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

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

“TASDIQLAYMAN”
O‘quv ishlari bo‘yicha prorektor
Dj.Sultanov
_____
“___” _____ 2023-yil

Ro‘yxatga olindi: № 5
2023-yil “4” 09

FOYDALANISHNI BOSHQARISH

O‘QUV DASTURI

Bilim sohasi: 600 000 - Axborot-kommunikatsiya texnologiyalari

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

Ta’lim yo‘nalishi: 60612100 - Kiberxavfsizlik injiniringi

Toshkent – 2023

Fan/modul kodi	O‘quv yili 2023-2024	Semestr 5	ECTS - kreditlar 6
Fan/modul turi Majburiy	Ta’lim tili O‘zbek/rus		Xaftadagi dars soatlari 5

	Fanning nomi	Auditoriya mashg’ulotlari (soat)	Mustaqil ta’lim (soat)	Jami yuklama (soat)
1.	**Foydalanishni boshqarish**	**74**	**106**	**180**

2. I. Fanning mazmuni

Fanni o‘qitishdan maqsad – talabalarga xavfsizlikning asosiy tushunchalari, foydalanishlarni nazoratlash, tashkilot axborot xavfsizligi siyosati, parolga asoslangan autentifikasiya, tokenga asoslangan autentifikasiya, biometrik autentifikasiya usullari, identifikasiya qilish qurilmalari, shaxsni identifikasiya qilishning biometrik vositalari, biometrik nazoratni amalga oshirishning statik metodlari, shaxsni identifikasiya qilishning biometrik vositalari, biometrik nazoratni amalga oshirishning dinamik metodlari, foydalanishlarni boshqarishni nazoratlash tizim kontrollerlari, identifikatorlarni boshqarish modellari, ishonch paradigmalarining elementlari, mandatli, diskresion, rolli, atributli foydalanishlarni boshqarish modellari, fizik himoyalashda foydalanishlarni boshqarishning bajaruvchi vositalari, Windows operasion tizimida foydalanishlarni boshqarish, Linux operasion tizimida foydalanishlarni boshqarish, Mobil telefon operasion tizimlarida foydalanishlarni boshqarish, foydalanishlarni boshqarishni nazoratlash tizimlarini amalga oshirish variantlari va tahlili, foydalanishlarni boshqarishni nazoratlash tizimlarini tanlash kabilarni o‘rgatish va ularni amaliyotga tatbiq etish ko‘nikmasini hosil silishdan iborat.

Fanning vazifasi – talabalarning nazariy bilimlari, amaliy ko‘nikmalarini shakillantirishda foydalanishlarni nazoratlash, parolga, tokenga, biometrik parametrlarga asoslangan autentifikatsiya usullari, mandatli, diskresion, rolli, atributli foydalanishlarni boshqarish modellari, operasion tizimlarda foydalanishlarni boshqarish, fizik himoyalashda foydalanishlarni boshqarishning bajaruvchi vositalari, foydalanishlarni boshqarishni nazoratlash tizimlarini amalga oshirish variantlari va tahlilini o‘rgatish, shuningdek amaliy faoliyatda olgan bilim va ko‘nikmalarini kasbiy faoliyatida qo‘llay olishiga erishish.

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

II.I. Fan tarkibiga quyidagi mavzular kiradi:

1-mavzu. Xavfsizlikning asosi va foydalanishlarni nazoratlash.

Konfidensiallik. Yaxlitlik. Foydalanuvchanlik. Rad etishni oldini olish. Identifikatsiya. Autentifikatsiya. Avtorizatsiya. Foydalanishni nazoratlash. Autentifikatsiya usullari. Taqqoslash omillari. Bir tomonlama va ikki tomonlama autentifikatsiya. Ko‘p faktorli autentifikatsiya.

2-mavzu. Tashkilot axborot xavfsizligi siyosati.

Axborot xavfsizligi siyosati. Axborot xavfsizligi siyosatining ahamiyati. Axborot xavfsizligi siyosati tarkibi. Unga qo‘yiladigan talablar.

3-mavzu. Parolga asoslangan autentifikatsiya usuli.

Parolga asoslangan autentifikatsiya usuli. Parollarni saqlash va solishtirish. “Salt” yordamida parollarni saqlash. Parollarni boshqarish tizimlari. Parollarni generatsiyalashga qo‘yilgan talablar.

4-mavzu. Tokenga asoslangan autentifikatsiya usullari.

Tokenga asoslangan autentifikatsiya usullarining umumiy sxemasi. Dasturiy va apparat tokenlar. Dasturiy tokenlarga misollar. Apparat tokenlarni yaratish usullari va ularga misollar.

5-mavzu. Biometrik autentifikatsiya usullari.

Biometrik parametrlar. Xatolik turlari. Turli biometrik parametrlarni taqqoslash omillari. Biometrik autentifikatsiya va identifikatsiya.

6-mavzu. Identifikatorlarni boshqarish modellari.

Lokal identifikatorlar. Tarmoq identifikatori. Federatsiya identifikatori. Global veb identifikator. Yagona foydalanishli tizim (Single Sign-On). Global veb identifikatorlar uchun XNS yondashuvi. Markazlashgan tashkilot darajasidagi identifikatorlarni boshqarish.

7-mavzu. Ishonch paradigmalarining elementlari.

Uchinchi tomonga asoslangan autentifikasiyalash paradigmalari. Kerberos protokoli. Ochiq kalitlar infratuzilmasiga asoslangan haqiqiylikni ta’minlash. PKI. X.509 standarti. Umumlashgan vebga asoslangan ishonch modeli. SAML yondashuvi.

8-mavzu. Mandatli foydalanishlarni boshqarish modeli.

Mandatli foydalanishni boshqarish. Bell-Lapadulla modeli. Biba modeli.

9-mavzu. Diskretsion foydalanishlarni boshqarish modeli.

Foydalanishlarni boshqarish matrisasi. ACL. C-list. Foydalanishlarni boshqarish matrisalarining xavfsizlik muammolari.

10-mavzu. Rolli foydalanishlarni boshqarish modeli.

Foydalanuvchi, rol va imtiyoz tushunchalari. Vazifalarni ajratish. Eng kichik imtiyoz. Rollar iyerarxiyasi. Mandatli siyosatni rolli modelga o‘tkazish. Diskresion foydalanishni nazoratlashdan rolli modelga o‘tish.

11-mavzu. Atributli foydalanishlarni boshqarish modeli.

Foydalanishlarni boshqarish mexanizmlarining rivojlanishi. Obyekt atributlari, subyekt atributlari, muhit atributlari tushunchalari. XACML standarti. XACML standarti asosida amalga oshirilgan siyosatga misol.

12-mavzu. Windows operatsion tizimida foydalanishni boshqarish.

NTFS dan foydalanish huquqlari. Vorislik qilish huquqlari (prava na nasledovaniye). Vorislik qilingan huquqlarni bloklash. Fayllar va papkalarni ko‘chirish va nusxa olishda foydalanish huquqlari. Tarmoqdagi fayllar va papkalardan umumiy foydalanish huquqi. Umumiy papkalarni boshqarish. OneDrive. Active Directory. Active Directory xususiyatlari. Active Directory arxitekturasi.

13-mavzu. Linux operatsion tizimida foydalanishni boshqarish.

Linux/UNIX operasion tizimlarida foydalanishlarni boshqarishning umumiy qoidalari. Linuxda obyektlar atributlari. Birinchi va o‘n oltinchi simvollar. Ruxsatlarni o‘zgartirish. Foydalanish huquqlarining raqamli formati. Umask, setuid, setgid, sticky bit, immutable bit. SELinux.

14-mavzu. Mobil telefon operatsion tizimlarida foydalanishni boshqarish.

Mobil qurilmalar konfidensial ma’lumotlari. Apple iOSda autentifikatsiya va foydalanishlarni boshqarish. Apple iOS cheklovlarini olib tashlash hamda autentifikasiyani chetlab o‘tish texnikalari. Google Android-da autentifikatsiya va foydalanishlarni boshqarish. Cheklovlarni olib tashlash texnikalari.

15-mavzu. Fizik himoyalashda identifikatsiyalash qurilmalari.

Kod terish qurilmalari. Kontaktsiz o‘qib oluvchi qurilmalar. HID Corporation kontaktsiz o‘qib olish qurilmaliri. iCLASS kontaktsiz o‘qib olish qurilmaliri. ProxPro klaviaturali proksimiti-o‘qib olish qurilmalar. Avtomobilga o‘rnatish uchun ProxPass faol proksimiti-identifikatorlari. Viganda identifikatsion kartalar o‘qib olish qurilmalari. Yashirin shtrix kodli o‘qib olish qurilmalari.

16-mavzu. Shaxsni identifikatsiyalashning biometrik vositalari.

Biometrik nazoratni amalga oshirishning statik metodlari. Shaxsni identifikatsiyalashning biometrik vositalarining klassifikatsiyasi. Biometrik nazoratni amalga oshirishning statik metodlari. Pappilyar chiziqlar namunasi bo‘yicha identifikasiya. Ko‘zning kamalaksimon qobig’i bo‘yicha identifikasiya. Ko‘z to‘rpardasi kappilyarlari bo‘yicha identifikasiya. Yuz geometriyasi va termik tasviri bo‘yicha identifikasiya. Qo‘l kafti geometriyasi bo‘yicha identifikasiya. Biometrik nazoratni amalga oshirishning dinamik metodlari. Husnixat va imzo dinamikasi bo‘yicha identifikatsiya. Ovoz va nutq xususiyatlari

bo‘yicha identifikatsiya. Klaviaturada ishlash ritmi bo‘yicha identifikasiya. Kelajak biometrik texnologiyalari.

17-mavzu. Foydalanishni boshqarishning nazoratlash tizimi kontrollerlari.

Avtonom kontrollerlar. Tarmoq kontrollerlari. Taqsimlangan foydalanishlarni boshqarishni nazoratlash tizimlari. iSecure Pro foydalanishlarni boshqarishni nazoratlash tizimi kontrollerlari.

18-mavzu. Fizik himoyalashda foydalanishni boshqarishning bajaruvchi vositalari.

Elektrik qulflar. Turniketlar. Shlyuzli kabinalar. TEDRIA yarim avtomat tambur-shlyuzlari. SIRIO avtomatik tambur shlyuzlari. Darvoza va shlagbaumlar. Foydalanishlarni boshqarishning bajaruvchi vositalariga misollar.

19-mavzu. Foydalanishni boshqarishda nazoratlash tizimlarining tahlili va ularni amalga oshirish

Foydalanishlarni boshqarishni nazoratlash avtonom va tarmoq tizimlari. “Flex” tizimlari oilasi. “CONCEPT” integrasion xavfsizlik tizimi. “OnGuard Access” integratsion xavfsizlik tizimi.

20-mavzu. Foydalanishni boshqarishda nazoratlash tizimlarini tanlash.

Foydalanishlarni boshqarishni nazoratlash tizimlarini tanlash bo‘yicha umumiy savollar, ularni tanlash bo‘yicha maslahatlar. Texnik ko‘rsatkichlar, iqtisodiy ko‘rsatkichlar bo‘yicha foydalanishlarni boshqarishni nazoratlash tizimlarini tanlash. Biometrik foydalanishlarni boshqarishni nazoratlash tizimlarini tanlash.

III. Amaliy mashg’ulotlar bo‘yicha ko‘rsatma va tavsiyalar

Amaliy mashg’ulotlar uchun quyidagi mavzular tavsiya etiladi:

1. Tashkilot uchun axborot xavfsizligi siyosatining foydalanishlarni boshqarish bandini ishlab chiqish.
2. Windows OT qayd yozuvlarini sozlash va parol bardoshliligini tekshirish.
3. RFID tizimi orqali identifikatsiya/ autentifikatsiyani amalga oshirish.
4. Barmoq izi orqali identifikatsiya/autentifikatsiya tizimini amalga oshirish.
5. Yuz shakli orqali identifikatsiya/autentifikatsiya tizimini amalga oshirish.
6. Ovoz orqali identifikatsiya/autentifikatsiya tizimini amalga oshirish.
7. SSO protokollarini ishlash jarayoni bilan tanishib chiqish va tahlillash.
8. Operatsion tizimlarda foydalanuvchilar va guruhlar uchun foydalanish huquqlarini sozlash.

IV. Mustaqil ta’lim va mustaqil ishlar

Mustaqil ta’lim uchun tavsiya etiladigan tapshiriqlar:

1. Simmetrik kalitli kriptoalgoritmlarga asoslangan autentifikatsiya protokollari.
2. Ochiq kalitli kriptoalgoritmlarga asoslangan autentifikatsiya protokollari.
3. Bir martali parolga asoslangan autentifikatsiyalash usullari.
4. PIN-kodga asoslangan autentifikatsiya usullarini ahamiyati.
5. Internet xizmatlarda ikki faktorli autentifikatsiyadan foydalanish usullari.
6. Kerberos protokoli va uning xavfsizlik tahlili.
7. Biometrik autentifikatsiya usullarining tahlili.
8. Autentifikatsiya masalasini yechishda QR-kod texnologiyasining o‘rni.
9. Grafik parol asosida autentifikatsiya usullarining tahlili.
10. Ko‘p faktorli autentifikatsiyalash usuli va uning ahamiyati.
11. DNK asosida autentifikatsiyalash usulining tahlili.
12. Odamning yurish tarzi orqali autentifikatsiyalash usulining tahlili.
13. Mavjud autentifikatsiya vositalarining tahlili.
14. Windows OT-da foydalanuvchi qayd yozuvini sozlash tartibi.
15. Linux OT-da foydalanuvchi qayd yozuvini sozlash tartibi.
16. Windows OT-da foydalanuvchi parolini buzish.
17. PDF fayllariga qo‘yilgan sodda parollarni buzish.
18. RAR fayllariga qo‘yilgan sodda parollarni buzish.
19. Google Authenticator tokeni yordamida turli tizimlar uchun ikkinchi faktorni sozlash.
20. Microsoft Authenticator tokeni yordamida turli tizimlar uchun ikkinchi faktorni sozlash.

3. V. Fan o‘qitilishining natijalari (shakllanadigan kompetentsiyalar)

Fanni o‘zlashtirish natijasida talaba:

- foydalanishlarni boshqarishning asosiy tushunchalarini aytib berish;
- foydalanishlarni boshqarishning dolzarbligini asoslab berish;
- foydalanishlarni boshqarishning formal modellari tahlilini amalga amalga oshirish;
- identifikatsiya/autentifikatsiya usullarini tushuntira olish va undan foydalanish;
- foydalanishlarni boshqarish vositalari ishlash prinsiplarini bilish va qo‘llay olish.

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, yakuniy nazorat bo‘yicha yozma ishni yoki test topshirish.

6. Asosiy adabiyotlar

1. S.K.Ganiyev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –T.: «Fan va texnologiya», 2016, 372 bet.
2. S.K.Ganiyev, A.A.Ganiev, D.Y.Irgasheva, Ma'lumotlar bazasi xavfsizligi: darslik, - T. : Fan va Texnologiya, 2016. - 228 b. - 75 экз. - ISBN 978-9943-11-367-1
3. S.K.Ganiyev, A. A.Ganiyev, Z.T.Xudoyqulov; Kiberxavsizlik asoslari: o'quv qo'llanma, -T.: “Nihol print” OK, 2021. – 224 b.

Qo‘shimcha adabiyotlar

1. В.В.Волхонский. Системы контроля и управления доступом. Учебное пособие. Университет ИТМО. Санкт-Петербург. 2015.
2. Information Security. Mark Stamp. John Wiley & Sons. 2011.
3. В.А.Ворона, В.А.Тихонов. Системы контроля и управления доступом. Москва Горячая линия – Телеком. ISBN 978-5-9912-0059-2.
4. Messaoud Benantar. Access Control Systems Security, Identity Management. Springer, ISBN-10: 0-387-00445-9.

7. Fan dasturi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kengashining 2023-yil 30-avgustdagi 9(731)/1(732)-son bayonnomasi bilan tasdiqlangan.

8. Fan/modul uchun mas'ullar:

A.T.Imamaliyev – Muhammad al-Xorazmiy nomidagi TATU, “Kriptologiya” kafedrasi katta o‘qituvchisi

N.F.Axmedova – Muhammad al-Xorazmiy nomidagi TATU, “Kriptologiya” kafedrasi assistenti

9. Taqrizchilar:

O.M.Allanov – Muhammad al-Xorazmiy nomidagi TATU, “Kiberxavfsizlik va kriminalistika” kafedrasi mudiri, PhD.

N.B. Nasrullayev - Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Nurafshon filiali direktori, PhD, dotsent.