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

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

“TASDIQLAYMAN”
“Kiberxavfsizlik” fakulteti dekani
_____ Sh.R.G‘ulomov
“10” 04 2025 yil

AXBOROTNI HIMOYALASHNING DASTURIY VA APPARAT VOSITALARI FANI BO‘YICHA SILLABUS

Kunduzgi ta’lim uchun

Bilim sohasi:	600000	– Axborot-kommunikatsiya texnologiyalari
Ta’lim sohasi:	610000	– Axborot-kommunikatsiya texnologiyalari
Ta’lim yo‘nalishi:	60610200	– Axborot xavfsizligi

Toshkent – 2025

Fan nomi:	**Axborotni himoyalashning dasturiy va apparat vositalari**
Fan turi:	Tanlov
Fan kodi:	SHDM26TBK
Bosqich:	2
Semestr:	4
Ta'lim shakli:	Kunduzgi
Mashg'ulotlar shakli va semestrga ajratilgan soatlar:	180
Ma'ruza	42
Amaliy mashg'ulotlar	30
Laboratoriya ishi	-
Seminar	-
Mustaqil ta'lim	108
Sinov birligi miqdori:	6
Baholash shakli:	imtihon
Fan tili:	O'zbek

Fanning qisqacha mazmuni (QM)	
QM1	Talabalarga axborotni himoyalashning zamonaviy dasturiy va apparat vositalarini chuqur o'rgatish, tahdidlarni aniqlash va baholash, xavfsizlik yechimlarini ishlab chiqish, ularni amaliy tizimlarga tatbiq qilish ko'nikmalarini shakllantirishni maqsad qiladi. Bundan tashqari, fan talabalarda real muammolarni hal qilishga yo'naltirilgan mustaqil fikrlashni, xavfsizlik strategiyalarini loyihalash va joriy etish malakasini rivojlantirishga xizmat qiladi. Talabalar nafaqat mavjud xavfsizlik vositalari bilan tanishadi, balki ularni tanlash, sozlash, testdan o'tkazish va auditi bo'yicha zamonaviy yondashuvlarni o'zlashtiradilar.

Fanni o'zlashtirish uchun zarur bo'lgan asosiy bilimlar	
1.	Kiberxavfsizlik asoslari

Ta'lim natijalari (TN)	
Kursni tugatgandan so'ng, talaba quyidagilarni bilishi kerak:	
TN1	Axborotni himoyalashning muhim yo'nalishlari va texnologiyalarini.
TN2	Dasturiy va apparat xavfsizlik vositalarining imkoniyatlarini farqlaydi.
TN3	Himoya vositalarini real tizimlarga joriy etadi/
TN4	Testlash va baholash vositalaridan foydalanadi.
TN5	Mustaqil tarzda xavfsizlik strategiyalarini ishlab chiqadi.

Mashg‘ulotlar shakli: ma’ruza (M)		Soat
M1.	**Fanga kirish.** Apparat va dasturiy vositalarning xavfsizlik muammolari hamda ularning ta’siri.	2
M2.	**Dasturiy vositalarning xavfsizligini ta’minlashda apparat vositalarning xususiyatlari.** Apparat-Dastur arxitekturasiga ilk qadam: yuklovchi modul (bootloader), dastlabku yuklash (Early Boot), yadro (kernel), foydalanuvchi interfeysi uchun boshlang‘ich konfiguratsiya bosqichi (Early Userspace), tizimni faollashtirishning fundamental vositasi (Init System), tizimning yakuniy foydalanuvchi muhiti (Late Userspace).	4
M3.	**Apparat vositalar xavfsizligining asosiy funksyalari:** bajarilmaydigan xotira (NX memory – Non executable memory), virtual xotira (virtual memory)	2
M4.	**Xavfsiz qism protsessorlar.** Ishonchli platforma moduli (Trusted Platform Module-TPM) va Apparatli xavfsizlik moduli (Hardware Security Module - HSM), maxfiy ma’lumotlarni boshqarish (secret handling), Ishonchli platforma modulining boshqaruv mexanizmi (Trusted Platform Module Management Engine - TPM ME), Xavfsizlik darajasini baholash uchun mo‘ljallangan bajarish va yuklash modeli (Measured execution and measured boot), Xavfsiz yuklash (Secure boot), Xavfsizlik imkoniyatlaridan foydalanuvchi dasturiy ta’minot arxitekturalari (Software patterns that leverage these)	4
M5.	**“Kengaytirilgan” (Advanced) protsessor darajasidagi xavfsizlik xususiyatlari**. (Virtualizatsiya ko‘rsatmalari va qo‘ng‘iroq -1 (shuningdek, ARM); Gipervisor turlari; Paravirtualizatsiya va virtual apparat; ARMv8 da yadro nom maydonlari va konteynerlar ko‘rsatkichi autentifikatsiyasi; Imkoniyatli apparat ta’minoti bo‘yicha kengaytirilgan RISC ko‘rsatmalari (CHERI))	4
M6.	**Kengaytirilgan protsessor xavfsizligi**. Xavfsiz muhitlar (enclave): SGX va TrustZone; Masofaviy ishonch tasdig'i (remote attestation) va muhit sertifikatlari; Xavfsiz muhitlar uchun dasturlash.	2
M7.	**Protsessorlar:** Ishonchli domen kengaytmalari (Intel TDX). Yengil virtual mashinalar (Lightweight VMs). oraliq nazorat va oraliq tahlil (midterm review)	2
M8.	**Akseleratorlar va qo‘llaniluvchi protsessorlar hamda ko‘p protsessorli xavfsizlik.** Ko‘p protsessorli va ko‘p yadroli himoya usullari; chuqur o‘rganish (deep learning) akseleratorlari va asosiy dastur bilan o‘zaro ta’siri; boshqa periferik qurilmalar bilan bog‘liq xavfsizlik.	4
M9.	**Apparat vositalarga bo‘ladigan dasturiy hujumlar.** Yon kanal hujumlari asoslari: vaqtga asoslangan hujumlar (timing attacks); maxfiy kalitlar va parollarni ajratib olish; doimiy vaqt solishtirish (constant-time compare) va boshqa himoyalar.	4
M10.	**Yon kanal hujumlari.** Oldindan bashorat qilinadigan bajarish mexanizmi. Spectre, Meltdown va ularga o‘xshash xavfsizlik zaifliklari. Dasturiy ta’minot darajasidagi bartaraf etish choralari (masalan, retpoline).	2
M11.	**Apparat vositalarga bo‘ladigan dasturiy hujumlar.** Rowhammer hujumlari; Protsessorning eskirishi (aging); Amaliy misollar: flip feng shui; Rowhammer va eskirishdan himoyalanish usullari.	4
M12.	**Firmwarega qarshi hujumlar.** Firmware yangilash vektorlari va ulardan foydalanish orqali exploit qilish. Arm TrustZone-ni exploit qilish. Tegishli dasturiy himoya choralari..	2
M13.	**Firmware, apparat fuzzing va nosozlikni kiritish (fault injection).** Dvoich (binary) dasturlarni boshqa muhitda ishga tushirish orqali fuzzing; yashirin protsessor buyruqlari (chip fuzzing); ISA va protsessor implementatsiyasi orasidagi farq; periferik qurilmalarni fuzz qilish; sun’iy nosozlik kiritish.	4

M14.	**Turli hujumlar va himoya usullari.** VLSI dasturiy ta'minot yo'nalishiga qarshi hujumlar; Apparatga oid dasturiy ta'minotning ta'minot zanjiriga hujumlar; FPGA xavfsizligi.	2
	Jami:	**42**
Mashg'ulotlar shakli: amaliyot (A)		**Soat**
A1	GRUB va init tizimining ishlashini kuzatish. dmesg, journalctl vositalari bilan boot jarayonini tekshirish.	4
A2	GDB orqali bufer toshib ketishi (buffer overflow) holatlarini sinash. NX xotira bilan himoyalanishni kuzatish.	4
A3	tpm2-tools orqali TPM funksiyalarini ko'rish, maxfiy kalitlar yaratish va saqlash.	4
A4	VirtualBox / KVM yordamida virtual mashina yaratish, Docker orqali izolyatsiya mexanizmini sinash.	2
A5	ARM TrustZone yoki SGX emulyatori orqali xavfsiz hudud (enclave) yaratish va ishlatish.	4
A6	AWS Firecracker asosida yengil VM yaratish va ishga tushirish, tahlil qilish	4
A7	htop, taskset, va perf orqali bir nechta yadrodagi dasturlarni tahlil qilish.	4
A8	AFL, QEMU yordamida oddiy fuzzing; fault injection konseptini ko'rish.	4
	Jami:	**30**

№	Mustaqil ta'lim (MT)	Soat hajmi
MI1	Tahliliy referat: "Dasturiy xavfsizlik vositalarining solishtirma tahlili"	**15**
MI2	Taqdimot: "Apparat tahdidlar va ularga qarshi zamonaviy choralar"	**15**
MI3	Online laboratoriyalar (Cybrary, HackTheBox, Cisco Netacad, Google Cloud Labs)	**45**
MI4	Kitob va maqolalar o'qish: Stallings, Anderson, OWASP, ISO/NIST hujjatlari	**33**
	Jami:	**108**

Ta'lim strategiyasi

Axborotni himoyalashning dasturiy va apparat vositalari kursini o'qitish ta'limning kredit tizimi asosida ma'ruza, amaliyot mashg'ulotlari, taqdimotlar, hamda mavzu bo'yicha vazifalar va mustaqil topshiriqlarni o'z ichiga oladi.

Ma'ruza, amaliyot ishlariga oid o'quv materiallarida ko'rsatilgan mavzular bo'yicha nazariy va amaliy ma`lumotlar beriladi, amaliyot ishlarini bajarish va natijalarni hisoblash tartibi tushuntiriladi. Kurs bo'yicha qo'yilgan o'quv materiallari talabalar tomonidan mustaqil o'rganiladi, testlar, amaliyot ishlari talabalar tomonidan individual tarzda bajariladi.

Talabalar quyidagi materiallardan foydalanish imkoniga egadirlar:

- Elektron shakldagi ma'ruza matnlari;
- Har bir mavzuga doir taqdimot materiallari;
- Amaliyot mashg'ulotlariga doir uslubiy ko'rsatmalar;
- Har bir dars mavzusi yuzasidan nazorat savollari;
- Elektron shakldagi darsliklar va qo'llanmalar.

Ma'ruza davomida, talabaga taqdimot materiallari orqali mavzu yuzasidan kerakli bo'lgan konsepsiyalar yetkazib beriladi. Talabalarga mavzuni yanada mustahkamlashlari uchun prezentasiyalar, darsliklar, o'quv qo'llanmalari va boshqa o'quv-uslubiy mahsulotlardan foydalanish bo'yicha ko'rsatmalar beriladi. Talabalarning mavzuni

o‘zlashtirish darajasini tekshirish maqsadida, har bir mavzudan so‘ng nazorat savollari beriladi.

Amaliyot mashg‘ulotlarda har bir mavzu bo‘yicha masalalarni yechish bo‘yicha materiallar, prezentasiyalar, ko‘rsatmalar talabalarga taqdim etiladi, shuningdek, mavzuni o‘zlashtirish darajasini tekshirish maqsadida topshiriqlar beriladi.

Ma’ruza va amaliyot mashg‘ulotlarining barcha mavzularini to‘la o‘zlashtirgan talabalarga yakuniy nazoratda ishtirok etishga ruxsat etiladi. Talaba semestr oxirida universitetga kelib, yakuniy nazorat topshiradi.

Talabalarni baholash

Talabalar bilimini baholash semestr va yakuniy nazorat davomida o‘qitish materiallarini o‘zlashtirish ko‘rsatkichi (test, topshiriq va yozma ish natijasi)ga asoslangan.

Axborotni himoya qilishning dasturiy va apparat vositalari kursi davomida talabalar 100 ballik tizimda baholanadi. Shundan 50% ball mustaqil ish, joriy va oraliq natijasiga baholash uchun beriladi, qolgan 50% ball esa yakuniy nazorat natijasiga ajratiladi.

Joriy va oraliq ballarning umumiy natijasi 30 balldan past bo‘lgan talabalar yakuniy nazorat imtixoniga kiritilmaydi. Yakuniy nazoratda 30 va undan ko‘p ball to‘plagan talaba fanni o‘zlashtirgan hisoblanadi.

Joriy oraliq va yakuniy nazorat ballari quyidagicha taqsimlanadi:

	Reyting baholash turlari	%	O‘tkazish vaqti
	Joriy baholash:	**20**	
1.	Amaliy ish № 1: 2%	20	Semestr davomida
2.	Amaliy ish № 2: 2%		
3.	Amaliy ish № 3: 2%		
4.	Amaliy ish № 4: 2%		
5.	Amaliy ish № 5: 4%		
6.	Amaliy ish № 6: 2%		
7.	Amaliy ish № 7: 2%		
8.	Amaliy ish № 8: 4%		
	Oraliq baholash	**30**	
	Oraliq nazorat yozma ish hisoblanadi (ma’ruzachi tomonidan qabul qilinadi).	15	14-hafta
	Mustaqil o'quv topshiriqlarini o'z vaqtida va sifatli bajarish: - referat tayyorlash: 5 % - taqdimot tayyorlash va himoya qilish: 10 %	15	Semestr davomida
	Yakuniy nazorat	**50**	16-hafta
	Jami:	**100**	

	Asosiy adabiyotlar
1.	Blue Fox: Arm Assembly Internals & Reverse Engineering , Markstedter, Maria , Wiley , 2023 , ISBN No. 978-1-119-74530-3
2.	Principles of Secure Processor Architecture Design , Szefer, Jakub , Springer , 2018 , ISBN No. 978-3-031-00632-6
3.	Trusted Computing Platforms: TPM2.0 in Context , Proudler, Graeme; Chen, Liqun; Dalton, Chris , Springer , 2015 , ISBN No. 978-3319087436
4.	В.А. Гриднев, Ю.А. Губсков, А.С. Дерябин, А.В. Яковлев. "Программно-аппаратные Средства защиты Информации". В трех частях Часть 3. ISBN 978-5-8265-2464-0. 2024 г.
5.	S.K.Ganiev, A.A.Ganiev, Z.T.Xudoykulov. Kiberxavfsizlik asoslari: O'quv qo'llanma, – T. "Nihol print" OK, 2021. – 224 b.
	Tavsiya qilinadigan qo'shimcha adabiyotlar
1.	Anderson, Ross J.."Security Engineering: A Guide to Building Dependable Distributed Systems" 3rd Edition. ISBN 10: 1119642787 . ISBN 13: 978-1119642787. December 22, 2020
2.	William Stallings. "Cryptography and Network Security: Principles and Practice". ISBN 10: 0-13-609704-9. ISBN 13: 978-0-13-609704-4
3.	Matt Bishop. "Computer Security: Art and Science"
4.	"Axborot texnologiyasi. Axborotlarni kriptografik muxofazasi. Ma'lumotlarni shifrlash algoritmi" O'zbekiston Davlat standarti. O'zDSt 1105:2009.
5.	Хорев П.Б. "Программно-аппаратная защита информации". Учебное пособие, Москва 2019, с.352
	Elektron manbalar:
1.	https://uzinfocom.uz/uz/
2.	https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2018-2019/
3.	https://www.securitylab.ru/news/499156.php
4.	https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf

Fan o'qituvchisi haqida ma'lumot

Dastur mualliflari:	Xolimtayeva Iqbol Ubaydullayevna Fayziyeva Dilsora Salimovna
E-mail:	iqbola.ubaydullayevna@gmail.com dilsora.salimovna@gmail.com
Tashkilot:	Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, "Axborot xavfsizligi" kafedrasi
Taqrizchilar:	Axmedova O.P. – Fan texnika va marketing tadqiqotlari markazi – "UNICON.UZ" MChJ Axborot xavfsizligi va kriptologiya Ilmiy-tadqiqot bo'limi boshlig'i, t.f.n. (turdosh ITM). Kerimov K.F. – Muhammad al-Xorazmiy nomidagi TATU, "Tizimli va amaliy dasturlashtirish" kafedrasi professori, t.f.d..

Mazkur Sillabus "Axborot xavfsizligi" kafedrasining 2025-yil 09.04 dagi 15-sonli yig'ilish bayoni bilan ma'qullangan.

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

Kafedra mudiri E.D. Haydarov

Tuzuvchilar I.U. Xolimtayeva

D.S. Fayziyeva