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

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

Ro‘yxatga olindi:
№ 8/9/750/931
2025-yil "29" 04.

"TASDIQLAYMAN"
O‘quv ishlari bo‘yicha prorektor
D.Sattarov
"29" 04 2025-yil

FOYDALANISHLARNI BOSHQARISH

FANINING O‘QUV DASTURI

Bilim sohasi:	600 000 –	Axborot-kommunikatsiya texnologiyalari
Ta’lim sohasi:	610 000 –	Axborot-kommunikatsiya texnologiyalari
Ta’lim yo‘nalishlari:	60610300 –	Axborot xavfsizligi (axborot kommunikatsiya texnologiyalari va servis)
	60612100 –	Kiberxavfsizlik injiniringi

Toshkent – 2025

Fan/modul kodi ACON16MBK	O'quv yili 2025-2026	Semestr 5	ECTS - kreditlar 6
Fan/modul turi Majburiy	Ta'lim tili O'zbek/rus		Xaftadagi dars soatlari 4/6

1.	Fanning nomi	Auditoriya mashg'ulotlari (soat)	Mustaqil ta'lim (soat)	Jami yuklama (soat)
	Foydalanishlarni boshqarish	72	**108**	**180**

2. **I. Fanning mazmuni**

Fanni o'qitishdan maqsad – talabalarga foydalanishni boshqarish sohasining asosiy tushunchalari, modellashtirish usullari, xavfsizlik siyosatlari, rollarga asoslangan boshqaruv tizimlari, operatsion tizimlardagi foydalanish nazorati va ishonchli boshqaruv yondashuvlari haqida chuqur nazariy va amaliy bilim berishdir.

Fanning vazifasi — foydalanishni boshqarishning mandatli va diskretsion modellari, Bell-LaPadula, Noninterference, RBAC kabi xavfsizlik modellari, operatsion tizimlar va taqsimlangan tizimlardagi foydalanishni boshqarish mexanizmlari, mantiqiy dasturlash asosida ishonchli boshqaruv, shuningdek, zamonaviy AT\N texnologiyalaridagi avtomatlashtirilgan ishonchli muzokaralarni tushunish, tahlil qilish, modellashtirish va amaliyotda qo'llay olish ko'nikmalarini shakllantirishdan iborat.

II. Asosiy nazariy qism (ma'ruza mashg'ulotlari)

II.I. Fan tarkibiga quyidagi mavzular kiradi:

1-bo'lim. Fanga kirish

1-mavzu. Foydalanishni boshqarish faniga kirish

Foydalanishni boshqarish. Foydalanishni boshqarishning keng tarqalishi. Foydalanishni boshqarishning muhimligi. Foydalanishni boshqarish tamoyillari. Foydalanishni boshqarish sohasida tadqiqotlar tarixi. Ma'lumotlar bazasiga foydalanishni boshqarish. Konfidensiallik. Yaxlitlik. Foydalanuvchanlik. Taqsimlangan tizimlarda foydalanishni boshqarish.

2-mavzu. Foydalanish matritsasi, modellashtirish tizimlari

Foydalanishni boshqarish matritsasi modeli. Tizimning rasmiy modelga bo'lgan ehtiyoji. Kripke tuzilmalari. Reaktiv tizimlarni modellashtirish.

2-bo'lim. Konfidentsiyallikni ta'minlash uchun mandatli foydalanishni boshqarish

3-mavzu. Bell-LaPadula modeli (4 soat)

BLP ning asosiy maqsadi. BLPda metodologiya. BLPning yondashuvi BLP ning asosiy tashkil etuvchilari. BLP ning asosiy texnik kamchiliklari. Asosiy xavfsizlik teoremasi. Xavfsizlikni statik tekshirish.

4-mavzu. Aralashuvsizlik (Noninterference) va xulosa qilib bo'lmaslik (Nondeducibility) modellari

Xavfsizlik siyosati va modellari. Aralashuvsizlik (Noninterference) va BLP ni taqqoslash. Aralashuvsizlik (Noninterference) siyosatini baholash. Axborot modeli. Aralashuvsizlik (Noninterference) va xulosa qilib bo'lmaslik (Nondeducibility) o'rtasidagi bog'liqliklar.

5-mavzu. Axborot oqimi, cheklash va yashirin kanallar

Axborot oqimini nazorat qilishda panjara (lattice) modeli. Cheklov muammosi haqida izoh. Yashirin kanallardagi munozaralar.

3-bo'lim. Yaxlitlik

6-mavzu. Kompyuter tizimlari xavfsizligini ta'minlashda yaxlitlik muammolari (4 soat)

Bibaning yaxlitlik siyosati. Beshta mandatli siyosatlar. Maxfiylik va yaxlitlik o'rtasidagi asosiy farqlar.

4-bo'lim. Diskretsion foydalanishlarni boshqarish va xavfsizlik tahlili

7-mavzu. Formallashtirilgan foydalanishni boshqarish matritsalari (4-soat)

Graham-Denning modeli. Graham-Denning modelidagi sakkizta buyruq. Harrison-Ruzzo-Ullman (HRU) modeli. HRUda xavfsizlik tahlili.

5-bo'lim. Rolli foydalanishni boshqarish modeli

8-mavzu. Rolli foydalanishni boshqarish

RBAC96 Modellar oilasi. Foydalanuvchi, rol va imtiyoz tushunchalari. Vazifalarni ajratish. Eng kichik imtiyoz. Rollar iyerarxiyasi. RBAC uchun NIST standartiga umumiy sharh.

9-mavzu. Rolli foydalanishni boshqarish modeli asosida cheklash (4 soat).

SoD(Separation of Duties) siyosati va cheklovlari. SoD va RBAC. SMER(Security Management and Evaluation Requirements) cheklovlari. SsoD (Single Separation of Duties) va SMER. Majburiy tekshirish (EV) muammosi. Kengaytirilgan EV (CEV) muammosi.

6-bo'lim. Operatsion tizimda foydalanishni boshqarish

10-mavzu. UNIX operatsion tizimida foydalanishni boshqarish

Foydalanuvchilar va guruhlar. Demistifikatsiyalangan SETUID. Foydalanuvchi ID modeli. Dastlabki va zamonaviy UNIX OTda foydalanishni boshqarish.

11-mavzu. UNIX jarayonlarini cheklash

UNIX chroot() operatsiyalari. Jail - FreeBSD-da amalga oshirilgan chroot kengaytmasi. Ildiz dasturlarini domen va turlarni qo'llash bilan cheklash. Tizimning ikkilik fayllarini Rootkit-dan himoya qilish. UNIXda foydalanishni boshqarishning umumiy tavsifi.

12-mavzu. Imtiyozlarga asoslangan tizimlar

C-list va ACL. KeyKOS-dagi asosiy tushunchalar. OTda qo'llaniladigan to'rta model(ACLs as columns (of access matrices). Capabilities as rows. Capabilities as keys. Object capabilities)

7-bo'lim. Ishonchli boshqarish va avtomatlashtirilgan ishonch muzokaralari

13-mavzu. Mantiq va mantiqiy dasturlash asoslari (4 soat)

Mantiq. Mantiq turlari. Aniq mantiqiy dasturlar (Definite Logic Programs). Aniq klauzalar (Definite Clauses). Aniq dasturlar va maqsadlar (Definite Programs and Goals). Eng kichik Herbrand modeli (The Least Herbrand Model). Eng kichik Herbrand modellarini qurish (Construction of Least Herbrand Models). Noformal kirish (Informal Introduction). Birlashma (Unification). SLD-qarorlashtirish (SLD-Resolution). SLD-qarorlashtirishning to'g'riligi (Soundness of SLD-resolution). SLD-qarorlashtirishning to'liqligi (Completeness of SLD-resolution). Isbot daraxtlari (Proof Trees).

14-mavzu. OACerts yordamida avtomatlashtirilgan ishonchli muzokaralar

Markazlashtirilmagan foydalanishni boshqarish. Avtomatlashtirilgan ishonchli muzokaralar. Kriptografik majburiyat sxemasi. Maxfiy atribut sertifikatlari (Oblivious Attribute Certificates). Maxfiy majburiyat asosidagi konvert (Oblivious Commitment-Based Envelope). OACertsni ATNga integratsiyalash.

15-mavzu. Ishonchli boshqaruv bo'yicha umumiy ma'lumotlar

Taqsimlangan avtorizatsiya. Ishonchli boshqaruv (TM) yondashuvlari. Ochiq kalit sertifikatlari. Ochiq kalit infratuzilmalarining mavjud turlari (PKI). Ishonchli boshqaruv tillari. SPKI/SDSI da sertifikat zanjiri.

	16-mavzu. Ishonchli boshqaruvda taqsimlangan hisob ma'lumotlari zanjirining tadqiqi Rolga asoslangan ishonchli boshqaruv tillari. RT0 and SDSI 2.0 tillari. Ilg'or qidirish algoritmi. Backward va Bi-direction algoritmlari. Rolga asoslangan ishonchli boshqaruv tizimini loyihalash. **III. Amaliy mashg'ulotlar bo'yicha ko'rsatma va tavsiyalar** *Amaliy mashg'ulotlar uchun quyidagi mavzular tavsiya etiladi:* 1. Foydalanishni boshqarish matritsasi asosida foydalanuvchi huquqlarini boshqarish. 2. Bell-LaPadula modeli asosida axborot xavfsizligini ta'minlash. 3. Axborot oqimi modeli asosida axborot oqimini boshqarish va tahlil qilish (4-soat). 4. Biba modeli asosida axborot yaxlitligini himoyalash. 5. Clark-Wilson modeli asosida axborot yaxlitligini ta'minlash (4-soat). 6. Graham-Denning va Harrison-Ruzzo-Ullman (HRU) xavfsizlik modellari bo'yicha axborot tizimlaridan foydalanishni boshqarish (4-soat). 7. Rolli foydalanishni boshqarish modeli asosida xavfsizlik tizimini qurish (4-soat). 8. Linux OTda foydalanishni boshqarish (4-soat). 9. OACerts yaratish va OpenSSL yordamida ishonchni tasdiqlash (4-soat). **IV. Mustaqil ta'lim va mustaqil ishlar** *Mustaqil ta'lim uchun tavsiya etiladigan topshiriqlar:* 1. RBAC yordamida Bell-LaPadula xavfsizlik siyosatini modellashtirish. 2. MLS siyosatiga asoslangan maxfiylik va yaxlitlikni ta'minlovchi xavfsizlik modeli. 3. Xavfsizlik modellari tahlili. 4. Kompyuter xavfsizligini modellashtirish. 5. Xavfsizlik siyosati va xavfsizlik modellari. 6. Xavfsiz axborot oqimining panjara modeli. 7. Konfiniyatsiya(izolyatsiya) muammosi. 8. Tijorat va harbiy kompyuter xavfsizligi siyosatlarini taqqoslash. 9. Xitoy devori xavfsizligi siyosati. 10. Xitoy devori xavfsizligi siyosatini amalga oshirishda panjara strukturasi. 11. Operatsion tizimlarda himoyani tashkil etish. 12. Himoya mexanizmlari modellari va ularning imkoniyatlari 13. Rolli foydalanishni boshqarish. 14. Rolli foydalanishni boshqarish bo'yicha ANSI standartining tadqiqi. 15. O'zaro chegaralangan rollar va vazifalarni ajratish. 16. Setuid (Set User ID) haqida tushuncha. 17. Jail'lar: qudratli rootni hammaga cheklash. 18. Capability myths`lari va ularning yengilishi. 19. Mantiq, Dasturlash va Prolog. 20. Markazlashtirilmagan ishonchni boshqarish. 21. SPKI/SDSI tizimlarida sertifikat zanjirini aniqlash. 22. Ishonch boshqaruvida tarqatilgan credential zanjirini aniqlash. Izoh: Ushbu mavzular **qo'shimcha adabiyotlar** asosida shakllantirilgan Talabalar ushbu manbalarni tarjima qilgan holda o'rganib, mustaqil ishi bo'yicha referat va taqdimot tayyorlaydilar.
3.	**V. Fan o'qitilishining natijalari (shakllanadigan kompetentsiyalar)** *Fanni o'zlashtirish natijasida talaba:* • talaba foydalanishni boshqarish (access control) nazariyasi va asosiy usullarini tizimli tarzda tushunadi hamda ularning qo'llanilish sohalarini tahlil qila oladi;

	• mavjud foydalanishni boshqarish modellarining (masalan, DAC, MAC, RBAC) afzalliklari va cheklovlarini baholay oladi va ularni real tizimlarda qo'llash samaradorligini tushuntira oladi; • ilmiy maqolalarni o'rganish, tanqidiy fikrlash va tadqiqot savollarini aniqlash orqali mustaqil ilmiy tahlil yurita oladi; • tizimlardagi foydalanishni boshqarish funksiyalarini o'rganib, ularni mavjud modellar bilan taqqoslash va baholash qobiliyatiga ega bo'ladi; • ilmiy tadqiqotlar doirasida materiallarni izlab topish, tahlil qilish, natijalarni tuzish va og'zaki yoki yozma tarzda taqdim etish ko'nikmalarini rivojlantiradi.
4.	**VI. Ta'lim texnologiyalari va metodlari** • ma'ruzalar; • amaliy ishlarni bajarish va xulosalash; • interfaol keys-studylar; • blits-so'rovi; • guruhlarda ishlash; • taqdimotlar tayyorlash; • jamoa bo'lib ishlash va himoya qilish uchun loyihalar.
5.	**VII. Kreditlarni olish uchun talabalar:** Fanga oid nazariy va uslubiy tushunchalarni to'la o'zlashtirish, tahlil natijalarini to'g'ri aks ettira olish, o'rganilayotgan jarayonlar haqida mustaqil mushohada yuritish va nazorat uchun berilgan vazifa va topshiriqlarni bajarish, oraliq va yakuniy nazorat bo'yicha yozma ishni yoki test topshirish.
6.	**Asosiy adabiyotlar** 1. M.Gasser, Building A Secure Computer System. Van Nostrand Reinhold Co., 1988. 2. R.Anderson, Security engineering: a guide to building dependable distributed systems. Second Edition, Wiley, 2008. 3 D.Gollmann, Computer Security. Third Edition. Wiley, 2011. **Qo'shimcha adabiyotlar** 4. Zhao G., Chadwick D. W. On the modeling of bell-lapadula security policies using RBAC //2008 IEEE 17th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. – IEEE, 2008. – C. 257-262. 5. Xue M., Hu A., He C. Application-Oriented Confidentiality and Integrity Dynamic Union Security Model Based on MLS Policy //IEICE TRANSACTIONS on Information and Systems. – 2012. – T. 95. – №. 6. – C. 1694-1697. 6. McLean J. Reasoning about security models //1987 IEEE Symposium on Security and Privacy. – IEEE, 1987. – C. 123-123. 7. Bell D. E. Concerning modeling of computer security //S&P. – 1988. – C. 8-13. 8. Goguen J. A., Meseguer J. Security policies and security models //1982 IEEE Symposium on Security and Privacy. – IEEE, 1982. – C. 11-11. 9. Denning D. E. A lattice model of secure information flow //Communications of the ACM. – 1976. – T. 19. – №. 5. – C. 236-243. 10. Lampson B. W. A note on the confinement problem //Communications of the ACM. – 1973. – T. 16. – №. 10. – C. 613-615. 11. Lipner S. B. A comment on the confinement problem //ACM SIGOPS Operating Systems Review. – 1975. – T. 9. – №. 5. – C. 192-196. 12. Clark D. D., Wilson D. R. A comparison of commercial and military computer security policies //1987 IEEE Symposium on Security and Privacy. – IEEE, 1987. – C. 184-184. 13. Brewer D. F. C., Nash M. J. The Chinese Wall Security Policy //S&P. – 1989. – C. 206-214.

14. Sandhu R. S. Lattice-based enforcement of chinese walls //Computers & Security. – 1992. – T. 11. – №. 8. – C. 753-763.
15. Harrison M. A., Ruzzo W. L., Ullman J. D. Protection in operating systems //Communications of the ACM. – 1976. – T. 19. – №. 8. – C. 461-471.
16. Jones A. Protection mechanism models: their usefulness //Foundations of secure Computation. – 1978. – C. 237-252.
17. Sandhu R. S. Role-based access control //Advances in computers. – Elsevier, 1998. – T. 46. – C. 237-286.
18. ANSI Standard on Role-Based Access Control// https://www.cs.purdue.edu/homes/ninghui/readings/AccessControl/ANSI+INCITS+359-2004.pdf
19. Li N., Byun J. W., Bertino E. A critique of the ANSI standard on role-based access control //IEEE Security & Privacy. – 2007. – T. 5. – №. 6. – C. 41-49.
20. Li N., Tripunitara M. V., Bizri Z. On mutually exclusive roles and separation-of-duty //ACM Transactions on Information and System Security (TISSEC). – 2007. – T. 10. – №. 2. – C. 5-es.
21. Chen H., Wagner D., Dean D. Setuid demystified //11th USENIX Security Symposium (USENIX Security 02). – 2002.
22. Kamp P. H., Watson R. N. M. Jails: Confining the omnipotent root //Proceedings of the 2nd International SANE Conference. – 2000. – T. 43. – C. 116.
23. Miller M. S. et al. Capability myths demolished. – Technical Report SRL2003-02, Johns Hopkins University Systems Research Laboratory, 2003. http://www. erights. org/elib/capability/duals, 2003. – T. 5.
24. U. Nilsson, J. Maluszynski: Logic, Programming and Prolog. John Wiley & Sons Ltd, 2000
25. Blaze M., Feigenbaum J., Lacy J. Decentralized trust management //Proceedings 1996 IEEE symposium on security and privacy. – IEEE, 1996. – C. 164-173.
26. Clarke D. et al. Certificate chain discovery in SPKI/SDSI //Journal of Computer security. – 2001. – T. 9. – №. 4. – C. 285-322.
27. Li N., Winsborough W. H., Mitchell J. C. Distributed credential chain discovery in trust management //Proceedings of the 8th ACM Conference on Computer and Communications Security. – 2001. – C. 156-165.
28. Li N., Mitchell J. C., Winsborough W. H. Design of a role-based trust-management framework //Proceedings 2002 IEEE Symposium on Security and Privacy. – IEEE, 2002. – C. 114-130.

7.	Fanning o'quv dasturi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kengashining 20[illegible]-yil [illegible] bayonnomasi bilan tasdiqlangan.
8.	**Fan/modul uchun mas'ullar:** A.T.Imamaliyev – Muhammad al-Xorazmiy nomidagi TATU, "Kriptologiya" kafedrasi dotsenti v.b. N.F.Axmedova – Muhammad al-Xorazmiy nomidagi TATU, "Kriptologiya" kafedrasi katta o'qituvchisi
9.	**Taqrizchilar:** O.M.Allanov – Muhammad al-Xorazmiy nomidagi TATU, "Kiberxavfsizlik va kriminalistika" kafedrasi mudiri, PhD, dotsent. N.B. Nasrullayev - Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Nurafshon filiali direktori, PhD, dotsent.