ANDIJON DAVLAT PEDAGOGIKA INSTITUTI

Ma’ruza materiallari · 2026–2027 o‘quv yili

FAN

Axborot tizimlari va Raqamli Texnologiyalar

15-ma’ruza · Ma’lumotlar xavfsizligi

2 soat

Ma’ruzachi: **Ismailov Alisher**

E-pochta: alisherismailov1991@gmail.com

Aloqa: **99-499-73-64**

15-MA’RUZA · 2 SOAT

KOMPYUTER ASOSLARI · 9-MAVZU

Ma’lumotlar xavfsizligi

Ma’lumotni himoyalash: tahdidlar, shifrlash, parollar, zaxira nusxalar va qulflar

CIA · AES · 2FA · 3-2-1



Telefoningiz avtobusda yo‘qoldi. Endi nima bo‘ladi?

Begona odam telefoningizda nimalarni ko‘rishi mumkin — va siz nimani butunlay yo‘qotasiz?

O‘ylang · Juftlik · Bo‘lishing (3 daq)

1 Telefoningizdagi qaysi ma’lumot eng shaxsiy?

2 Hozir uni nima himoya qilyapti?

3 Birinchi o‘n daqiqada nima qilgan bo‘lardingiz?

Hozircha noto‘g‘ri javob yo‘q. Dars oxirida bunga qaytamiz.

Dars oxirida siz quyidagilarni bajara olasiz…

1. **Tushuntirish —** ma’lumotlar xavfsizligi nima ekanini maxfiylik, yaxlitlik va mavjudlik orqali.
2. **Aniqlash —** ma’lumotga tahdidlarni: zararli dasturlar, fishing, xakerlik, inson xatosi va ofatlar.
3. **Tasvirlash —** shifrlash ma’lumotni qanday himoya qilishini, simmetrik va ochiq kalitli misollar bilan.
4. **Yaratish —** kuchli parollar va ikki bosqichli autentifikatsiya hamda parol menejerlaridan foydalanish.
5. **Rejalashtirish —** 3-2-1 qoidasi bo‘yicha zaxira nusxalar va ma’lumotni tiklash qadamlarini.
6. **Qo‘llash —** qurilmalar, xonalar va eski saqlash vositalariga jismoniy xavfsizlik choralarini.

CIA uchligi: ma’lumotlar xavfsizligining uch maqsadi

Ma’lumotlar xavfsizligi = raqamli axborotni butun hayoti davomida ruxsatsiz kirish, o‘zgartirish yoki yo‘qolishdan himoya qilish.

Maxfiylik

Ma’lumotni faqat ruxsat berilganlar ko‘radi. Misol: baholaringizni faqat siz va o‘qituvchingiz ko‘radi.

Yaxlitlik

Ma’lumot to‘g‘ri va to‘liq qoladi; uni hech kim ruxsatsiz o‘zgartirmaydi. Misol: bahoni yashirincha o‘zgartirib bo‘lmaydi.

Mavjudlik

Ma’lumot kerak bo‘lganda mavjud. Misol: elektron jurnal imtihon kuni ishlaydi.

Eslab qoling: har bir xavfsizlik chorasi C, I yoki A dan kamida bittasini himoya qiladi.

Biz nimani himoya qilyapmiz?

Shaxsiy ma’lumotlar

Ism, pasport raqami, manzil, telefon raqami, rasmlar.

Moliyaviy ma’lumotlar

Bank karta raqamlari, to‘lov ilovalari, maosh ma’lumotlari.

Tibbiy yozuvlar

Tashxislar, tahlil natijalari, retseptlar.

O‘qish va ish yozuvlari

Baholar, imtihon ishlari, hisobotlar, shartnomalar.

G‘oyalar va ijodiy ishlar

Loyihalar, dizaynlar, dastur kodi, tadqiqotlar.

Kirish ma’lumotlari

Login, parol va bir martalik kodlar — qolgan hamma narsaning kalitlari.

Ma’lumotlar xavfsizligiga tahdidlar

Zararli dasturlar

Ma’lumotni buzadigan yoki o‘g‘irlaydigan virus, qurt, troyan va josus dasturlar.

To‘lov talab qiluvchi dastur

Fayllaringizni qulflab, ochish uchun pul talab qiladi.

Fishing

Parol yoki pulni aldab olishga qaratilgan soxta xabarlar.

Xakerlik

Tizimlarga ruxsatsiz buzib kirish.

Zaif parollar

Oson topiladigan, qayta ishlatilgan yoki sizib chiqqan parollar.

Inson xatosi

Fayllarni o‘chirib yuborish, ma’lumotni noto‘g‘ri odamga yuborish.

Ofatlar va nosozliklar

Yong‘in, suv toshqini, elektr uzilishi va buzilgan qattiq disklar.

O‘g‘irlik va yo‘qotish

O‘g‘irlangan yoki yo‘qolgan telefon, noutbuk va fleshkalar.

Zararli dasturlar: olti turi

TURI	Qanday ishlaydi	Ogohlantiruvchi belgi
Virus	Faylga yopishadi; fayl ochilganda tarqaladi	Fayllar o‘zgaradi yoki ochilmaydi
Qurt (worm)	Tarmoq orqali o‘zini o‘zi ko‘paytiradi	Tarmoq birdan sekinlashadi
Troyan oti	Foydali dastur bo‘lib ko‘rinadi	Noma’lum saytdan “bepul” ilova
Josus dastur	Sizni yashirincha kuzatib, ma’lumot o‘g‘irlaydi	Hisoblaringizdan sizsiz foydalanilgan
To‘lov talab qiluvchi	Fayllaringizni shifrlab, to‘lov talab qiladi	Pul so‘ragan xabar
Reklama dasturi	Ekranni keraksiz reklamalar bilan to‘ldiradi	Hamma joyda qalqib chiquvchi oynalar

Himoya: antivirus, yangilanishlar va ilovalarni faqat rasmiy do‘konlardan o‘rnatish.

TUSHUNISHNI TEKSHIRISH

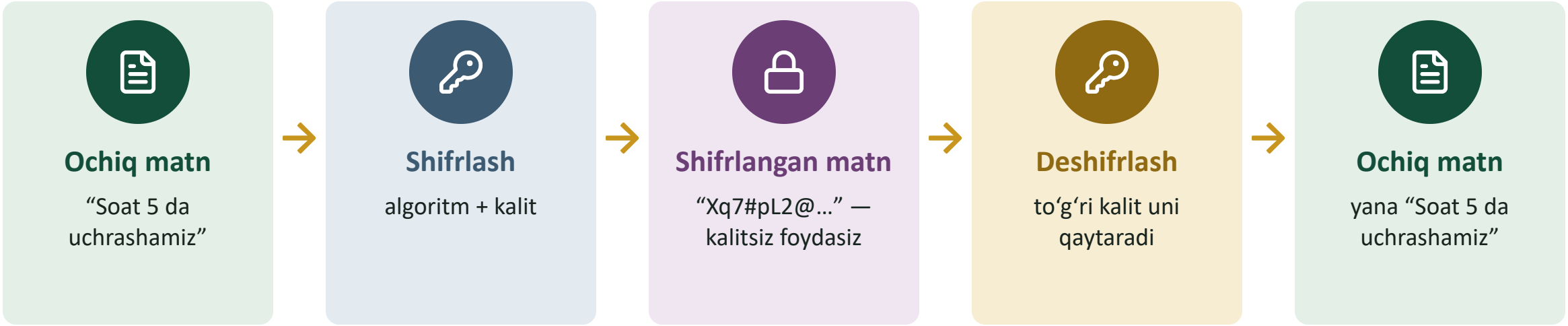
Tahdidni nomlang

A	Noma’lum saytdagi bepul o‘yin kontaktlaringizni yashirincha begona odamga yuboradi.
B	Maktab kompyuteridagi barcha fayllar qulflangan va “Ochish uchun to‘lang” degan xabar chiqqan.
C	O‘quvchi sinf loyihasining yagona nusxasini adashib o‘chirib yuboradi.
D	SMS sizdan g‘alati saytda “kartangizni tasdiqlash”ni so‘raydi.
E	Kafe stolida qoldirilgan noutbuk g‘oyib bo‘ladi.
F	Dastur kompyuter xonasidagi barcha kompyuterlarga o‘zi tarqaladi.

Tanlang

- Troyan / josus dastur
- To‘lov talab qiluvchi dastur
- Inson xatosi
- Fishing
- O‘g‘irlik va yo‘qotish
- Qurt (worm)

Shifrlash: ma’lumotni kalit bilan chalkashtirish



Simmetrik shifrlash

Bitta umumiy maxfiy kalit qulflaydi va ochadi.

Tez; fayl va disklar uchun. Misol: AES.

Ochiq kalitli shifrlash

Ochiq kalit qulflaydi; faqat yopiq kalit ochadi.

HTTPS va xavfsiz e-mail uchun. Misol: RSA.

Sinab ko‘ring: Sezar shifri

Qanday ishlaydi

har bir harfni 3 o‘ringa suring

- A → D B → E C → F … X → A
- DATA → GDWD
- Kalit — 3 soni.
- Yuliy Sezar undan taxminan 2 000 yil oldin foydalangan.

Topshiriq

deshifrlash uchun 3 o‘ringa orqaga suring

- Deshifrlang: VHFXUH
- Deshifrlang: KHOOR
- Ismingizni shifrlang.
- Nega bu shifrni buzish oson?

Bugun: AES kabi haqiqiy shifrlar shunchalik uzun kalitlardan foydalanadiki, ularni topishga milliardlab yillar kerak bo‘ladi.

Atrofingizdagi shifrlash

HTTPS saytlar

Manzil satridagi qulf belgisi: siz va sayt orasidagi ma’lumot shifrlangan.

Xavfsiz xabarlar

Uchdan-uchga shifrlash: faqat jo‘natuvchi va qabul qiluvchi o‘qiydi.

Qurilma shifrlash

Telefon va noutbuklar (m-n, BitLocker) butun diskni shifrlaydi.

Wi-Fi xavfsizligi

WPA2 / WPA3 tarmog‘ingiz radiosignalini shifrlaydi.

Asosiy g‘oya: shifrlangan diskli o‘g‘irlangan noutbuk o‘g‘riga mashinani beradi — ma’lumotingizni emas.

TUSHUNISHNI TEKSHIRISH

Shifrlash bo‘yicha tekshiruv

01 Shifrlangan matn nima?

02 Qaysi shifrlash turi bitta umumiy maxfiy kalitdan foydalanadi?

03 3 ga suriladigan Sezar shifri bilan deshifrlang: FRGH

04 Veb-manzil yonidagi qulf belgisi nimani bildiradi?

05 Nega shifrlangan noutbuk o‘g‘irlansa, xavfsizroq?

06 Ochiq kalitmi yoki yopiq kalit — qaysi birini sir saqlash kerak?

Parolni nima kuchli qiladi?

01

Uzun

12 va undan ortiq belgi. 4 ta tasodifiy so‘zdan iborat parol-ibora uzun va eslab qolish oson.

02

Aralash

Katta va kichik harflar, raqamlar va belgilar.

03

Takrorlanmas

Har bir hisob uchun alohida parol.

04

Kutilmagan

Ism, tug‘ilgan kun, 123456, qwerty yoki “password” emas.

05

Maxfiy

Hech kimga aytilmaydi, monitorga yopishtirilmaydi.

06

Sizib chiqsa, o‘zgartiriladi

Sayt ma’lumot sizib chiqqanini xabar qilsa, darhol o‘zgartiring.

Uni topish qancha vaqt oladi?

PAROL	Nega	Taxminiy topish vaqti
123456	U barcha keng tarqalgan parollar ro‘yxatida bor	Bir zumda
aziza2008	Ism va yil — ma’lum qolip	Soniyalar–daqiqalar
Tashkent2024!	Uzunroq, lekin baribir so‘z, yil va belgi	Soatlar–kunlar
blue-river-samarkand-72	Uzun, tasodifiy so‘zlar — qolipsiz	Asrlar

Izoh: tez kompyuter taxmin qilishi uchun taxminiy baholar; haqiqiy vaqt farq qiladi.

Paroldan tashqari: 2FA va parol menejerlari

Ikki bosqichli autentifikatsiya

bu siz ekaningizni ikki xil isboti

- Siz BILADIGAN narsa: parol yoki PIN
- Sizda BOR narsa: telefondagi kod yoki xavfsizlik kaliti
- SIZ o‘zingiz: barmoq izi yoki yuz
- Endi o‘g‘irlangan parolning o‘zi yetmaydi.

Parol menejerlari

barcha parollaringiz uchun bitta kuchli seyf

- Barcha parollarni shifrlab saqlaydi
- Siz uchun uzun tasodifiy parollar yaratadi
- Siz faqat bitta bosh parolni eslab qolasiz
- Misollar: Bitwarden hamda telefon va brauzerlarga o‘rnatilgan menejerlar

Oltin qoida: bir martalik kodni hech kimga aytmang — hatto “bank”ka ham.

TUSHUNISHNI TEKSHIRISH

Kuchlimi yoki zaifmi?

A	Parol: qwerty123
B	Parol: Barsik (mushuk ismi)
C	Parol-ibora: cloud-apricot-river-7
D	E-mail va o‘yinlar uchun bitta paroldan foydalanish
E	E-mailingiz uchun 2FA’ni yoqish
F	Monitorga yopishtirilgan parolli qog‘oz

K yoki Z deb yozing

K = kuchli / xavfsiz odat

Z = zaif / xavfli odat

Bonus: har bir zaifini tuzating.

Zaxira nusxaning uch turi

TURI	Nima nusxalanadi	Tezlik va joy	Tiklash uchun kerak
To‘liq	Har safar hamma narsa	Eng sekin, eng ko‘p joy	Faqat oxirgi to‘liq nusxa
Inkremental	Faqat oxirgi har qanday zaxiradan keyin o‘zgargan narsa	Eng tez, eng kam joy	To‘liq nusxa + undan keyingi barcha inkremental
Differensial	Oxirgi to‘liq zaxiradan keyin o‘zgargan hamma narsa	O‘rtacha	To‘liq nusxa + oxirgi differensial

Zaxira nusxa = ma’lumotning yo‘qolgandan keyin tiklash uchun alohida saqlanadigan qo‘shimcha nusxasi.

3-2-1 zaxira qoidasi

01

3 ta nusxa

Asl nusxa va ikkita zaxira.

02

2 xil vosita

Masalan, noutbuk SSD’si va tashqi disk.

03

1 ta nusxa boshqa joyda

Bulutda yoki boshqa binoda — yong‘in va o‘g‘irlikdan xavfsiz.

Va tekshiring: hech qachon tiklanmagan zaxira — faqat umid. Har oy bitta faylni tiklab ko‘ring.

Ma’lumotni tiklash: uni qaytarib olish



Tezkor najot

Savat (Recycle Bin)

Google Docs va OneDrive’dagi versiyalar tarixi

Xatodan so‘ng darhol “Bekor qilish” (Undo)

Zaxira bo‘lmaganda

Fayl tiklash dasturlari o‘chirilgan fayllarni topishi mumkin

Buzilgan disklar uchun mutaxassis laboratoriyasi kerak — sekin va qimmat

TUSHUNISHNI TEKSHIRISH

Zaxira detektivi

01 To‘lov talab qiluvchi dastur barcha fayllaringizni qulfladi. Sizni nima qutqaradi?

02 Har kuni qilish uchun qaysi zaxira turi eng tez?

03 3-2-1 qoidasi nechta nusxani talab qiladi?

04 Noutbuk bilan bitta sumkada saqlanadigan fleshka boshqa joydagi zaxirami?

05 Kecha Google Doc’dagi bir xatboshini o‘chirib yubordingiz. Uni qanday qaytarasiz?

06 Nega fayllarni adashib o‘chirgandan keyin diskdan foydalanishni to‘xtatish kerak?

Jismoniy xavfsizlik: uskunalarni himoya qilish

Qulflar va kirish kartalari

Server xonalari va laboratoriyalar faqat ruxsatli odamlarga ochiladi.

Kameralar va qo‘riqchilar

Videokuzatuv va xodimlar kim kirib-chiqishini kuzatadi.

Ekran qulfi

Ketayotganda ekranni qulflang: Windows tugmasi + L.

Qurilmani yoningizda saqlang

Telefon yoki noutbukni qarovsiz qoldirmang; kabel qulfidan foydalaning.

Elektr va yong‘indan himoya

UPS, kuchlanish himoyachilari, tutun sezgichlari, o‘t o‘chirgichlar.

Xavfsiz yo‘q qilish

Eski disklarni tozalang yoki yo‘q qiling; shaxsiy ma’lumotli qog‘ozlarni maydalang.

Ma’lumotingizni himoya qiladigan o‘n soniyalik odatlar

✓ QILING

- Yangilanishlarni kelishi bilan o‘rnating
- Har safar o‘rningizdan turganda ekranni qulflang
- E-mail va bank uchun 2FA’ni yoqing
- Avtomatik zaxiralang va tekshirib turing

✗ QILMANG

- Kutilmagan xabarlardagi havolalarni bosmang
- Topib olgan yoki sizga berilgan fleshkalarni ulamang
- Noma’lum saytlardan «buzilgan» dasturlarni o‘rnatmang
- Parol yoki bir martalik kodlarni ulashmang

TUSHUNISHNI TEKSHIRISH

Qaysi himoya mos?

A	O‘g‘ri noutbukni o‘g‘irlaydi, lekin undagi birorta faylni o‘qiy olmaydi.
B	Sizib chiqqan parolning o‘zi e-mailingizni ochishga yetmaydi.
C	Qattiq disk buzilgandan keyin maktab barcha baholarni tushlikkacha tiklaydi.
D	Server xonasiga faqat kirish kartasi bor xodimlar kira oladi.
E	Elektr uzildi, lekin server xavfsiz o‘chdi.
F	Eski qattiq disk sotilishidan oldin maxsus dastur bilan tozalanadi.

Tanlang

- Shifrlash
- Ikki bosqichli autentifikatsiya
- Zaxira va tiklash
- Kirishni nazorat qilish
- UPS
- Xavfsiz yo‘q qilish

Atrofingizdagi ma’lumotlar xavfsizligi

BANK

Click yoki Payme orqali to‘lash

→ SMS kodlar (2FA) + shifrlash

DAVLAT

OneID bilan my.gov.uz’ga kirish

→ Shaxsni tekshirish + kirishni nazorat qilish

MAKTAB

Elektron jurnal barcha baholarni saqlaydi

→ Parollar + kundalik zaxira

SHIFOXONA

Tarmoqdagi bemor yozuvlari

→ Kirish huquqlari + shifrlash

BIZNES

To‘lov talab qiluvchi dasturga uchragan kompaniya

→ Oflayn zaxiralar vaziyatni qutqaradi

SIZ

Telefoningiz

→ Ekran qulfi + shifrlash + bulutli zaxira

Takrorlash: bularga javob bera olasizmi?

01 C, I va A harflari nimani anglatadi?

02 Ma’lumotlar xavfsizligiga to‘rtta tahdidni ayting.

03 Qurt virusdan nimasi bilan farq qiladi?

04 Ochiq matn, shifrlangan matn va kalit nima?

05 Kuchli parolning uchta qoidasini ayting.

06 2FA hisobni qanday himoya qiladi?

07 3-2-1 zaxira qoidasini tushuntiring.

08 Uchta jismoniy xavfsizlik chorasini ayting.

Chiqish chiptasi

Chiqishdan oldin qog‘oz varaqqa javob yozing.

1. Ma’lumotingizga ikkita tahdidni ayting — biri odamlar sababli, biri baxtsiz hodisa yoki tabiat sababli.

2. Zaif “samarkand” parolini kuchli parolga aylantiring va nimani o‘zgartirganingizni tushuntiring.

3. Noutbukingizda bitiruv loyihangiz bor. 3-2-1 qoidasiga mos zaxira rejasini yozing.