4 soat)
M13	Mobil VoIP aloqa tizimi xavfsizligi (4 soat)
M14	Mobil xavfsizlikdagi zamonaviy yo'nalishlar
Mashg'ulotlar shakli: amaliy mashg'ulot (A)	
A1	Android ilovalarining zaifliklarini topish
A2	AES, RSA algoritmlari yordamida shifrlash va deshifrlash . (4 soat)
A3	KASUMI algoritmi va o'zaro autentifikatsiya jarayonini tahlil qilish
A4	EPS AKA (Evolved Packet System Authentication and Key Agreement) protsedurasini simulyatsiya qilish va kalitlar iyerarxiyasini tahlil qilish . (4 soat)
A5	WPA2-PSK parolini buzish va WPA3 bilan farqlarini tahlil qilish. Bluetooth sniffing va MITM hujumlarining simulyatsiya qilish . (4 soat)
A6	SIM kartalarda OTA (Over-The-Air) hujumlarining mexanizmini tushuntirish va SIM kartani klonlash tahlili. (4 soat)
A7	Zararli android ilovasini MobSF va Genymotion dasturiy vositalari yordamida tekshirish
A8	Android ilova ruxsatlarini noto'g'ri sozlashni sinab ko'rish
A9	SMS firibgarligi tahdidlari haqida tahliliy ish bajarish
A10	SIP (Session Initiation Protocol) suhbati va shifrlanmagan trafikni Wireshark yordamida tahlil qilish . (4 soat)

Mustaqil ta'lim (MT)		
1.	**Seminar va amaliy mashg'ulotlarga tayyorgarlik ko'rish va uy ishlarini bajarish.**	**28 soat**
2.	**Har bir talaba ilmiy salohiyatdidan kelib chiqib tanlagan mavzuga mos referat tayyorlash va himoya qilish.**	**40 soat**
1.	Autentifikatsiya va Avtorizatsiya tizimlari: mobil muhitdagi qo'llanilishi	
2.	Kriptografik kalitlar bilan ishlash va xavfsiz boshqaruv mexanizmlari	
3.	Raqamli imzo texnologiyasi va mobil xavfsizlikdagi ahamiyati	
4.	Maxfiylik (Confidentiality) va ma'lumotlarni shifrlashning mobil qurilmalardagi roli	
5.	GSM (2G) tarmoqlaridagi xavfsizlik zaifliklari va A5 algoritmlari	
6.	IMSI Catcher: ishlash prinsipi va himoyalanish usullari	

7.	3G (UMTS) tarmog`idagi o`zaro autentifikatsiya va KASUMI shifrlash	
8.	LTE (4G) tarmog`i xavfsizlik arxitekturasi va EPS AKA protokoli	
9.	IMSI yashirish texnologiyasi va mobil maxfiylikni oshirish usullari	
10.	WPA2 va WPA3 xavfsizlik protokollari: taqqoslash va zaifliklar	
11.	Bluetooth ning birlashish jarayoni va MITM hujumlariga qarshi himoya	
12.	Mobil qurilmalarda sniffing xavfi va uni oldini olish choralari	
13.	WiFi va Bluetooth orqali mobil ma`lumotlarga hujumlar: amaliy misollar	
14.	SIM/UICC kartalarining autentifikatsiya jarayoni	
15.	OTA (Over-the-Air) buyrug`lari xavfsizligi va potentsial tahdidlar	
16.	SIM klonlash texnikasi va unga qarshi kurashish usullari	
17.	Mobil zararli dasturlar turlari: spyware, ransomware, trojan	
18.	Android ilovalarda ruxsatlar bilan bog`liq xavfsizlik muammolari	
19.	Ilova xavfsizligini tahlil qilish: statik va dinamik tahlil	
20.	Android xavfsizlik modeli: sandbox, ruxsatlar va SELinux	
21.	Root qilingan qurilmalardagi xavflar va himoya choralari	
22.	iOS xavfsizlik modeli: Secure Boot, Keychain va App Sandboxing	
23.	Touch ID, Face ID va biometrik autentifikatsiya xavfsizligi	
24.	Jailbreak tahdidlari va Apple ning cheklash mexanizmlari	
25.	Windows Phone xavfsizligi va AppContainer texnologiyasi	
26.	SMS firibgarligi va MMS orqali zararli fayllar tarqatilishi	
27.	Geolokatsiya va foydalanuvchini kuzatish xavflari	
28.	Mobil veb brauzerlardagi zaifliklar: phishing, XSS	
29.	VoIP xizmatlari xavfsizligi: WhatsApp, Skype va boshqalar	
30.	SIP, SRTP va ZRTP protokollarining xavfsizlik taqqoslanishi	
3.	**Berilgan mavzu bo`yicha taqdimot tayyorlash**	**40 soat**
1.	Suniy yo`ldosh tizmlari yordamida globol mobil tizimlarni yaratish usullari.	
2.	Mobil kriptografik algoritmlar: AES, RSA va SHA taqqoslanishi	
3.	Mobil tizimlar uchun yaaratilgan operatsion tizimlar.	
4.	Shaxsiy mobil tarmoqlar.	
5.	IMSI yashirish texnologiyasi va mobil maxfiylikni oshirish usullari	
6.	Mobil tizimlarga yo`naltirilgan xavf extimollari va ularni bartaraf etish usullari.	
7.	IEEE 802.1x/EAP standarti tahlili.	
8.	Mobil xavfsizlik texnologiyalari va himoyalangan mobil sigmentni yaratish usullari.	
9.	Mobil VPN texnologiyasi.	
10.	Mobil xavfsizlik uchun kriptografik himoya usullari.	
11.	Mobil ma`lumotlar uzatish standartlari.	
12.	Mobil dasturlarda xavf extimollari va ularni bartaraf etish	
13.	Suhbatlarni yozib olish va identifikatsiyani soxtalashtirish xavflari	
14.	Suqulib kirishlarga testlash va hisobotlarini tayyorlash	
15.	Zero Trust Arxitekturasi va SI asosidagi zararli harakatlarni aniqlash	
16.	Mobil hisoblashlardan foydalanish usullari.	
17.	Mobil tizmlar xavfsizligida buluth texnologiyalarning o`rni.	

18.	Zero-Day zaifliklar va mobil platformalarga ta'siri
19.	Ilova do'konlari (App Store, Google Play) xavfsizlik siyosati va nazorat mexanizmlari
20.	Mobil qurilmalarda foydalanuvchi identifikatsiyasi va biometrik autentifikatsiya xavfsizligi
21.	Mobil tizimlarni joriy etishda xavfsizlik siyosatini joriy etishga yo'naltirilgan talablar
22.	Mobil tizimlar xavfsizligiga yo'naltirilgan zararkunanda dasturlar.
23.	Mobil tizim va tarmoq xavfsizligi auditi.
24.	4G va LTE o'rtasidagi farqlar tahlili.
25.	5G texnologiyasi tahlili.
26.	Mobil ilovalarda ma'lumotlar saqlanishi va shifrlash amaliyoti
27.	Mobile Device Management (MDM) tizimlari: tashkilotlar uchun xavfsizlik yechimi
28.	Mobil qurilmalarda SI yordamida zararli faoliyatni aniqlash usullari
29.	6G texnologiyasi tahlili.
30.	Mobil qurilmalarda tarmoq monitoringi va trafikni tahlil qilish

Talabaning fan bo'yicha o'zlashtirish ko'rsatkichini nazorat qilishda quyidagi mezonlar tavsiya etiladi:

a) 5 baho «a'lo» (90-100) olish uchun talabaning bilim darajasi quyidagilarga javob berishi lozim:

- mobil xavfsizlik tushunchalarni aniq yoritib berish;
- mobil xavfsizlikni taminlashda foydalaniladigan usullar va vositalar haqida kengroq bilishi;
- mobil tizimlar xavfsizligi, tahdidlari, mexanizmlari haqida bilimga ega bo'lish;
- mobil tizimlar himoyasini taminlash usullari, vositalari, muhitlari haqida bilimga ega bo'lishi;
- mobil xavfsizlik darjasini tahlil qila olish va qo'shimcha dasturiy vositalardan foydalana olish.

b) 4 baho «yaxshi» (70-89) olish uchun talabaning bilim darajasi quyidagilarga javob berishi lozim:

- mobil xavfsizlik tushunchalarni aniq yoritib berish;
- mobil xavfsizlikni ta'minlashda foydalaniladigan usullar va vositalar haqida kengroq bilishi;
- mobil tizimlar himoyasini taminlash usullari, vositalari, muhitlari haqida bilimga ega bo'lishi;
- mobil xavfsizlik darjasini tahlil qila olish va qo'shimcha dasturiy vositalardan foydalana olish.

d) 3 baho «qoniqarli» (60-69) olish uchun talabaning bilim darajasi quyidagilarga javob berishi lozim:

- mobil xavfsizlik mohiyatini tushunish;
- mobil xavfsizlik sohasida vositalar haqida ma'lumotga ega bo'lish;
- mobil xavsizlik darajasini belgilay olish.

e) quyidagi hollarda talabaning bilim darajasi qoniqarsiz 2 baho (0-59) bilan baholanishi mumkin:

- mobil xavfsizlik mohiyatini tushunmaslik;
- mobil xavfsizlikni asoslarini bilmaslik, aytib bera olmaslik;
- mobil xavfsizlik sohasidagi vositalar haqida tushunchaga ega bo'lmaslik.

Reyting baholash turlari	%	O'tkazish vaqti
Joriy baholash:	**20**	
Amaliy mashg'ulotlarda faolligi, savollarga to'g'ri javob berganligi, amaliy topshiriqlarni bajarganligi uchun: 1-amaliy ish uchun: 2% 2-amaliy ish uchun: 2% 3-amaliy ish uchun: 2% 4-amaliy ish uchun: 2% 5-amaliy ish uchun: 2% 6-amaliy ish uchun: 2% 7-amaliy ish uchun: 2% 8-amaliy ish uchun: 2% 9-amaliy ish uchun: 2% 10-amaliy ish uchun: 2%	20	Semestr davomida
Oraliq baholash:	**30**	
Oraliq nazorat yozma ish (ma'ruzachi o'qituvchi tomonidan qabul qilinadi).	15	14-hafta
Mustaqil ta'lim topshiriqlarining o'z vaqtida va sifatli bajarilishi: - referat tayyorlash: 8% - taqdimot tayyorlash va himoya qilish: 7%.	15	Semestr davomida
Yakuniy nazorat	**50**	16-hafta
JAMI:	**100**	

	Asosiy adabiyotlar
1.	S.K.Ganiev., T.A.Kuchkarov. Tarmoq Xavfsizligi (Mobil Tarmoq Xavfsizligi). 2018. 159 b.
2.	Sougata Mukherjea. IBM India. Mobile Application Development, Usability, and Security. Published in the United States of America by IGI Global. 2016. -P. -340.
3.	Himanshu Dwivedi., Chris Clark., David Thiel. Mobile Application Security. Copyright 2010 by The McGraw-Hill Companies. 2009. -P. -432.
	Qo'shimcha adabiyotlar
1.	Security of Mobile Communications. Noureddine Boudriga. 2009
2.	I.S. Olimov, S.M. Bozorov, E.D. Haydarov, B.B. Turdibekov "Kiberxavfsizlik asoslari". Uslubiy ko'rsatma. -Toshkent: TATU. 2022. -124 b.
3.	Mobile Operating System Security A Complete Guide - 2021 Edition
	Elektron manbalar:
1.	https://www.fortinet.com/resources/cyberglossary/mobile-security
2.	https://techwell.com.au/blogs/why-is-mobile-security-important-how-to-protect-yourself/
3.	https://blog.rsisecurity.com/importance-of-mobile-security/
4.	https://www.proofpoint.com/uk/threat-reference/mobile-security
5.	https://www.site2.com/cybersecurity/mobile-security
6.	https://www.techtarget.com/whatis/definition/mobile-security
7.	https://www.kaspersky.com/resource-center/definitions/what-is-mobile-security
8.	https://en.wikipedia.org/wiki/Mobile_security
9.	https://www.ibm.com/think/topics/mobile-security

Fan o'qituvchisi to'g'risida ma'lumot

Dastur mualliflari:	Salimov Sirojiddin
E-mail:	sirojiddin1224@gmail.com
Tashkilot:	Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti, "Kiberxavfsizlik va Kriminalistika" kafedrasi.

Fanning sillabusi Universitet Kengashining 2025-yil "29"-04 dagi 8/9 -son bayonnomasi bilan tasdiqlangan. (450/751)

Fanning sillabusi "Kiberxavfsizlik va kriminalistika" kafedrasining 2025-yil 17"-04 dagi 14- son bayonnomasi bilan tasdiqlangan.

O'quv-uslubiy boshqarma boshlig'i A. Ergashev

Fakultet dekani Sh. G'ulomov

Kafedra mudiri O. Allanov

Tuzuvchi S. Salimov