

**O‘ZBEKISTON RESPUBLIKASI
MAKTABGACHA VA MAKTAB TA’LIMI VAZIRLIGI
NAMANGAN DAVLAT PEDAGOGIKA INSTITUTI**
“Intellectual fanlar va axborot texnologiyalari” kafedrası

AXBOROT XAVFSIZLIGI

fanidan

O‘QUV-USLUBIY MAJMUA

Kurs: Informatika fanini o‘qitish huquqini berish bo‘yicha
kasbiy va pedagogik qayta tayyorlash

Ta’lim dasturi: 10011013
(*ishlab chiqarishdan ajralgan va ajralmagan holda*)

Umumiy yuklama: 50 soat (ma’ruza – 20, amaliy – 20, laboratoriya – 10)

Namangan – 2026

MUNDARIJA

SO‘Z BOSHI	4
I. FANNING O‘QUV DASTURI.....	6
II. ISHCHI O‘QUV DASTURI	10
III. FANNI O‘QITISHDA FOYDALANILADIGAN INTERFAOL TA’LIM METODLARI	14
IV. NAZARIY MATERIALLAR (MA’RUZA MATNLARI)	17
1-MAVZU. AXBOROT XAVFSIZLIGI ASOSIY TUSHUNCHALARI: KONFIDENSIALLIK, YAXLITLIK, FOYDALANUVCHANLIK (CIA). TAHDID, ZAIFLIK VA XAVF	17
2-MAVZU. AXBOROT XAVFSIZLIGINING HUQUQIY ASOSLARI. XAVFSIZLIK SIYOSATI	20
3-MAVZU. AXBOROTGA TAHDIDLAR TASNIFI. ZARARLI DASTURLAR: VIRUSLAR, TROYANLAR, CHUVALCHANGLAR, TO‘LOV TALAB QILUVCHI DASTURLAR.....	24
4-MAVZU. IJTIMOY MUHANDISLIK VA FISHING HUUMLARI, ULARDAN HIMOYALANISH	27
5-MAVZU. IDENTIFIKATSIYA, AUTENTIFIKATSIYA VA AVTORIZATSIYA. PAROL SIYOSATI, IKKI FAKTORLI AUTENTIFIKATSIYA.....	30
6-MAVZU. KRIPTOGRAFIYA ASOSLARI: SIMMETRIK VA ASIMMETRIK SHIFRLASH, XESH-FUNKSIYALAR, ELEKTRON RAQAMLI IMZO.....	33
7-MAVZU. TARMOQ XAVFSIZLIGI: TARMOQLARARO EKRANLAR, VPN, HUJUMLARNI ANIQLASH TIZIMLARI.....	37
8-MAVZU. VEB-XAVFSIZLIK: OWASP TOP-10 ZAIFLIKLARI (SQL INJECTION, XSS) VA HIMOYALANISH USULLARI	41
9-MAVZU. AXBOROT TIZIMLARI XAVFSIZLIGINI BOSHQARISH: XAVFLARNI BAHOLASH, ZAXIRA NUSXALASH, INSIDENTLARGA JAVOB BERISH	44
10-MAVZU. TA’LIM MUASSASASIDA AXBOROT XAVFSIZLIGI VA O‘QUVCHILARNING RAQAMLI XAVFSIZLIGI. KIBERXAVFSIZLIK MADANIYATINI SHAKLLANTIRISH	47
V. AMALIY MASHG‘ULOT MATERIALLARI.....	51
1-AMALIY MASHG‘ULOT. AXBOROT TIZIMI UCHUN TAHDID VA ZAIFLIKLAR MODELINI TUZISH.....	51
2-AMALIY MASHG‘ULOT. KUCHLI PAROLLAR YARATISH, PAROL MENEJERLARI VA IKKI FAKTORLI AUTENTIFIKATSIYANI SOZLASH.....	53
3-AMALIY MASHG‘ULOT. FISHING XATLARINI ANIQLASH VA TAHLIL QILISHGA DOIR KEYSLAR	55
4-AMALIY MASHG‘ULOT. KLASSIK SHIFRLASH USULLARI (SEZAR, VIJINER) BO‘YICHA MASALALAR YECHISH.....	57
5-AMALIY MASHG‘ULOT. ZAMONAVIY SHIFRLASH: AES VA RSA ALGORITMLARINI DASTURIY VOSITALARDA QO‘LLASH	60
6-AMALIY MASHG‘ULOT. XESH-FUNKSIYALAR VA FAYL YAXLITLIGINI TEKSHIRISH	63
7-AMALIY MASHG‘ULOT. ANTIVIRUS VA ZARARLI DASTURLARNI ANIQLASH VOSITALARI BILAN ISHLASH	66

8-AMALIY MASHG‘ULOT. OPERATSION TIZIM XAVFSIZLIK SOZLAMALARI: FOYDALANUVCHI HUQUQLARI, YANGILANISHLAR, TARMOQLARARO EKTRAN.....	68
9-AMALIY MASHG‘ULOT. VEB-ILOVALARDAGI ZAIFLIKARNI O‘QUV MUHITIDA (OWASP JUICE SHOP) TAHLIL QILISH	69
10-AMALIY MASHG‘ULOT. MAKTAB UCHUN AXBOROT XAVFSIZLIGI SIYOSATI LOYIHASINI ISHLAB CHIQISH.....	71
VI. LABORATORIYA MASHG‘ULOTLARI MATERIALLARI.....	73
1-LABORATORIYA ISHI. MA’LUMOTLARNI SHIFRLASH VOSITALARI (VERACRYPT, BITLOCKER) BILAN ISHLASH.....	73
2-LABORATORIYA ISHI. ELEKTRON RAQAMLI IMZO VA SERTIFIKATLAR BILAN ISHLASH	74
3-LABORATORIYA ISHI. WIRESHARK YORDAMIDA SHIFRLANMAGAN VA SHIFRLANGAN TRAFIKNI SOLISHTIRISH.....	76
4-LABORATORIYA ISHI. ZAXIRA NUSXA Olish VA MA’LUMOTLARNI TIKLASH STRATEGIYASINI AMALDA QO‘LLASH	77
5-LABORATORIYA ISHI. YAKUNIY LOYIHA: O‘QUVCHILAR UCHUN “RAQAMLI XAVFSIZLIK” DARS VA TRENING MATERIALLARINI TAYYORLASH VA HIMOYA QILISH	79
VII. MUSTAQIL TA’LIM TOPSHIRIQLARI.....	81
VIII. KEYSLAR BANKI	85
IX. GLOSSARIY	88
X. TEST SAVOLLARI	92
XI. YAKUNIY NAZORAT (YOZMA ISH) MATERIALLARI VA BAHOLASH MEZONLARI	104
XII. ADABIYOTLAR RO‘YXATI.....	111

SO‘Z BOSHI

Mazkur o‘quv-uslubiy majmua Namangan davlat pedagogika institutida tashkil etilgan 10011013 – “Informatika fanini o‘qitish huquqini berish bo‘yicha kasbiy va pedagogik qayta tayyorlash” kursi tinglovchilari uchun “Axborot xavfsizligi” fanining o‘quv dasturi asosida tayyorlangan. Majmua fanning maqsad va vazifalari, ta’lim natijalari (TN1–TN10), ma’ruza, amaliy va laboratoriya mashg‘ulotlari mazmuni hamda mustaqil ta’lim topshiriqlarini to‘liq qamrab oladi.

Fan bo‘yicha jami auditoriya yuklamasi 50 soatni tashkil etadi: ma’ruza mashg‘ulotlari – 20 soat (10 ta mavzu), amaliy mashg‘ulotlar – 20 soat (10 ta mashg‘ulot), laboratoriya mashg‘ulotlari – 10 soat (5 ta mashg‘ulot). Mashg‘ulotlar ketma-ketligi tinglovchini axborot xavfsizligining asosiy tushunchalari va huquqiy asoslaridan boshlab tahdidlar, ijtimoiy muhandislik, autentifikatsiya, kriptografiya, tarmoq va veb-xavfsizlik, xavfsizlikni boshqarish orqali ta’lim muassasasi uchun xavfsizlik siyosatini ishlab chiqish va o‘quvchilarga raqamli xavfsizlikni o‘rgatishgacha olib boradi.

Majmua quyidagi qismlardan iborat:

- fanning o‘quv dasturi;
- ishchi o‘quv dasturi (mavzular va soatlar taqsimoti, nazorat shakllari);
- fanni o‘qitishda foydalaniladigan interfaol ta’lim metodlari;
- nazariy materiallar (M1–M10 ma’ruza matnlari, reja, tayanch iboralar, nazorat savollari);
- amaliy mashg‘ulot materiallari (A1–A10: maqsad, bajarish tartibi, dastur kodlari, variantli topshiriqlar);
- laboratoriya mashg‘ulotlari materiallari (L1–L5: qadamma-qadam yo‘riqnomalar);
- mustaqil ta’lim topshiriqlari (variantlar, kooperativ topshiriqlar, baholash mezonlari);
- keyslar banki;
- glossariy (o‘zbek, ingliz, rus tillarida atamalar va izohlar);
- test savollari va javoblar kaliti;
- yakuniy nazorat (yozma ish) materiallari va baholash mezonlari;
- foydalanilgan adabiyotlar va axborot manbalari.

Axloqiy va huquqiy eslatma: majmuadagi barcha amaliy va laboratoriya ishlari faqat himoya maqsadida, o‘quv muhitida (o‘z kompyuteri, virtual mashina, ataylab zaif qilib yaratilgan o‘quv ilovalari) bajariladi. Boshqa shaxslar yoki tashkilotlarning axborot tizimlariga ruxsatsiz kirish, ularni sinash yoki ma’lumotlarini olish O‘zbekiston Respublikasi qonunchiligiga ko‘ra javobgarlikka sabab bo‘ladi. Tinglovchilar birinchi mashg‘ulotda ushbu qoidalar bilan tanishib, tilxat beradi.

Python dasturlari Python 3.10+ va **cryptography** kutubxonasida tekshirilgan.

Majmuadan informatika o'qituvchilari, qayta tayyorlash kursi tinglovchilari hamda "Matematika va informatika" ta'lim yo'nalishi talabalari foydalanishlari mumkin.

Tuzuvchilar: D. Sodirova – NamDPI "Intellektual fanlar va axborot texnologiyalari" kafedrası o'qituvchisi

N. Xudayberdiyev – NamDPI "Intellektual fanlar va axborot texnologiyalari" kafedrası o'qituvchi-stajyori

Taqrizchilar: Sh. Boltabayev – NamDU "Raqamli ta'lim texnologiyalar" kafedrası dotsenti

Sh. Jurayev – NamDU "Raqamli ta'lim texnologiyalar" kafedrası dotsenti

Mazkur o'quv-uslubiy majmua "Intellektual fanlar va axborot texnologiyalari" kafedrasining 2026-yil "___" _____dagi ___-sonli yig'ilishida muhokama qilingan va Aniq va tabiiy fanlar fakulteti Kengashining 2026-yil "___" _____dagi ___-sonli yig'ilish bayoni bilan ma'qullangan.

I. FANNING O'QUV DASTURI

1. Fan ma'lumotlari

Ko'rsatkich	Qiymat	Ko'rsatkich	Qiymat
Fan/modul kodi	AX	O'quv yili	2026–2027
Fan/modul turi	Umumkasbiy fanlar	Ta'lim tili	O'zbek
O'quv rejadagi tartib raqami	10011013 – 3.05	O'qitish oylari	5–9
Jami auditoriya yuklamasi	50 soat	Ma'ruza / Amaliy / Lab.	20 / 20 / 10

2. Fanning mazmuni

Fanning maqsadi – tinglovchilarga axborot xavfsizligining nazariy asoslari, tahdidlar va himoya usullari, kriptografiya hamda axborot xavfsizligining huquqiy asoslari bo'yicha bilimlarni berish, ta'lim muassasasida axborot xavfsizligini ta'minlash va o'quvchilarda raqamli xavfsizlik madaniyatini shakllantirish ko'nikmalarini rivojlantirishdan iborat.

Fanning vazifalari – axborot xavfsizligining asosiy tushunchalari va huquqiy asoslarini o'rganish; tahdidlar, zararli dasturlar va ijtimoiy muhandislik usullarini tahlil qilish; autentifikatsiya, kriptografiya va tarmoq xavfsizligi vositalarini o'zlashtirish; veb-zaifliklar va ulardan himoyalaniшни o'rgatish; maktab uchun xavfsizlik siyosatini ishlab chiqish ko'nikmalarini shakllantirishdan iborat.

3. Fanni o'zlashtirish uchun zarur boshlang'ich bilimlar

- Informatika va raqamli texnologiyalar;
- Kompyuter ta'minoti;
- Umumta'lim maktablarda huquqiy masalalar.

4. Ta'lim natijalari (TN)

Kod	Ta'lim natijasi
Kasbiy kompetensiyalar	
TN1	axborot xavfsizligining asosiy tushunchalari (konfidensiallik, yaxlitlik, foydalanuvchanlik), tahdid va zaifliklar haqida bilimga ega bo'lishi kerak
TN2	axborot xavfsizligi va shaxsga doir ma'lumotlarni himoya qilishning huquqiy asoslarini bilishi kerak
TN3	zararli dasturlar va ijtimoiy muhandislik hujumlarining turlari va ulardan himoyalaniş usullarini bilishi kerak
TN4	identifikatsiya, autentifikatsiya va avtorizatsiya mexanizmlarini bilishi kerak

Kod	Ta'lim natijasi
TN5	kriptografiya asoslari, shifrlash algoritmlari va elektron raqamli imzoni tushunishi kerak
TN6	tarmoq va veb-ilovalar xavfsizligini ta'minlash usullarini tushunishi kerak
Ko'nikmalar	
TN7	parol siyosati, ikki faktorli autentifikatsiya va operatsion tizim xavfsizlik sozlamalarini qo'llash ko'nikmasiga ega bo'ladi
TN8	shifrlash vositalari va antivirus dasturlaridan foydalanish ko'nikmasiga ega bo'ladi
TN9	fishing va boshqa kiberhujumlarni aniqlash, zaxira nusxalash va ma'lumotlarni tiklash ko'nikmasiga ega bo'ladi
TN10	ta'lim muassasasi uchun axborot xavfsizligi siyosatini ishlab chiqish va o'quvchilarga raqamli xavfsizlikni o'rgatish bo'yicha amaliy tajribaga ega bo'ladi

5. Fan mazmuni va mashg'ulotlar shakli

№	Mavzu va uning mazmuni	Soat
Ma'ruza (M)		20
M1	Axborot xavfsizligi asosiy tushunchalari: konfidensiallik, yaxlitlik, foydalanuvchanlik (CIA). Tahdid, zaiflik va xavf. [1,4]	2
M2	Axborot xavfsizligining huquqiy asoslari: "Kiberxavfsizlik to'g'risida"gi va "Shaxsga doir ma'lumotlar to'g'risida"gi qonunlar. Xavfsizlik siyosati. [5,6,11]	2
M3	Axborotga tahdidlar tasnifi. Zararli dasturlar: viruslar, troyanlar, chuvalchanglar, to'lov talab qiluvchi dasturlar. [1,3]	2
M4	Ijtimoiy muhandislik va fishing hujumlari, ulardan himoyalaniish. [7,9]	2
M5	Identifikatsiya, autentifikatsiya va avtorizatsiya. Parol siyosati, ikki faktorli autentifikatsiya. [1,4]	2
M6	Kriptografiya asoslari: simmetrik va asimmetrik shifrlash, xesh-funksiyalar, elektron raqamli imzo. [2]	2
M7	Tarmoq xavfsizligi: tarmoqlararo ekranlar, VPN, hujumlarni aniqlash tizimlari. [2,3]	2
M8	Veb-xavfsizlik: OWASP Top-10 zaifliklari (SQL injection, XSS) va himoyalaniish usullari. [8,13]	2
M9	Axborot tizimlari xavfsizligini boshqarish: xavflarni baholash, zaxira nusxalash, insidentlarga javob berish. [4,10]	2
M10	Ta'lim muassasasida axborot xavfsizligi va o'quvchilarning raqamli xavfsizligi. Kiberxavfsizlik madaniyatini shakllantirish. [6,9,12]	2
Amaliy mashg'ulot (A)		20
A1	Axborot tizimi uchun tahdid va zaifliklar modelini tuzish. [1,4]	2
A2	Kuchli parollar yaratish, parol menejerlari va ikki faktorli autentifikatsiyani sozlash. [1,9]	2
A3	Fishing xatlarini aniqlash va tahlil qilishga doir keyslar. [7,9]	2
A4	Klassik shifrlash usullari (Sezar, Vijiner) bo'yicha masalalar yechish. [2]	2

№	Mavzu va uning mazmuni	Soat
A5	Zamonaviy shifrlash: AES va RSA algoritmlarini dasturiy vositalarda qo'llash. [2]	2
A6	Xesh-funksiyalar va fayl yaxlitligini tekshirish. [2]	2
A7	Antivirus va zararli dasturlarni aniqlash vositalari bilan ishlash. [1,3]	2
A8	Operatsion tizim xavfsizlik sozlamalari: foydalanuvchi huquqlari, yangilanishlar, tarmoqlararo ekran. [1,10]	2
A9	Veb-ilovalardagi zaifliklarni o'quv muhitida (OWASP Juice Shop) tahlil qilish. [8]	2
A10	Maktab uchun axborot xavfsizligi siyosati loyihasini ishlab chiqish. [4,5,6]	2
Laboratoriya mashg'uloti (L)		10
L1	Ma'lumotlarni shifrlash vositalari (VeraCrypt, BitLocker) bilan ishlash. [2,10]	2
L2	Elektron raqamli imzo va sertifikatlar bilan ishlash. [2,11]	2
L3	Wireshark yordamida shifrlanmagan va shifrlangan trafikni solishtirish. [2,3]	2
L4	Zaxira nusxa olish va ma'lumotlarni tiklash strategiyasini amalda qo'llash. [4,10]	2
L5	Yakuniy loyiha: o'quvchilar uchun "Raqamli xavfsizlik" darsi va trening materiallarini tayyorlash va himoya qilish. [9,12]	2

6. Mustaqil ta'lim topshiriqlari

№	Topshiriq
1	"Kiberxavfsizlik to'g'risida"gi Qonunning asosiy qoidalari bo'yicha tahliliy referat tayyorlash. [5,11]
2	Zararli dasturlarning turlari va ularning tarqalish usullari bo'yicha taqdimot tayyorlash. [1,3]
3	Ijtimoiy muhandislik hujumlariga doir real keyslar to'plamini tayyorlash va tahlil qilish (kichik guruhlarda hamkorlikda). [7,9]
4	Shifrlash algoritmlari bo'yicha qiyosiy jadval tuzish. [2]
5	OWASP Top-10 zaifliklari bo'yicha qisqacha qo'llanma tayyorlash. [8]
6	O'quvchilar va ota-onalar uchun "Internetda xavfsiz yurish" eslatmasini ishlab chiqish (kichik guruhlarda hamkorlikda). [6,9]

Izoh: fan (modul) yuzasidan tinglovchilar bajaradigan mustaqil ish topshiriqlari variativ tavsifga ega; mustaqil ish topshiriqlarining 1/3 qismi (3- va 6-topshiriqlar) kichik guruhlarda hamkorlikda ishlashga (kooperativlik) mo'ljallangan.

7. Ta'lim texnologiyalari va metodlari

– ma'ruzalar;

- amaliy va laboratoriya ishlarini bajarish va xulosalash;
- interfaol keys-stadilar;
- blits-so‘rov;
- guruhlarda ishlash;
- taqdimotlar qilish;
- jamoa bo‘lib ishlash va himoya qilish uchun loyihalar.

8. Kreditlarni olish uchun talablar

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 topshirish.

9. Tinglovchi bilimini baholash mezonlari

Baholash mezonlari ushbu majmuaning XI bo‘limida batafsil keltirilgan (5 – “a’lo”, 4 – “yaxshi”, 3 – “qoniqarli”, 2 – “qoniqarsiz”).

10. Foydalanilgan adabiyotlar

Adabiyotlar ro‘yxati majmuaning XII bo‘limida keltirilgan. Mavzular yonidagi kvadrat qavs ichidagi raqamlar ([1,4]) ushbu ro‘yxatdagi tartib raqamlariga mos keladi.

Tuzuvchilar: D. Sodirova, N. Xudayberdiyev

Kafedra mudiri: A. Matkarimov

II. ISHCHI O'QUV DASTURI

1. Fanning o'quv yuklamasi taqsimoti

Mashg'ulot turi	Soat	Mashg'ulotlar soni	Nazorat shakli
Ma'ruza	20	10	Blits-so'rov, keys tahlili, nazorat savollari
Amaliy mashg'ulot	20	10	Amaliy ish natijasini namoyish etish va himoya qilish
Laboratoriya mashg'uloti	10	5	Laboratoriya hisobotini himoya qilish
Jami auditoriya	50	25	–
Mustaqil ta'lim	–	6 ta topshiriq	Hisobot / mahsulot himoyasi
Yakuniy nazorat	–	–	Yozma ish

2. Ma'ruza mashg'ulotlarining mavzuli rejasi

№	Mavzu nomi va asosiy savollari	Soat	Metod	TN
M1	Axborot xavfsizligi asosiy tushunchalari 1. Axborot va axborot xavfsizligi. 2. Konfidensiallik, yaxlitlik, foydalanuvchanlik (CIA). 3. Tahdid, zaiflik, xavf. 4. Himoya choralari turlari	2	BBB, klaster	TN1
M2	Axborot xavfsizligining huquqiy asoslari. Xavfsizlik siyosati 1. Me'yoriy-huquqiy baza. 2. "Kiberxavfsizlik to'g'risida"gi Qonun. 3. "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun. 4. Xavfsizlik siyosati	2	FSMU, keys-stadi	TN2
M3	Tahdidlar tasnifi. Zararli dasturlar 1. Tahdidlar tasnifi. 2. Virus, chuvalchang, troyan. 3. To'lov talab qiluvchi dasturlar. 4. Zararli dasturlardan himoyalaniish	2	Klaster, "Zigzag"	TN3
M4	Ijtimoiy muhandislik va fishing 1. Ijtimoiy muhandislik psixologiyasi. 2. Fishing turlari. 3. Fishing belgilari. 4. Himoyalaniish choralari	2	Keys-stadi, aqliy hujum	TN3, TN9
M5	Identifikatsiya, autentifikatsiya, avtorizatsiya 1. Asosiy tushunchalar. 2. Autentifikatsiya omillari. 3. Parol siyosati. 4. 2FA/MFA. 5. Kirishni boshqarish modellari	2	Venn diagrammasi, blits-so'rov	TN4, TN7
M6	Kriptografiya asoslari 1. Asosiy tushunchalar. 2. Klassik shifrlar. 3. Simmetrik shifrlash (AES). 4. Asimmetrik shifrlash (RSA). 5. Xesh-funksiyalar. 6. ERI	2	Venn diagrammasi, "Zigzag"	TN5, TN8

№	Mavzu nomi va asosiy savollari	Soat	Metod	TN
M7	Tarmoq xavfsizligi 1. Tarmoq tahdidlari. 2. Tarmoqlararo ekranlar. 3. VPN. 4. IDS/IPS. 5. Simsiz tarmoq xavfsizligi	2	Klaster, namoyish	TN6
M8	Veb-xavfsizlik. OWASP Top-10 1. Veb-ilova arxitekturasi va HTTPS. 2. OWASP Top 10:2025. 3. SQL injection. 4. XSS. 5. Xavfsiz dasturlash tamoyillari	2	Keys-stadi, SWOT	TN6
M9	Axborot tizimlari xavfsizligini boshqarish 1. Xavflarni baholash. 2. Xavfni boshqarish strategiyalari. 3. Zaxira nusxalash (3-2-1). 4. Insidentlarga javob berish	2	Xavf matritsasi, keys-stadi	TN9, TN10
M10	Ta'lim muassasasida axborot xavfsizligi 1. Maktab AT infratuzilmasi xavflari. 2. O'quvchilar ma'lumotlarini himoya qilish. 3. O'quvchilarning raqamli xavfsizligi. 4. Kiberxavfsizlik madaniyati	2	Loyiha, FSMU	TN10
Jami		20		

3. Amaliy mashg'ulotlarning mavzuli rejasi

№	Amaliy mashg'ulot mavzusi va natijasi	Soat	Shakli	TN
A1	Tahdid va zaifliklar modeli. Natija: maktab axborot tizimi uchun aktivlar, tahdidlar va zaifliklar jadvali	2	Kichik guruh	TN1
A2	Kuchli parollar, parol menejeri, 2FA. Natija: parol siyosati qoidalari, sozlangan 2FA	2	Individual	TN7
A3	Fishing xatlarini aniqlash. Natija: 6 ta xat tahlili jadvali va eslatma	2	Juftlikda	TN9
A4	Sezar va Vijiner shifrlari. Natija: yechilgan masalalar va Python dasturi	2	Individual	TN5
A5	AES va RSA dasturiy vositalarda. Natija: shifrlangan fayllar, Python dasturi, hisobot	2	Individual	TN5, TN8
A6	Xesh-funksiyalar va fayl yaxlitligi. Natija: xesh qiymatlar jadvali, tekshiruv dasturi	2	Individual	TN5, TN8
A7	Antivirus va zararli dasturlarni aniqlash vositalari. Natija: tekshiruv hisoboti va EICAR sinovi	2	Individual	TN8
A8	OS xavfsizlik sozlamalari. Natija: sozlamalar nazorat varag'i (checklist)	2	Individual	TN7
A9	OWASP Juice Shop o'quv muhitida veb-zaifliklar tahlili. Natija: zaiflik toifalari va himoya choralari jadvali	2	Juftlikda	TN6
A10	Maktab uchun axborot xavfsizligi siyosati loyihasi. Natija: siyosat hujjati va taqdimot	2	Kichik guruh	TN10
Jami		20		

4. Laboratoriya mashg'ulotlarining mavzuli rejasi

№	Laboratoriya ishi mavzusi va natijasi	Soat	Shakli	TN
L1	VeraCrypt va BitLocker bilan shifrlash. Natija: shifrlangan konteyner va USB disk, hisobot	2	Individual	TN8
L2	Elektron raqamli imzo va sertifikatlar. Natija: imzolangan hujjat, sertifikat tahlili	2	Individual	TN5
L3	Wireshark: HTTP va HTTPS trafikini solishtirish. Natija: trafik tahlili hisoboti	2	Juftlikda	TN6
L4	Zaxira nusxalash va tiklash. Natija: 3-2-1 strategiyasi, tiklash sinovi bayonnomasi	2	Individual	TN9
L5	Yakuniy loyiha: "Raqamli xavfsizlik" darsi va trening materiallari. Natija: dars ishlanmasi, taqdimot, himoya	2	Kichik guruh	TN10
Jami		10		

5. Mustaqil ta'lim topshiriqlarining taqsimoti

№	Topshiriq	Bog'liq mavzu	Shakli	Topshirish muddati
1	"Kiberxavfsizlik to'g'risida"gi Qonun bo'yicha tahliliy referat	M2	Individual	A3 mashg'ulotigacha
2	Zararli dasturlar bo'yicha taqdimot	M3, A7	Individual	A7 mashg'ulotigacha
3	Ijtimoiy muhandislik keyslari to'plami	M4, A3	Kichik guruh (3–4 kishi)	A5 mashg'ulotigacha
4	Shifrlash algoritmlari qiyosiy jadvali	M6, A4–A6	Individual	L2 mashg'ulotigacha
5	OWASP Top-10 bo'yicha qisqacha qo'llanma	M8, A9	Individual	A10 mashg'ulotigacha
6	"Internetda xavfsiz yurish" eslatmasi	M10, L5	Kichik guruh (3–4 kishi)	L5 mashg'ulotida

6. Nazorat turlari va baholash tartibi

Tinglovchilar bilimi joriy va yakuniy nazorat orqali 5 baholik tizimda baholanadi.

Joriy nazorat amaliy va laboratoriya ishlarini himoya qilish, ma'ruzalardagi blits-so'rov va keys tahlili hamda mustaqil ta'lim topshiriqlarini himoya qilish orqali amalga oshiriladi. Joriy baho barcha amaliy, laboratoriya ishlari va mustaqil topshiriqlar baholarining o'rtacha arifmetigi sifatida aniqlanadi.

Yakuniy nazorat yozma ish shaklida o'tkaziladi. Yozma ish varianti 3 ta topshiriqdan iborat: ikkita nazariy savol va bitta amaliy topshiriq (masalan, shifrlash

masalasi, tahdid modeli, fishing xati tahlili yoki xavfsizlik siyosati bandi). Yozma ish uchun 80 daqiqa vaqt ajratiladi.

Yakuniy nazoratga barcha amaliy va laboratoriya ishlarini topshirgan va joriy nazoratdan kamida “3” baho olgan tinglovchilar qo‘yiladi. Fan bo‘yicha umumiy baho joriy nazorat (40%) va yakuniy nazorat (60%) natijalarining o‘lchangan o‘rtachasi sifatida, butun songa yaxlitlangan holda qo‘yiladi.

Nazorat turi	Shakli	Ulushi
Joriy nazorat	Amaliy va laboratoriya ishlari himoyasi, blits-so‘rov, mustaqil ta’lim	40%
Yakuniy nazorat	Yozma ish (3 topshiriq, 80 daqiqa)	60%

7. Fanni o‘qitish uchun zarur moddiy-texnik va dasturiy ta’minot

- kompyuter sinfi (har bir tinglovchiga bitta kompyuter, Windows 10/11 Pro yoki Linux), proyektor, barqaror Internet aloqasi;
- har bir tinglovchiga o‘quv maqsadidagi USB-flesh disk (8 GB va undan katta, ichida muhim ma’lumot bo‘lmagan);
- VirtualBox va o‘quv virtual mashinalari (laboratoriya ishlari asosiy tizimga ta’sir qilmasligi uchun);
- Python 3.10+ va **cryptography** kutubxonasi (**pip install cryptography**);
- KeePassXC yoki Bitwarden parol menejeri; Google Authenticator yoki Microsoft Authenticator ilovasi (tinglovchi smartfonida);
- 7-Zip, VeraCrypt, Wireshark, OpenSSL;
- Microsoft Defender (Windows tarkibida), ClamAV (ixtiyoriy);
- OWASP Juice Shop (Docker konteynerida yoki lokal o‘rnatilgan; faqat **localhost** da ishlatiladi);
- E-IMZO dasturi va o‘quv sertifikatlari (L2 uchun; real kalitlar bilan ishlanmaydi).

Kompyuter sinfi tarmog‘ida Wireshark bilan faqat o‘z kompyuteringiz trafigi tahlil qilinadi. Boshqa foydalanuvchilar trafigini ushlash, tarmoqni skanerlash va institut tizimlarini sinash taqiqlanadi.

III. FANNI O‘QITISHDA FOYDALANILADIGAN INTERFAOL TA’LIM METODLARI

Fanni o‘qitishda an’anaviy metodlar bilan bir qatorda keys-stadi, rolli o‘yin va loyiha metodlariga alohida e’tibor beriladi, chunki axborot xavfsizligi bo‘yicha bilimlar real vaziyatlarda qaror qabul qilish orqali mustahkamlanadi. Har bir metod uchun maqsad, o‘tkazish tartibi va fan bo‘yicha namuna ko‘rsatilgan. Tinglovchilar metodni avval ishtirokchi sifatida his qiladi, so‘ngra maktabda o‘quvchilar bilan qanday qo‘llashni tahlil qiladi.

1. “BBB” (Bilaman – Bilishni xohlayman – Bilib oldim) metodi

Maqsadi: mavzu bo‘yicha oldingi bilimlarni faollashtirish, o‘rganish ehtiyojini aniqlash va o‘rganilganini anglash.

O‘tkazish tartibi: tinglovchilar uch ustunli jadval chizadi. Mavzu boshida 1-ustunga bilganlarini, 2-ustunga bilishni xohlaganlarini yozadi; mavzu oxirida 3-ustunga yangi bilib olganlarini yozadi.

Namuna (M1): “Bilaman: antivirus kerak, parolni hech kimga aytmaslik kerak”; “Bilishni xohlayman: xakerlar parolni qanday biladi? Maktab kompyuterlarini qanday himoya qilish kerak?”; “Bilib oldim: CIA uchligi, tahdid – zaiflik – xavf zanjiri”.

2. “Klaster” metodi

Maqsadi: tushunchalar o‘rtasidagi bog‘lanishlarni grafik shaklda aks ettirish.

Namuna (M3): markazda – “Zararli dasturlar”; tarmoqlar: o‘z-o‘zidan ko‘payuvchilar (virus, chuvalchang), niqoblanganlar (troyan, “orqa eshik”), daromad olishga yo‘naltirilganlar (to‘lov talab qiluvchi, reklama, kriptomayner), josuslik (spyware, keylogger), tarqalish yo‘llari, himoya choralari.

Onlayn variant: Miro, Canva yoki Padlet onlayn doskalari.

3. “Venn diagrammasi” metodi

Maqsadi: ikki yoki uch tushunchani taqqoslash.

Namunalar: “Simmetrik va asimmetrik shifrlash” (M6), “Identifikatsiya, autentifikatsiya va avtorizatsiya” (M5), “Virus va chuvalchang” (M3), “Shifrlash va xeshlash” (M6), “IDS va IPS” (M7).

4. “FSMU” metodi

Maqsadi: muammo bo‘yicha o‘z fikrini asoslash ko‘nikmasini shakllantirish.

FSMU – to‘rt bosqichning bosh harflari: **F** – fikringizni bayon eting; **S** – fikringizga sabab ko‘rsating; **M** – ko‘rsatgan sababingizni isbotlovchi misol keltiring; **U** – fikringizni umumlashtiring.

Namuna savollari: “Maktab o‘quvchilarning telefonlarini kuzatish dasturi bilan nazorat qilishi kerakmi?” (M2, M10); “Parolni har oy majburan almashtirish xavfsizlikni oshiradimi?” (M5).

5. “Keys-stadi” metodi

Maqsadi: real vaziyatlarni tahlil qilish orqali yechim ishlab chiqish.

Bosqichlari:

- keys bilan individual tanishish;
- muammoni aniqlash (qaysi aktiv, qaysi tahdid, qaysi zaiflik);
- kichik guruhlarda yechim ishlab chiqish (darhol choralar va uzoq muddatli choralar);
- yechimlarni taqdim etish va himoya qilish;
- o‘qituvchi tomonidan umumlashtirish.

Fan bo‘yicha keyslar banki majmuaning VIII bo‘limida berilgan.

6. “Aqliy hujum” metodi

Maqsadi: qisqa vaqtda ko‘p g‘oya to‘plash.

Namuna (M4): “O‘quvchilarni fishingdan himoya qilish uchun maktabda qanday tadbirlar o‘tkazish mumkin?” G‘oyalar tanqidsiz yoziladi, keyin guruhlanadi va eng amaliy 5 tasi tanlanadi.

7. “Zigzag” (Jigsaw) metodi

Maqsadi: katta hajmdagi materialni qisqa vaqtda o‘zlashtirish.

Namuna (M6): ekspert guruhlarini mos ravishda klassik shifrlar, AES, RSA, xesh-funksiyalar va ERI ni o‘rganadi; so‘ngra uy guruhlarida bir-biriga tushuntiradi va qiyosiy jadvalni to‘ldiradi (4-mustaqil topshiriqqa asos bo‘ladi).

8. “SWOT-tahlil” metodi

Maqsadi: texnologiya yoki qarorni kuchli (S), zaif (W) tomonlari, imkoniyatlar (O) va xavflar (T) bo‘yicha tahlil qilish.

Namuna (M8, M10): “Maktabda bulutli xizmatlardan (Google Workspace) foydalanish”: S – zaxira nusxa va 2FA provayder tomonidan ta‘minlanadi; W – Internetga bog‘liqlik; O – yagona hisob, hamkorlik; T – noto‘g‘ri ulashish sozlamalari tufayli ma‘lumot sizib chiqishi.

9. “Xavf matritsasi” metodi

Maqsadi: xavflarni ehtimollik va ta’sir bo’yicha baholash va ustuvorlikni aniqlash.

O’tkazish tartibi: guruh aktivlar va tahdidlar ro’yxatini tuzadi; har bir xavf uchun ehtimollik (1–3) va ta’sir (1–3) baholanadi; ko‘paytma bo’yicha xavf matritsaga joylanadi; yuqori xavflar uchun choralar belgilanadi. M9 va A1, A10 da qo‘llaniladi.

10. “Rolli o‘yin: insidentga javob” metodi

Maqsadi: insident yuz berganda harakatlar ketma-ketligini amalda mashq qilish.

O’tkazish tartibi: rollar taqsimlanadi (direktor, informatika o‘qituvchisi – AT mas’uli, o‘qituvchi, ota-ona, o‘quvchi). O‘qituvchi bosqichma-bosqich “xabarlar” beradi (masalan: “Kompyuter sinfidagi 3 ta kompyuterda fayllar shifrlangan, ekranda to‘lov talabi”). Har bir rol o‘z harakatini aytadi; oxirida insidentga javob bosqichlari (aniqlash – cheklash – bartaraf etish – tiklash – xulosa) bo’yicha tahlil qilinadi. M9 da qo‘llaniladi.

11. “Blits-so‘rov” va onlayn viktorina

Maqsadi: tayanch tushunchalarni tez takrorlash.

Onlayn variant: Kahoot yoki Quizizz’da 8–10 ta savol (X bo‘limdagi test savollaridan); natijalar statistikasi keyingi darsda qiyin savollarni tushuntirish uchun ishlatiladi.

12. Loyiha metodi

Maqsadi: egallangan bilim va ko‘nikmalarni yaxlit mahsulotga – maktab uchun xavfsizlik siyosati (A10) va o‘quvchilar uchun “Raqamli xavfsizlik” darsiga (L5) yo‘naltirish.

Bosqichlari: muammo va auditoriyani tahlil qilish → aktivlar va xavflarni aniqlash → yechim (siyosat, dars ishlanmasi) loyihasini tuzish → materiallarni tayyorlash → taqdimot va himoya → tahlil va takomillashtirish.

IV. NAZARIY MATERIALLAR (MA'RUZA MATNLARI)

1-MAVZU. AXBOROT XAVFSIZLIGI ASOSIY TUSHUNCHALARI: KONFIDENSIALLIK, YAXLITLIK, FOYDALANUVCHANLIK (CIA). TAHDID, ZAIFLIK VA XAVF

Reja:

1. Axborot, axborot resurslari va axborot xavfsizligi tushunchalari.
2. Axborot xavfsizligining asosiy xususiyatlari: CIA uchligi.
3. Qo'shimcha xususiyatlar: autentiklik, inkor etib bo'lmalik, hisobdorlik.
4. Aktiv, tahdid, zaiflik, xavf va himoya chorasi.
5. Himoya choralarining turlari va ko'p qatlamli himoya.

Tayanch iboralar:

axborot, axborot resursi, axborot xavfsizligi, kiberxavfsizlik, konfidensiallik, yaxlitlik, foydalanuvchanlik, CIA uchligi, autentiklik, inkor etib bo'lmalik, aktiv, tahdid, zaiflik, xavf, hujum, himoya chorasi, ko'p qatlamli himoya.

1. Axborot, axborot resurslari va axborot xavfsizligi tushunchalari

Axborot – manbalari va taqdim etilish shaklidan qat'i nazar shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to'g'risidagi ma'lumotlar. Zamonaviy jamiyatda axborot moddiy boyliklar bilan teng qiymatga ega bo'lgan resursdir: bank hisobvaraqlari, o'quvchilarning baholari, tibbiy yozuvlar, davlat reyestrlari – barchasi raqamli shaklda saqlanadi.

Axborot resursi – axborot tizimi tarkibidagi elektron shakldagi axborot, ma'lumotlar banki, ma'lumotlar bazasi. Maktab misolida: elektron jurnal, o'quvchilar va ota-onalar ro'yxati, o'qituvchilar shaxsiy yig'majildlari, dars ishlanmalari, nazorat ishlari variantlari.

Axborot xavfsizligi – axborot va uni qo'llab-quvvatlovchi infratuzilmaning tasodifiy yoki qasddan qilingan, egasi yoki foydalanuvchisiga zarar yetkazishi mumkin bo'lgan ta'sirlardan himoyalanganlik holati. Axborot xavfsizligi faqat texnik masala emas: u texnik, dasturiy, tashkiliy va huquqiy choralar hamda insonlarning xatti-harakati majmuidir.

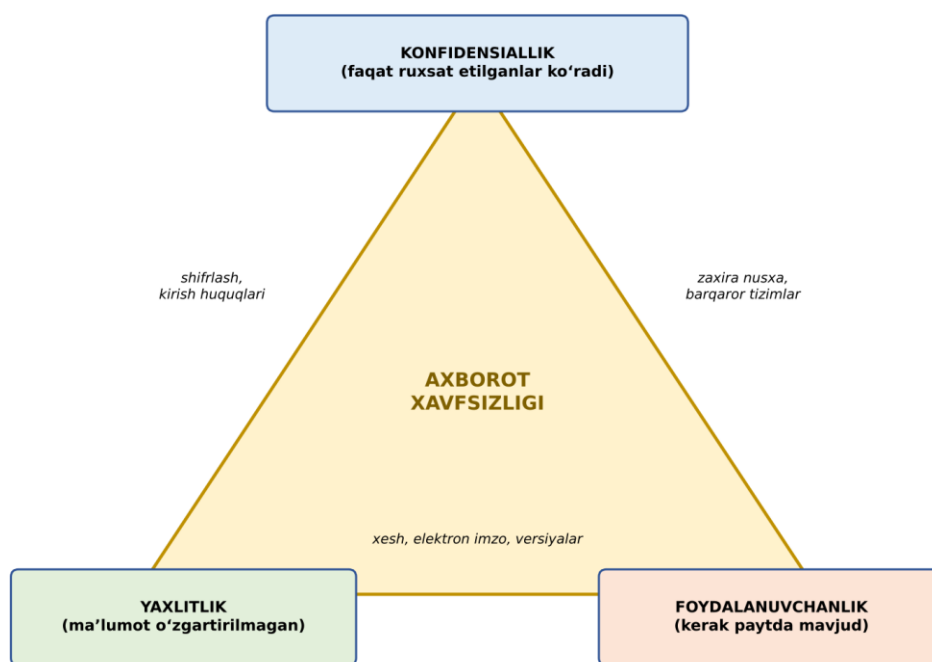
Kiberxavfsizlik – axborot xavfsizligining kibermakon (Internet va unga ulangan tizimlar) bilan bog'liq qismi. "Kiberxavfsizlik to'g'risida"gi Qonunda kiberxavfsizlik shaxs, jamiyat va davlat manfaatlarining kibermakondagi tashqi va ichki tahdidlardan himoyalanganlik holati sifatida belgilangan (2-mavzu).

Jihat	Axborot xavfsizligi	Kiberxavfsizlik
Qamrov	Har qanday shakldagi axborot (qog'oz, og'zaki, raqamli)	Kibermakondagi tizimlar va ma'lumotlar

Jihat	Axborot xavfsizligi	Kiberxavfsizlik
Misol	Nazorat ishi variantlari yozilgan qog'ozni stolda qoldirmaslik	Elektron jurnal serverini hujumlardan himoya qilish
Choralar	Tashkiliy, jismoniy, huquqiy, texnik	Asosan texnik va dasturiy, tashkiliy

2. Axborot xavfsizligining asosiy xususiyatlari: CIA uchligi

Axborot xavfsizligi an'anaviy ravishda uchta asosiy xususiyat orqali ta'riflanadi. Ular inglizcha nomlarining bosh harflari bo'yicha **CIA uchligi** (Confidentiality, Integrity, Availability) deb ataladi [1, 4].



1-rasm. Axborot xavfsizligining CIA uchligi

Konfidensiallik (Confidentiality) – axborotdan faqat unga ruxsati bor shaxslar foydalana olishi. Buzilishiga misollar: o'quvchilarning shaxsiy ma'lumotlari Telegram guruhga tarqalib ketishi; nazorat ishi javoblari oldindan ma'lum bo'lib qolishi; parol stikerga yozilib monitorga yopishtirilganidan begona kishi foydalanishi. Ta'minlash vositalari: shifrlash, kirishni boshqarish, autentifikatsiya, tashkiliy qoidalar.

Yaxlitlik (Integrity) – axborotning to'g'riligi va to'liqligi, unga ruxsatsiz o'zgartirish kiritilmaganligi. Buzilishiga misollar: o'quvchi o'qituvchi parolini bilib elektron jurnaldagi bahoni o'zgartirishi; yuklab olingan dastur fayliga zararli kod qo'shilgan bo'lishi; virus hujjatlarni buzishi. Ta'minlash vositalari: xesh-funksiyalar, elektron raqamli imzo, o'zgarishlar jurnali, kirish huquqlarini cheklash.

Foydalanuvchanlik (Availability) – ruxsati bor foydalanuvchilar axborot va xizmatdan kerakli vaqtda foydalana olishi. Buzilishiga misollar: to'lov talab

qiluvchi dastur maktab kompyuterlaridagi fayllarni shifrlab qo'yishi; server ishdan chiqib, zaxira nusxa bo'lmagani sababli ma'lumotlar yo'qolishi; xizmat ko'rsatishni rad etish (DoS) hujumi tufayli sayt ochilmasligi. Ta'minlash vositalari: zaxira nusxalash, uzluksiz elektr ta'minoti, takrorlanuvchi qurilmalar, hujumlardan himoya.

CIA xususiyatlari o'zaro muvozanatda bo'lishi kerak. Masalan, axborotni juda qattiq himoya qilish (har safar uchta parol so'rash) uning foydalanuvchanligini pasaytiradi. Xavfsizlik choralarini tanlashda muvozanat har bir aktivning qadriga qarab topiladi.

3. Qo'shimcha xususiyatlar

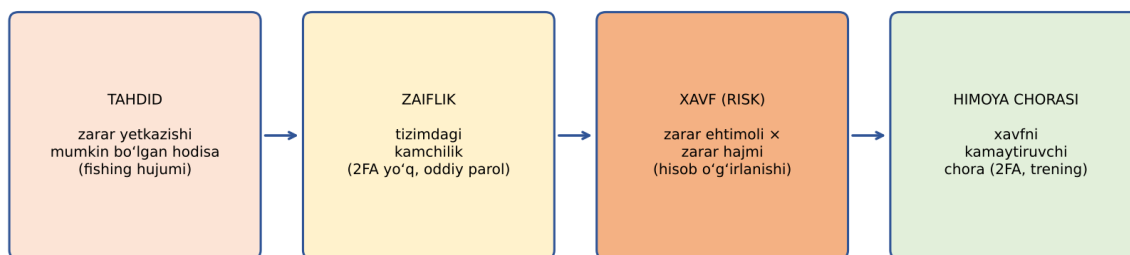
CIA uchligidan tashqari adabiyotda yana bir qator xususiyatlar ajratiladi [1]:

- **autentiklik (haqiqiylik)** – axborot yoki foydalanuvchi o'zini kim deb ko'rsatayotgan bo'lsa, aynan shu ekanligi (masalan, xat haqiqatan ham maktab direktoridan kelgani);
- **inkor etib bo'lmazlik (non-repudiation)** – harakatni bajargan shaxs keyinchalik undan tona olmasligi; elektron raqamli imzo bilan ta'minlanadi;
- **hisobdorlik (accountability)** – har bir harakatni aniq foydalanuvchiga bog'lash imkoniyati; tizim jurnallari (log) orqali ta'minlanadi.

4. Aktiv, tahdid, zaiflik, xavf va himoya chorasi

Axborot xavfsizligida quyidagi tushunchalar o'zaro bog'langan zanjirni tashkil etadi [4]:

Tushuncha	Ta'rif	Maktab misoli
Aktiv	Tashkilot uchun qadrlil bo'lgan har qanday resurs (axborot, dastur, qurilma, xizmat, inson)	Elektron jurnal, o'quvchilar ma'lumotlari, kompyuter sinfi
Tahdid	Aktivga zarar yetkazishi mumkin bo'lgan potensial hodisa yoki harakat	Parolni o'g'irlash, virus, yong'in, xodimning xatosi
Zaiflik	Tahdid amalga oshishiga imkon beruvchi kamchilik	Oddiy parol "123456", yangilanmagan OS, zaxira nusxaning yo'qligi
Hujum	Tahdidni zaiflik orqali amalga oshirishga qaratilgan qasddan harakat	Parollarni tanlab ko'rish, fishing xati yuborish
Xavf (risk)	Tahdid zaiflikdan foydalanib zarar yetkazish ehtimoli va zarar hajmining birikmasi	Jurnal paroli o'g'irlanib baholar o'zgartirilishi xavfi – yuqori
Himoya chorasi	Xavfni kamaytiruvchi vosita yoki harakat	Kuchli parol + 2FA, yangilanishlar, zaxira nusxa



2-rasm. Tahdid – zaiflik – xavf – himoya chorasi zanjiri

Xavf ko‘pincha quyidagi soddalashtirilgan formula bilan ifodalanadi:

$$\text{Xavf} = \text{Ehtimollik} \times \text{Ta'sir}$$

Bu yerda ehtimollik – tahdid zaiflik orqali amalga oshish ehtimoli, ta'sir – shunday hodisa yuz berganda yetkaziladigan zarar hajmi. Agar zaiflik bo‘lmasa, tahdid xavf tug‘dirmaydi; shuning uchun himoyaning asosiy yo‘li – zaifliklarni kamaytirish. Xavflarni baholash va boshqarish 9-mavzuda batafsil ko‘riladi.

Tahdidlar manbalari bo‘yicha

- **tabiiy va texnogen:** yong‘in, suv toshqini, elektr uzilishi, qurilmaning ishdan chiqishi;
- **inson omili (tasodifiy):** faylni adashib o‘chirish, xatni noto‘g‘ri manzilga yuborish, parolni yo‘qotish;
- **inson omili (qasddan):** xakerlar, zararli dastur mualliflari, norozi xodim, qiziquvchan o‘quvchi.

Statistik tadqiqotlar ko‘rsatishicha, insidentlarning katta qismi inson omili – xato, e’tiborsizlik yoki aldov (ijtimoiy muhandislik, 4-mavzu) bilan bog‘liq. Shu sababli foydalanuvchilarni o‘qitish eng samarali himoya choralaridan biridir.

5. Himoya choralarining turlari va ko‘p qatlamli himoya

Chora turi	Misollar
Huquqiy	Qonunlar, me‘yoriy hujjatlar, mehnat shartnomasidagi maxfiylik bandlari
Tashkiliy (ma‘muriy)	Xavfsizlik siyosati, yo‘riqnomalar, mas‘ul shaxs tayinlash, xodimlarni o‘qitish
Jismoniy	Server xonasini qulflash, kamera, kompyuter sinfiga kirish nazorati
Texnik va dasturiy	Parollar, shifrlash, antivirus, tarmoqlararo ekran, zaxira nusxalash

Vazifasi bo‘yicha choralar **oldini oluvchi** (parol, shifrlash), **aniqllovchi** (antivirus, jurnallar, IDS) va **tiklovchi** (zaxira nusxa, tiklash rejasi) turlarga bo‘linadi.

Ko‘p qatlamli himoya (defense in depth) tamoyiliga ko‘ra, bitta himoya vositasiga tayanib bo‘lmaydi: agar bir qatlam yengib o‘tilsa, keyingisi hujumni to‘xtatadi. Masalan, maktab kompyuter sinfi uchun: jismoniy qulf → foydalanuvchi hisobi va parol → cheklangan huquqlar (administrator emas) → antivirus → tarmoqlararo ekran → zaxira nusxa.

Mavzu bo‘yicha xulosa

Axborot xavfsizligi – axborot va infratuzilmaning zararli ta’sirlardan himoyalanganlik holati. Uning asosini konfidensiallik, yaxlitlik va foydalanuvchanlik (CIA) tashkil etadi; ularga autentiklik, inkor etib bo‘lmaslik va hisobdorlik qo‘shiladi. Xavf tahdid zaiflikdan foydalanganda yuzaga keladi va ehtimollik hamda ta’sir bilan baholanadi. Himoya huquqiy, tashkiliy, jismoniy va texnik choralarni ko‘p qatlamli tarzda birlashtiradi.

Nazorat savollari

1. Axborot xavfsizligi va kiberxavfsizlik tushunchalarining farqi nimada?
2. CIA uchligini maktab misolida tushuntiring.
3. Konfidensiallik buzilishiga uchta misol keltiring.
4. Yaxlitlikni ta’minlash vositalarini sanang.
5. Foydalanuvchanlik nima uchun xavfsizlik xususiyati hisoblanadi?
6. Inkor etib bo‘lmaslik qanday ta’minlanadi?
7. Tahdid va zaiflikning farqini misol bilan tushuntiring.
8. Xavf qanday baholanadi?
9. Himoya choralarining qanday turlari bor?
10. Ko‘p qatlamli himoya tamoyilini tushuntiring.

Adabiyotlar: [1], [4]

2-MAVZU. AXBOROT XAVFSIZLIGINING HUQUQIY ASOSLARI. XAVFSIZLIK SIYOSATI

Reja:

1. Axborot xavfsizligi sohasidagi me’yoriy-huquqiy baza.
2. “Kiberxavfsizlik to‘g‘risida”gi Qonun.
3. “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun.
4. Kompyuter axboroti sohasidagi huquqbuzarliklar uchun javobgarlik.
5. Xalqaro standartlar va axborot xavfsizligi siyosati.

Tayanch iboralar:

me’yoriy-huquqiy baza, kiberxavfsizlik, kibermakon, kiberxavfsizlik obyekti, kiberhujum, kiberinsident, muhim axborot infratuzilmasi, shaxsga doir ma’lumotlar, subyekt, mulkdor, operator, rozilik, ERI, ISO/IEC 27001, xavfsizlik siyosati.

1. Axborot xavfsizligi sohasidagi me'yoriy-huquqiy baza

O'zbekiston Respublikasida axborot xavfsizligi sohasidagi munosabatlar Konstitutsiya, qonunlar, Prezident farmon va qarorlari, Vazirlar Mahkamasining qarorlari hamda idoraviy hujjatlar bilan tartibga solinadi. Barcha amaldagi hujjatlarning rasmiy matni Qonunchilik ma'lumotlari milliy bazasida (lex.uz) e'lon qilinadi [11].

Hujjat	Asosiy mazmuni
O'zbekiston Respublikasi Konstitutsiyasi	Shaxsiy hayot daxlsizligi, yozishmalar va telefonda so'zlashuvlar sir saqlanishi huquqi; axborot olish erkinligi
"Axborotlashtirish to'g'risida"gi Qonun (2003-yil 11-dekabr, 560-II)	Axborot resurslari va tizimlari, axborotni muhofaza qilish
"Shaxsga doir ma'lumotlar to'g'risida"gi Qonun (2019-yil 2-iyul, O'RQ-547)	Shaxsga doir ma'lumotlarga ishlov berish va ularni himoya qilish
"Kiberxavfsizlik to'g'risida"gi Qonun (2022-yil 15-aprel, O'RQ-764)	Kiberxavfsizlik sohasidagi davlat siyosati, subyektlar, kiberinsidentlarga javob
"Elektron raqamli imzo to'g'risida"gi Qonun (2022-yil 12-oktabr, O'RQ-793)	ERI dan foydalanish, sertifikatlar, ro'yxatga olish markazlari (6-mavzu)
Jinoyat kodeksi va Ma'muriy javobgarlik to'g'risidagi kodeks	Axborot texnologiyalari sohasidagi huquqbuzarliklar uchun javobgarlik

Izoh: 2003-yil 11-dekabrda 562-II-sonli "Elektron raqamli imzo to'g'risida"gi Qonun 2023-yil yanvaridan kuchini yo'qotgan va uning o'rniga 2022-yil 12-oktabrdagi O'RQ-793-sonli Qonun amal qiladi. Hujjatlarning amaldagi tahririni har doim lex.uz da tekshirish lozim.

2. "Kiberxavfsizlik to'g'risida"gi Qonun

O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni 2022-yil 15-aprelda imzolangan (O'RQ-764) [5]. Qonunning maqsadi – kiberxavfsizlik sohasidagi munosabatlarni tartibga solish. Qonunda quyidagi asosiy tushunchalar belgilangan:

- **kibermakon** – axborot texnologiyalari, Internet va boshqa telekommunikatsiya tarmoqlari yordamida yaratiladigan virtual muhit;
- **kiberxavfsizlik obyektlari** – axborot tizimlari, resurslar, ma'lumotlar bazalari, telekommunikatsiya tarmoqlari va ularni boshqaruvchi infratuzilma;
- **kiberhujum** – kiberxavfsizlik obyektlariga qasddan, dasturiy-texnik vositalar yordamida amalga oshiriladigan ta'sir;
- **kiberinsident** – kiberxavfsizlik obyektlarining ishlashidagi buzilishga olib kelgan yoki olib kelishi mumkin bo'lgan hodisa;

- **muhim axborot infratuzilmasi obyektlari** – faoliyati buzilganda davlat, jamiyat va shaxs manfaatlariga jiddiy zarar yetkazishi mumkin bo‘lgan tizimlar (energetika, transport, bank, telekommunikatsiya va boshqalar).

Qonunga ko‘ra, kiberxavfsizlik sohasidagi vakolatli davlat organi O‘zbekiston Respublikasi Davlat xavfsizlik xizmati hisoblanadi. Qonun kiberxavfsizlik subyektlarining (davlat organlari, tashkilotlar, axborot tizimlari egalari) huquq va majburiyatlarini, kiberinsidentlar haqida xabar berish va ularga javob qaytarish tartibini belgilaydi. Ta’lim muassasalari ham o‘z axborot tizimlari va resurslari (veb-sayt, elektron jurnal, ma’lumotlar bazalari) xavfsizligini ta’minlash majburiyatiga ega.

Ma’ruzada qonunning moddalari bo‘yicha batafsil tahlil lex.uz dagi rasmiy matn asosida olib boriladi. 1-mustaqil topshiriq (referat) aynan shu qonunga bag‘ishlangan.

3. “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun

Qonun 2019-yil 2-iyulda qabul qilingan (O‘RQ-547) va shaxsga doir ma’lumotlarga ishlov berish hamda ularni himoya qilish sohasidagi munosabatlarni tartibga soladi [6].

Shaxsga doir ma’lumotlar – muayyan jismoniy shaxsga taalluqli bo‘lgan yoki uni identifikatsiya qilish imkonini beradigan axborot: familiya, ism, sharif, tug‘ilgan sana, manzil, telefon raqami, pasport ma’lumotlari, JShShIR, fotosurat, baholar va boshqalar.

Qonundagi asosiy ishtirokchilar

Ishtirokchi	Mazmuni va maktab misoli
Subyekt	Ma’lumotlari ishlov berilayotgan jismoniy shaxs – o‘quvchi, ota-ona, o‘qituvchi
Mulkdor	Ma’lumotlar bazasiga egalik qiluvchi shaxs – ta’lim muassasasi
Operator	Ma’lumotlarga ishlov beruvchi shaxs – direktor o‘rinbosari, sinf rahbari, kotib, elektron jurnal tizimi
Uchinchi shaxs	Subyekt, mulkdor va operatoridan tashqari har qanday shaxs

Ishlov berishning asosiy qoidalari

- ma’lumotlar faqat aniq va qonuniy maqsadlarda yig‘iladi va maqsadga zarur hajmdan ortiq yig‘ilmaydi;
- ishlov berish subyektning (voyaga yetmaganlar uchun – qonuniy vakilining) roziligi bilan yoki qonunda nazarda tutilgan hollarda amalga oshiriladi;
- mulkdor va operator ma’lumotlarning maxfiyligini ta’minlashi, ularni ruxsatsiz foydalanishdan himoya qilishi shart;

- subyekt o‘z ma’lumotlari haqida axborot olish, ularni aniqlashtirish, ishlov berishga rozilikni qaytarib olish huquqiga ega;
- O‘zbekiston fuqarolarining shaxsga doir ma’lumotlariga Internetdan foydalanib ishlov berilganda ular O‘zbekiston hududida joylashgan ma’lumotlar bazalarida saqlanishi lozim (qonunga 2021-yilda kiritilgan qo‘shimcha).

Maktab amaliyotida: o‘quvchilar ro‘yxatini, telefon raqamlarini yoki suratlarini ochiq ijtimoiy tarmoqlarda e‘lon qilish, ota-ona rozilgisiz tadbir videolarini joylash, ro‘yxatlarni shaxsiy elektron pochtaga yuborish – qonun talablarini buzish xavfini tug‘diradi.

4. Kompyuter axboroti sohasidagi huquqbuzarliklar uchun javobgarlik

O‘zbekiston Respublikasi Jinoyat kodeksida “Axborot texnologiyalari sohasidagi jinoyatlar” bobi mavjud (278¹–278⁶-moddalar va boshqalar). Unda quyidagi harakatlar uchun javobgarlik belgilangan: axborotlashtirish qoidalarini buzish; kompyuter axborotidan qonunga xilof (ruxsatsiz) foydalanish; ruxsatsiz foydalanish uchun maxsus vositalarni tayyorlash yoki o‘tkazish; kompyuter axborotini modifikatsiyalash; kompyuter sabotaji; zararli dasturlarni yaratish, ishlatish yoki tarqatish. Ma’muriy javobgarlik to‘g‘risidagi kodeksda ham shaxsga doir ma’lumotlar to‘g‘risidagi qonunchilikni buzish uchun javobgarlik nazarda tutilgan.

O‘quvchilarga tushuntirish muhim: “qiziqib ko‘rish”, sinfdoshining akkauntiga “hazil uchun” kirish yoki maktab saytini “sinab ko‘rish” ham qonunga xilof ruxsatsiz foydalanish hisoblanishi mumkin. Xavfsizlikni o‘rganish faqat ruxsat etilgan o‘quv muhitlarida amalga oshiriladi.

5. Xalqaro standartlar va axborot xavfsizligi siyosati

Xalqaro amaliyotda axborot xavfsizligini boshqarish **ISO/IEC 27000** standartlar oilasi asosida tashkil etiladi. Ulardan **ISO/IEC 27001** axborot xavfsizligini boshqarish tizimiga (AXBT) talablarni belgilaydi, **ISO/IEC 27002** esa himoya choralari bo‘yicha amaliy qo‘llanma hisoblanadi. AQSh Milliy standartlar va texnologiyalar instituti (NIST) Kiberxavfsizlik bazaviy tizimi (Cybersecurity Framework, CSF 2.0) xavfsizlik faoliyatini oltita funksiyaga ajratadi: boshqarish (Govern), aniqlash (Identify), himoya qilish (Protect), aniqlash/payqash (Detect), javob berish (Respond), tiklash (Recover) [10].

Axborot xavfsizligi siyosati – tashkilotning axborotni himoya qilish bo‘yicha maqsadlari, qoidalari va mas’uliyatini belgilovchi rasmiy hujjat. Siyosat rahbariyat tomonidan tasdiqlanadi va barcha xodimlarga yetkaziladi.

Xavfsizlik siyosatining namunaviy tuzilishi

1. Maqsad va qo‘llanish sohasi.

2. Atamalar va ta'riflar.
3. Rollar va mas'uliyat (direktor, AT mas'uli, o'qituvchilar, o'quvchilar).
4. Aktivlar ro'yxati va ularni toifalash (ochiq, ichki, maxfiy).
5. Kirishni boshqarish va parol siyosati.
6. Qurilmalar va dasturlardan foydalanish qoidalari (qabul qilinadigan foydalanish qoidalari).
7. Zararli dasturlardan himoya va yangilanishlar.
8. Zaxira nusxalash va tiklash.
9. Insidentlar haqida xabar berish va ularga javob.
10. Shaxsga doir ma'lumotlarni himoya qilish.
11. O'qitish va xabardorlik.
12. Siyosatni qayta ko'rib chiqish tartibi va javobgarlik.

Ushbu tuzilma A10 amaliy mashg'ulotida maktab uchun xavfsizlik siyosati loyihasini ishlab chiqishda asos bo'ladi.

Mavzu bo'yicha xulosa

O'zbekistonda axborot xavfsizligi Konstitutsiya, "Axborotlashtirish to'g'risida", "Shaxsga doir ma'lumotlar to'g'risida", "Kiberxavfsizlik to'g'risida", "Elektron raqamli imzo to'g'risida"gi qonunlar va kodekslar bilan tartibga solinadi. Ta'lim muassasasi o'quvchilar va xodimlarning shaxsga doir ma'lumotlari mulkdori sifatida ularni himoya qilishga majbur. Tashkilot darajasida xavfsizlik ISO/IEC 27001, NIST CSF kabi standartlarga tayangan xavfsizlik siyosati orqali boshqariladi.

Nazorat savollari

1. Axborot xavfsizligi sohasidagi asosiy qonunlarni sanang.
2. "Kiberxavfsizlik to'g'risida"gi Qonun qachon qabul qilingan va uning asosiy tushunchalari qaysilar?
3. Kiberhujum va kiberinsident tushunchalarining farqi nimada?
4. Muhim axborot infratuzilmasi obyektlariga misollar keltiring.
5. Shaxsga doir ma'lumotlarga nimalar kiradi?
6. Subyekt, mulkdor va operator tushunchalarini maktab misolida tushuntiring.
7. Shaxsga doir ma'lumotlarga ishlov berishning asosiy qoidalari qanday?
8. Jinoyat kodeksida qanday kompyuter jinoyatlari uchun javobgarlik belgilangan?
9. ISO/IEC 27001 va NIST CSF ning vazifasi nimada?
10. Xavfsizlik siyosati qanday bo'limlardan iborat bo'ladi?

Adabiyotlar: [5], [6], [11]

3-MAVZU. AXBOROTGA TAHDIDLAR TASNIFI. ZARARLI DASTURLAR: VIRUSLAR, TROYANLAR, CHUVALCHANGLAR, TO'LOV TALAB QILUVCHI DASTURLAR

Reja:

1. Axborotga tahdidlarning tasnifi.
2. Zararli dastur tushunchasi va tasnifi.
3. Viruslar va chuvalchanglar.
4. Trojanlar, josus dasturlar va boshqa turlar.
5. To'lov talab qiluvchi dasturlar.
6. Zararli dasturlarning tarqalish yo'llari va ulardan himoyalash.

Tayanch iboralar:

tahdid, passiv va faol hujum, zararli dastur (malware), virus, chuvalchang (worm), troyan, "orqa eshik" (backdoor), josus dastur (spyware), keylogger, reklama dasturi (adware), kriptomayner, botnet, rootkit, to'lov talab qiluvchi dastur (ransomware), nol kunlik zaiflik, antivirus, signatura, evristik tahlil.

1. Axborotga tahdidlarning tasnifi

Tahdidlar turli belgilar bo'yicha tasniflanadi [1, 3]:

Tasnif belgisi	Turlari
Manbai bo'yicha	Tabiiy, texnogen, antropogen (inson omili)
Niyat bo'yicha	Tasodifiy (xato, e'tiborsizlik), qasddan (hujum)
Joylashuvi bo'yicha	Ichki (xodim, o'quvchi), tashqi (Internetdagi hujumchi)
Buziladigan xususiyat bo'yicha	Konfidensiallikka, yaxlitlikka, foydalanuvchanlikka tahdid
Ta'sir xarakteri bo'yicha	Passiv (eshitib olish, trafikni kuzatish), faol (ma'lumotni o'zgartirish, xizmatni to'xtatish)
Vositasi bo'yicha	Dasturiy (zararli dastur), tarmoq (hujumlar), ijtimoiy (aldash), jismoniy (qurilmani o'g'irlash)

Passiv hujumlarda hujumchi ma'lumotni faqat kuzatadi yoki nusxalaydi; tizim ishida o'zgarish sezilmaydi, shuning uchun ularni aniqlash qiyin, asosiy himoya – shifrlash. **Faol hujumlarda** ma'lumot o'zgartiriladi, soxta xabar yuboriladi yoki xizmat to'xtatiladi; ularni aniqlash va oqibatlarini tiklash muhim [2].

2. Zararli dastur tushunchasi va tasnifi

Zararli dastur (malware – malicious software) – foydalanuvchi bilmagan holda yoki uning roziligisiz kompyuter tizimiga zarar yetkazish, axborotni

o'g'irlash, o'zgartirish, yo'q qilish yoki tizim resurslaridan ruxsatsiz foydalanish uchun yaratilgan dastur.

Turi	Asosiy xususiyati	Asosiy xavfi
Virus	Boshqa fayl yoki dasturga o'z kodini yozib ko'payadi; faollashishi uchun foydalanuvchi harakati kerak	Yaxlitlik, foydalanuvchanlik
Chuvalchang (worm)	Tarmoq orqali mustaqil tarqaladi, boshqa faylga ehtiyoj sezmaydi	Tez tarqalish, tarmoq yuklamasi
Trojan	Foydali dastur qiyofasida niqoblanadi, o'zi ko'paymaydi	Masofadan boshqarish, ma'lumot o'g'irlash
Josus dastur (spyware), keylogger	Foydalanuvchi harakatlari va klaviatura bosishlarini yashirincha yozib oladi	Konfidensiallik (parollar)
Reklama dasturi (adware)	Kerakmas reklamalarni ko'rsatadi	Noqulaylik, boshqa tahdidlar uchun yo'l
Kriptomayner	Kompyuter resurslaridan kriptovalyuta qazib olish uchun foydalanadi	Unumdorlik pasayishi
Rootkit	Zararli dastur mavjudligini OS darajasida yashiradi	Aniqlash qiyinligi
Botnet	Masofadan boshqariladigan zararlangan kompyuterlar tarmog'i	DDoS hujumlari, spam
To'lov talab qiluvchi dastur (ransomware)	Fayllarni shifrlab, ochish uchun to'lov talab qiladi	Foydalanuvchanlik, ma'lumotlar yo'qolishi

3. Viruslar va chuvalchanglar

Kompyuter virusi o'z nusxasini boshqa dasturlar, hujjatlar (makroviruslar) yoki disk yuklash sektoriga yozib ko'payadi. Virus "yuqtirilgan" fayl ishga tushirilganda faollashadi. Hayot sikli bosqichlari: yashirin (kutish) → tarqalish → ishga tushish sharti → zararli harakat (payload) [1].

Chuvalchang viruslardan farqli ravishda foydalanuvchi harakatisiz, tarmoqdagi zaifliklar yoki elektron pochta orqali o'zini o'zi tarqatadi. Tarixiy misollar:

- **Morris chuvalchangi (1988)** – Internetda keng tarqalgan ilk chuvalchanglardan biri; o'sha paytdagi Internetga ulangan kompyuterlarning sezilarli qismini ishdan chiqargan va kompyuter xavfsizligi bo'yicha javob guruhlari (CERT) tashkil etilishiga turtki bergan;
- **ILOVEYOU (2000)** – "sevgi maktubi" niqobidagi elektron pochta ilovasi orqali tarqalgan; ijtimoiy muhandislik va zararli dastur birikmasining klassik misoli.

4. Trojanlar, josus dasturlar va boshqa turlar

Trojan dasturi nomini qadimgi yunon afsonasidagi “Troya oti”dan olgan: foydali dastur (o‘yin, “bepul” dastur, “kreklangan” dastur, soxta yangilanish) qiyofasida tizimga kiradi. Troyanning keng tarqalgan turlari: masofadan boshqarish troyanlari (RAT), bank troyanlari, parol o‘g‘rilari (stealer), yuklovchilar (downloader).

Josus dasturlar va keyloggerlar foydalanuvchi kiritgan parollar, bank kartasi ma’lumotlari va yozishmalarni yashirincha yig‘adi. Ommaviy kompyuterlarda (Internet-kafe, kutubxona) shaxsiy akkauntga kirish shu sababli xavfli.

Pedagogik tavsiya: o‘quvchilar orasida eng ko‘p uchraydigan zararlanish yo‘li – o‘yinlar uchun “cheat”, “bepul skin” yoki pullik dasturlarning “kreklangan” versiyalarini yuklab olish. Bunday fayllar ko‘pincha parol o‘g‘rilari bilan birga tarqatiladi.

5. To‘lov talab qiluvchi dasturlar

To‘lov talab qiluvchi dastur (ransomware) foydalanuvchi fayllarini kuchli kriptografik algoritm bilan shifrlaydi va ochish kaliti evaziga (odatda kriptovalyutada) to‘lov talab qiladi. Zamonaviy guruhlar “ikki tomonlama tovlamachilik” usulini qo‘llaydi: avval ma’lumotlarni o‘g‘irlab, keyin shifrlaydi va to‘lanmasa e’lon qilish bilan tahdid qiladi.

WannaCry (2017) – Windows’dagi SMB protokoli zaifligidan foydalangan va chuvalchang kabi tarqalgan to‘lov talab qiluvchi dastur. U bir necha kun ichida 150 dan ortiq mamlakatda yuz minglab kompyuterlarni zararlagan, jumladan kasalxonalar faoliyatini to‘xtatgan. Microsoft tegishli yangilanishni hujumdan taxminan ikki oy oldin chiqargan edi – yangilanishlarni o‘z vaqtida o‘rnatgan tizimlar zararlanmagan [3].

To‘lov talab qiluvchi dasturlardan himoyaning asosiy qoidalari

- muntazam, **tarmoqdan ajratilgan** zaxira nusxalar (3-2-1 qoidasi, 9-mavzu);
- OS va dasturlarni o‘z vaqtida yangilash;
- foydalanuvchilarga administrator huquqlarini bermaslik;
- noma’lum ilovalarni ochmaslik, makroslarni o‘chirib qo‘yish;
- to‘lov to‘lash fayllar qaytarilishiga kafolat bermaydi va jinoyatchilarni rag‘batlantiradi; insident haqida mas’ul shaxsga va vakolatli organlarga xabar berish lozim.

6. Zararli dasturlarning tarqalish yo‘llari va ulardan himoyalash

Asosiy tarqalish yo‘llari

- elektron pochta ilovalari va fishing havolalari (4-mavzu);

- messenjerlarda yuborilgan fayllar (masalan, .apk, .exe, .scr, makrosli hujjatlar);
- norasmiy saytlardan yuklangan dasturlar, “kreklar”, o‘yin “cheat”lari;
- USB-flesh disklar va boshqa olinadigan qurilmalar;
- OS, brauzer va dasturlardagi yangilanmagan zaifliklar;
- zararlangan veb-saytlar va soxta reklama.

Antiviruslarning aniqlash usullari

Usul	Mazmuni
Signatura usuli	Fayl ma’lum zararli dasturlar bazasidagi “barmoq izlari” bilan solishtiriladi; ma’lum tahdidlarni aniq topadi, yangilarini topmaydi
Evristik tahlil	Kod tuzilishi va buyruqlar shubhali bo‘lsa ogohlantiradi
Xulq-atvor tahlili	Dastur ishlayotganda shubhali harakatlar (ko‘p faylni tez shifrlash, tizim sozlamalarini o‘zgartirish) kuzatiladi
Bulutli tahlil va qum qutisi (sandbox)	Noma’lum fayl ajratilgan muhitda ishga tushirilib tekshiriladi

Nol kunlik (zero-day) zaiflik – ishlab chiquvchiga hali ma’lum bo‘lmagan yoki tuzatish chiqarilmagan zaiflik. Bunday hujumlarga qarshi signatura usuli samarasiz, shuning uchun xulq-atvor tahlili, kam huquqlar tamoyili va zaxira nusxalar muhim ahamiyatga ega.

Mavzu bo‘yicha xulosa

Tahdidlar manbai, niyati, joylashuvi va ta’sir xarakteri bo‘yicha tasniflanadi. Zararli dasturlar virus, chuvalchang, troyan, josus dastur, rootkit, botnet, to‘lov talab qiluvchi dastur kabi turlarga bo‘linadi. Ularning asosiy tarqalish yo‘llari – elektron pochta, messenjerlar, norasmiy dasturlar va yangilanmagan zaifliklar. Himoya antivirus, yangilanishlar, cheklangan huquqlar, zaxira nusxalar va foydalanuvchilar ongliligini birlashtiradi.

Nazorat savollari

1. Tahdidlar qanday belgilar bo‘yicha tasniflanadi?
2. Passiv va faol hujumlarning farqi nimada?
3. Virus va chuvalchangning asosiy farqini tushuntiring.
4. Trojan dasturi nima uchun shunday nomlangan?
5. Keylogger qanday xavf tug‘diradi?
6. To‘lov talab qiluvchi dastur qanday ishlaydi?
7. WannaCry hujumidan qanday saboq olish mumkin?
8. Zararli dasturlarning asosiy tarqalish yo‘llarini sanang.
9. Signatura va xulq-atvor tahlili usullarini taqqoslang.
10. Nol kunlik zaiflik nima va undan qanday himoyalaniadi?

Adabiyotlar: [1], [3]

4-MAVZU. IJTIMOIIY MUHANDISLIK VA FISHING HUJUMLARI, ULARDAN HIMOYALANISH

Reja:

1. Ijtimoiy muhandislik tushunchasi va uning psixologik asoslari.
2. Ijtimoiy muhandislik hujumlarining turlari.
3. Fishing va uning turlari.
4. Fishing xatlari va saytlarini aniqlash belgilari.
5. Ijtimoiy muhandislikdan himoyalaniş choralari.

Tayanch iboralar:

ijtimoiy muhandislik, fishing, nishonli fishing (spear phishing), vishing, smishing, kvishing, pretexting, baiting, quid pro quo, tailgating, domen, URL, soxta sayt, ishonch, shoshilinchlik, avtoritet, ikki kanalli tekshiruv.

1. Ijtimoiy muhandislik tushunchasi va uning psixologik asoslari

Ijtimoiy muhandislik (social engineering) – texnik zaifliklar o‘rniga inson psixologiyasidan foydalanib, uni maxfiy axborotni oshkor qilishga yoki xavfsizlikni buzuvchi harakatni bajarishga undash usullari majmui. Mashhur sobiq xaker K. Mitnik o‘z kitobida xavfsizlik zanjirining eng zaif bo‘g‘ini – inson ekanligini ko‘plab misollar bilan ko‘rsatgan [7]: eng kuchli shifrlash ham parolini telefon orqali “texnik xizmat xodimi”ga aytib bergan foydalanuvchini himoya qila olmaydi.

Ijtimoiy muhandislar foydalanadigan psixologik omillar

Omil	Misol
Avtoritet (obro‘)	“Men vazirlikdanman / bank xavfsizlik xizmatidanman, darhol tasdiqlang”
Shoshilinchlik	“Hisobingiz 24 soat ichida bloklandi”, “Faqat bugun!”
Qo‘rquv	“Sizning nomingizga jinoiy ish ochilgan”, “Kompyuteringizda virus topildi”
Ochko‘zlik va qiziqish	“Siz iPhone yutib oldingiz”, “Sindoshingizning sirli suratlari”
Yordam berish istagi	“Hamkasbingizman, parolni unutibman, yordam bering”
Ijtimoiy isbot	“Barcha o‘qituvchilar allaqachon ro‘yxatdan o‘tdi”
Ishonch va tanishlik	Do‘stining buzilgan akkauntidan kelgan xabar

2. Ijtimoiy muhandislik hujumlarining turlari

Turi	Mazmuni
Fishing	Ishonchli tashkilot nomidan soxta xat yoki xabar orqali parol, karta ma’lumotlarini olish yoki zararli fayl ochtirish

Turi	Mazmuni
Pretexting (bahona)	Oldindan o‘ylab topilgan “ssenariy” asosida ishonch qozonish (masalan, o‘zini auditor deb tanishtirish)
Baiting (qarmoq)	Qiziqtiruvchi “o‘lja” – yo‘lakda qoldirilgan “Maoshlar 2026” yozuvli USB-flesh disk, “bepul” fayl
Quid pro quo (xizmat evaziga)	“Texnik yordam” taklif qilib, evaziga parol yoki masofadan ulanish ruxsatini so‘rash
Tailgating (izma-iz kirish)	Ruxsati bor xodim ortidan yopiq xonaga (server xonasi) kirib olish
Vishing	Telefon qo‘ng‘irog‘i orqali aldash (soxta “bank xodimi” SMS-kodni so‘raydi)
Smishing	SMS yoki messenjer xabari orqali fishing
Kvishing	QR-kod orqali soxta saytga yo‘naltirish

3. Fishing va uning turlari

Fishing (phishing) – inglizcha *fishing* (baliq ovlash) so‘zidan kelib chiqqan; ijtimoiy muhandislikning eng keng tarqalgan turi. Hujumchi bank, pochta xizmati, davlat portali, ta’lim platformasi yoki tanish odam nomidan xabar yuborib, qurbonni soxta saytga kirishga, ma’lumot kiritishga yoki faylni ochishga undaydi [9].

- **Ommaviy fishing** – minglab manzillarga bir xil xat yuboriladi;
- **Nishonli fishing (spear phishing)** – aniq shaxs yoki tashkilot haqida oldindan ma’lumot yig‘ilib, shaxsiylashtirilgan xat tuziladi (masalan, maktab direktori nomidan o‘qituvchilarga “Yangi dars jadvali” ilovasi);
- **Kit ovi (whaling)** – rahbarlarga qaratilgan nishonli fishing;
- **Biznes pochtasini buzish (BEC)** – rahbar yoki hamkor nomidan pul o‘tkazish yoki hujjat yuborish talabi;
- **Klon fishing** – ilgari olingan haqiqiy xat nusxalanib, havola yoki ilova zararlisiga almashtiriladi.

Generativ sun‘iy intellekt vositalari xatosiz va ishonarli fishing matnlarini yaratishni osonlashtirdi; endi “imlo xatolari” fishingning ishonchli belgisi bo‘la olmaydi. Asosiy e’tibor jo‘natuvchi manzili, havola domeni va so‘ralayotgan harakatga qaratilishi kerak.

4. Fishing xatlari va saytlarini aniqlash belgilari

Xatning belgilari

- jo‘natuvchi manzili tashkilot domeniga mos kelmaydi yoki o‘xshatib yozilgan (support@paypa1.com, info@uzedu-gov.com);
- umumiy murojaat (“Hurmatli mijoz”) yoki aksincha, sizning ma’lumotlaringiz ishlatilgan shoshiltiruvchi matn;
- shoshilinchlik, qo‘rquv yoki o‘ta qiziqarli taklif;

- parol, SMS-kod, karta raqami yoki CVV kodini so‘rash (rasmiy tashkilotlar buni hech qachon so‘ramaydi);
- kutilmagan ilova (.zip, .exe, .html, makrosli .docm, .xlsm);
- havola matni bilan haqiqiy manzil mos kelmasligi (sichqonchani havola ustiga olib borib tekshiriladi).

Havola (URL) tahlili

URL ning eng muhim qismi – **asosiy domen**: u birinchi / belgisidan oldingi qismning oxirgi ikki (ba’zan uch) bo‘lagidan iborat.

Havola	Haqiqiy domen va xulosa
https://my.gov.uz/oz/service/123	gov.uz – rasmiy portal
https://my.gov.uz.login-check.com/oz	login-check.com – soxta, my.gov.uz faqat subdomen nomi
http://emaktab-uz.net/kirish	emaktab-uz.net – rasmiy domen emas, HTTPS ham yo‘q
https://accounts.google.com.secure-verify.top/	secure-verify.top – soxta
https://www.g00gle.com/	g00gle.com – “o” o‘rniga nol (tayposkvotting)

HTTPS va qulf belgisi saytning **haqiqiyligini** emas, faqat ulanish shifrlanganini bildiradi. Hozirgi kunda fishing saytlarining katta qismi ham HTTPS dan foydalanadi.

5. Ijtimoiy muhandislikdan himoyalash choralari

Foydalanuvchi darajasida

- “To‘xta – o‘yla – tekshir” qoidasi: shoshiltiruvchi xabarga darhol javob bermaslik;
- **ikki kanalli tekshiruv**: shubhali so‘rovni boshqa kanal orqali (rasmiy telefon raqami, shaxsan) tasdiqlash;
- havolani bosish o‘rniga saytga brauzer manzil qatoriga o‘zi yozib yoki xatcho‘pdan kirish;
- SMS-kod va parollarni hech kimga aytmaslik;
- ikki faktorli autentifikatsiyani yoqish (5-mavzu);
- shubhali xatni “Spam/Fishing” deb belgilash va mas’ul shaxsga xabar berish.

Tashkilot darajasida

- xodimlarni muntazam o‘qitish va o‘quv fishing mashqlari;
- pochta filtrlari, SPF, DKIM va DMARC kabi pochta autentifikatsiyasi texnologiyalari;
- pul o‘tkazish va ma’lumot yuborish uchun aniq tasdiqlash tartibi;
- “ayblamaslik madaniyati”: adashib havolani bosgan xodim tezda xabar bera olishi kerak.

Mavzu bo'yicha xulosa

Ijtimoiy muhandislik inson psixologiyasidagi avtoritet, shoshilinchlik, qo'rquv va qiziqish kabi omillardan foydalanadi. Fishing, pretexting, baiting, vishing, smishing va kvishing uning keng tarqalgan turlaridir. Fishingni aniqlashning asosiy usuli – jo'natuvchi va havola domenini tekshirish hamda so'ralayotgan harakatni tanqidiy baholash. Eng samarali himoya – xabardor foydalanuvchi, ikki kanalli tekshiruv va 2FA.

Nazorat savollari

1. Ijtimoiy muhandislik nima va u nima uchun samarali?
2. Ijtimoiy muhandislar qanday psixologik omillardan foydalanadi?
3. Pretexting va baiting hujumlariga misol keltiring.
4. Ommaviy va nishonli fishingning farqi nimada?
5. Vishing, smishing va kvishing nima?
6. Fishing xatining asosiy belgilarini sanang.
7. URL dagi asosiy domen qanday aniqlanadi?
8. HTTPS belgisi saytning haqiqiyligini kafolatlaydimi?
9. Ikki kanalli tekshiruv nima?
10. Tashkilot fishingdan himoyalalanish uchun qanday choralar ko'radi?

Adabiyotlar: [7], [9]

5-MAVZU. IDENTIFIKATSIYA, AUTENTIFIKATSIYA VA AVTORIZATSIYA. PAROL SIYOSATI, IKKI FAKTORLI AUTENTIFIKATSIYA

Reja:

1. Identifikatsiya, autentifikatsiya va avtorizatsiya tushunchalari.
2. Autentifikatsiya omillari.
3. Parollar: hujum turlari va parol siyosati.
4. Ikki faktorli va ko'p faktorli autentifikatsiya.
5. Kirishni boshqarish modellari va kam huquqlar tamoyili.

Tayanch iboralar:

identifikator, identifikatsiya, autentifikatsiya, avtorizatsiya, autentifikatsiya omili, parol, parol iborasi (passphrase), entropiya, lug'at hujumi, to'liq tanlash, parollarni to'ldirish (credential stuffing), parol menejeri, 2FA, MFA, TOTP, passkey, DAC, MAC, RBAC, kam huquqlar tamoyili.

1. Identifikatsiya, autentifikatsiya va avtorizatsiya tushunchalari

Tizimga kirish jarayoni uch bosqichdan iborat [1, 4]:

Bosqich	Mazmuni	Savol va misol
Identifikatsiya	Foydalanuvchi o'zini tanishtiradi – identifikator (login) taqdim etadi	“Siz kimsiz?” – login: n.karimova
Autentifikatsiya	Taqdim etilgan identifikatorning haqiqiyliги tekshiriladi	“Buni isbotlang” – parol + SMS-kod
Avtorizatsiya	Autentifikatsiyadan o'tgan foydalanuvchiga huquqlar beriladi	“Sizga nima mumkin?” – o'qituvchi faqat o'z sinflari baholarini kiritadi

Bu bosqichlarga **hisobga olish (audit)** qo'shiladi: foydalanuvchi harakatlari jurnalga yoziladi (kim, qachon, nima qildi). Masalan, elektron jurnalda bahoni kim va qachon o'zgartirgani qayd etiladi.

2. Autentifikatsiya omillari

Omil turi	Mazmuni	Misollar
Bilish omili	Foydalanuvchi biladigan narsa	Parol, PIN-kod, maxfiy savol javobi
Egalik omili	Foydalanuvchida bor narsa	Smartfon (SMS, autentifikator ilovasi), smart-karta, USB-kalit (FIDO2)
Biometrik omil	Foydalanuvchining o'zi	Barmoq izi, yuz tasviri, ko'z qorachig'i, ovoz

Ikki **har xil** turdagi omilning birgalikda qo'llanishi ikki faktorli autentifikatsiya deyiladi. Parol va maxfiy savol – ikkalasi ham bilish omili, shuning uchun bu 2FA hisoblanmaydi.

3. Parollar: hujum turlari va parol siyosati

Parollarga hujum turlari

- **to'liq tanlash (brute force)** – barcha mumkin bo'lgan kombinatsiyalarni tekshirish;
- **lug'at hujumi** – keng tarqalgan parollar va so'zlar ro'yxatidan foydalanish (**123456, qwerty, parol, Toshkent2026**);
- **parollarni to'ldirish (credential stuffing)** – bir saytdan sizib chiqqan login-parollarni boshqa saytlarda sinash; bir xil parolni ko'p joyda ishlatish xavfining asosiy sababi;
- **fishing va keylogger** – parolni bevosita foydalanuvchidan o'g'irlash (3–4-mavzular);
- **yelka osha kuzatish (shoulder surfing)** – parol kiritilayotganda kuzatib turish.

Parol kuchliligi va entropiya

Parolning kuchliligi uning **uzunligi** va **belgilar alifbosi** hajmiga bog'liq. Mumkin bo'lgan kombinatsiyalar soni: N^L (N – alifbo hajmi, L – uzunlik). Entropiya (bitlarda): $H = L \cdot \log_2 N$.

Parol turi	N	L	Kombinatsiyalar	Entropiya, bit
Faqat raqamlar (PIN)	10	6	10^6	≈ 20
Kichik lotin harflari	26	8	$\approx 2,1 \cdot 10^{11}$	≈ 38
Katta-kichik harf + raqam	62	8	$\approx 2,2 \cdot 10^{14}$	≈ 48
Katta-kichik harf + raqam + belgilar	94	12	$\approx 4,8 \cdot 10^{23}$	≈ 79
4 ta tasodifiy so'zdan parol iborasi (7776 so'zli lug'at)	7776	4	$\approx 3,7 \cdot 10^{15}$	≈ 52
6 ta tasodifiy so'zdan parol iborasi	7776	6	$\approx 2,2 \cdot 10^{23}$	≈ 78

Izoh: entropiya formulasi belgilar **tasodifiy** tanlangan holat uchun to'g'ri. "Parol2026!" kabi inson o'ylab topgan parollar formal ravishda ko'p turdagi belgilarga ega bo'lsa-da, lug'at hujumlarida tez topiladi.

Zamonaviy parol siyosati (NIST SP 800-63B tavsiyalari asosida)

NIST ning raqamli identifikatsiya bo'yicha qo'llanmasi an'anaviy "murakkab, lekin qisqa va tez-tez almashtiriladigan parol" yondashuvidan voz kechib, quyidagilarni tavsiya etadi [10]:

- uzunlikka urg'u: kamida 8 belgi (faqat parol ishlatilsa – 15 belgi), kamida 64 belgigacha uzun parollarga ruxsat berish;
- majburiy "katta harf + raqam + belgi" tarkibi qoidalarini talab qilmaslik;
- parolni muntazam (masalan, har 90 kunda) majburiy almashtirmaslik, faqat buzilganlik belgisi bo'lganda almashtirish;
- yangi parolni sizib chiqqan va keng tarqalgan parollar ro'yxati bilan solishtirish;
- parolni joylashtirish (paste) va parol menejerlaridan foydalanishga ruxsat berish;
- noto'g'ri urinishlar sonini cheklash.

Parol menejeri (KeePassXC, Bitwarden va boshqalar) – parollarni shifrlangan ma'lumotlar bazasida saqlaydigan va har bir sayt uchun tasodifiy kuchli parol yaratadigan dastur. Foydalanuvchi faqat bitta kuchli asosiy parolni (parol iborasini) eslab qoladi.

4. Ikki faktorli va ko‘p faktorli autentifikatsiya

2FA (two-factor authentication) va **MFA (multi-factor authentication)** – ikki yoki undan ortiq har xil omil talab qilinadigan autentifikatsiya. Parol o‘g‘irlangan taqdirda ham hujumchi ikkinchi omilsiz kira olmaydi.

Usul	Afzalligi	Kamchiligi
SMS-kod	Oddiy, keng tarqalgan	SIM-kartani almashtirish (SIM swap), SMS ni ushlash, fishing
Autentifikator ilovasi (TOTP)	Har 30 soniyada yangilanadigan kod, Internet talab qilmaydi	Telefon yo‘qolsa zaxira kodlar kerak
Push-tasdiqlash	Qulay	“Bildirishnomalar bombardimoni” – charchagan foydalanuvchi tasdiqlab yuborishi
Apparat kalit, passkey (FIDO2/WebAuthn)	Fishingga chidamli: soxta saytda ishlamaydi	Qo‘shimcha qurilma yoki zamonaviy qurilma talab etiladi

TOTP (Time-based One-Time Password) algoritmda server va ilova umumiy maxfiy kalitga ega (odatda QR-kod orqali ulashiladi). Kod joriy vaqt va kalit asosida xesh-funksiya yordamida hisoblanadi, shuning uchun ikkala tomon ham bir xil kodni mustaqil hisoblaydi.

2FA ni sozlashda beriladigan **zaxira kodlar** chop etilib xavfsiz joyda saqlanishi kerak – telefon yo‘qolganda akkauntga faqat ular yordamida kirish mumkin.

5. Kirishni boshqarish modellari va kam huquqlar tamoyili

Model	Mazmuni
DAC – ixtiyoriy kirishni boshqarish	Resurs egasi kimga qanday huquq berishni o‘zi belgilaydi (Google Drive’da faylni ulashish)
MAC – majburiy kirishni boshqarish	Huquqlar maxfiylik darajalari asosida tizim tomonidan qat’iy belgilanadi (harbiy tizimlar)
RBAC – rollarga asoslangan boshqaruv	Huquqlar rollarga beriladi, foydalanuvchiga rol tayinlanadi (elektron jurnal: direktor, o‘qituvchi, sinf rahbari, o‘quvchi, ota-ona)

Kam huquqlar tamoyili (least privilege) – har bir foydalanuvchi va dasturga faqat vazifasini bajarish uchun zarur bo‘lgan minimal huquqlar beriladi. Masalan, kompyuter sinfida o‘quvchilar va hatto o‘qituvchi kundalik ishni oddiy foydalanuvchi hisobida bajaradi; administrator hisobidan faqat dastur o‘rnatish va sozlash uchun foydalaniladi. Bu zararli dasturlar yetkazadigan zararni keskin kamaytiradi (A8).

Mavzu bo'yicha xulosa

Tizimga kirish identifikatsiya, autentifikatsiya va avtorizatsiya bosqichlaridan iborat, ularni audit to'ldiradi. Autentifikatsiya bilish, egalik va biometrik omillarga asoslanadi. Parolning kuchliligi asosan uzunligi va tasodifiyligiga bog'liq; zamonaviy tavsiyalar uzun parol iboralari, parol menejerlari va sizib chiqqan parollarni tekshirishni qo'llab-quvvatlaydi. 2FA, ayniqsa fishingga chidamli passkey usullari, akkauntlar xavfsizligini keskin oshiradi. Kirish huquqlari RBAC va kam huquqlar tamoyili asosida beriladi.

Nazorat savollari

1. Identifikatsiya, autentifikatsiya va avtorizatsiyaning farqini tushuntiring.
2. Autentifikatsiya omillarining turlarini misollar bilan sanang.
3. Nima uchun parol va maxfiy savol 2FA hisoblanmaydi?
4. Credential stuffing hujumi qanday amalga oshiriladi?
5. Parol entropiyasi qanday hisoblanadi?
6. NIST ning zamonaviy parol tavsiyalari qanday?
7. Parol menejerining afzalliklari nimada?
8. 2FA usullarini xavfsizlik nuqtayi nazaridan taqqoslang.
9. TOTP qanday ishlaydi?
10. RBAC modeli va kam huquqlar tamoyilini maktab misolida tushuntiring.

Adabiyotlar: [1], [4]

6-MAVZU. KRIPTOGRAFIYA ASOSLARI: SIMMETRIK VA ASIMMETRIK SHIFRLASH, XESH-FUNKSIYALAR, ELEKTRON RAQAMLI IMZO

Reja:

1. Kriptografiyaning asosiy tushunchalari.
2. Klassik shifrlar: o'rniga qo'yish va o'rin almashtirish.
3. Simmetrik shifrlash. AES algoritmi.
4. Asimmetrik shifrlash. RSA algoritmi.
5. Xesh-funksiyalar.
6. Elektron raqamli imzo va ochiq kalitlar infratuzilmasi.

Tayanch iboralar:

kriptografiya, kriptotahlil, ochiq matn, shifrmtn, kalit, shifrlash, deshifrlash, Kerkgooffs tamoyili, Sezar shifri, Vijiner shifri, chastota tahlili, simmetrik shifrlash, AES, asimmetrik shifrlash, ochiq kalit, yopiq kalit, RSA, gibrid shifrlash, xesh-funksiya, SHA-256, ERI, sertifikat, ochiq kalitlar infratuzilmasi (PKI), E-IMZO.

1. Kriptografiyaning asosiy tushunchalari

Kriptografiya – axborotni ruxsatsiz shaxslar o‘qiy olmaydigan shaklga keltirish, uning yaxlitligi va haqiqiyligini ta‘minlash usullari haqidagi fan. **Kriptotahlil** – kalitni bilmasdan shifrnı ochish usullarini o‘rganadi; ikkalasi birgalikda **kriptologiyani** tashkil etadi [2].

Atama	Mazmuni
Ochiq matn (plaintext)	Shifrlanmagan dastlabki axborot
Shifrmatn (ciphertext)	Shifrlangandan keyingi o‘qib bo‘lmaydigan axborot
Kalit	Shifrlash va deshifrlash algoritmini boshqaruvchi maxfiy parametr
Shifrlash	Ochiq matnni kalit yordamida shifrmatnga aylantirish: $C = E(K, P)$
Deshifrlash	Shifrmatndan kalit yordamida ochiq matnni tiklash: $P = D(K, C)$

Kerkgooffs tamoyili (1883): shifrlash tizimining xavfsizligi algoritmnı sir saqlashga emas, faqat **kalitni** sir saqlashga asoslanishi kerak. Shu sababli zamonaviy algoritmlar (AES, RSA) ochiq e‘lon qilingan va dunyo olimlari tomonidan tekshirilgan.

2. Klassik shifrlar

Sezar shifri – o‘rniga qo‘yish shifrining eng oddiy turi: har bir harf alifboda k pozitsiya siljiriladi. Lotin alifbosi (26 harf) uchun: $C = (P + k) \bmod 26$, $P = (C - k) \bmod 26$.

Misol ($k = 3$): **INFORMATIKA** → **LQIRUPDWLND**. $I (8) + 3 = 11 \rightarrow L$; $A (0) + 3 = 3 \rightarrow D$ va hokazo.

Sezar shifrida faqat 25 ta mumkin bo‘lgan kalit bor, shuning uchun u to‘liq tanlash orqali bir zumda ochiladi. Bundan tashqari, barcha bir alifboli o‘rniga qo‘yish shifrlari **chastota tahlili** bilan ochiladi: tilda eng ko‘p uchraydigan harflar (o‘zbek tilida “a”, “i”) shifrmatnda ham eng ko‘p uchraydigan belgilarga mos keladi.

Vijiner shifri – ko‘p alifboli shifr: kalit so‘zning har bir harfi alohida siljish miqdorini beradi. $C_i = (P_i + K_{(i \bmod m)}) \bmod 26$, bu yerda m – kalit uzunligi.

Misol: ochiq matn **MAKTAB**, kalit **KOD** (siljishlar 10, 14, 3):

Ochiq matn	M	A	K	T	A	B
Kalit	K	O	D	K	O	D
Siljish	10	14	3	10	14	3
Shifrmatn	W	O	N	D	O	E

Vijiner shifri bir xil harfni turli belgilarga aylantirgani uchun oddiy chastota tahlilidan himoyalangan, ammo XIX asrda Kasiski usuli bilan kalit uzunligi

aniqlanib ochilgan. Klassik shifrlar bugungi kunda faqat o'quv maqsadida qo'llaniladi (A4).

3. Simmetrik shifrlash. AES algoritmi

Simmetrik shifrlashda shifrlash va deshifrlash uchun **bitta umumiy maxfiy kalit** ishlatiladi. Afzalligi – yuqori tezlik, katta hajmdagi ma'lumotlarni shifrlash uchun qulay. Asosiy muammosi – **kalitni tarqatish**: ikki tomon kalitni oldindan xavfsiz kanal orqali almashishi kerak; n ta foydalanuvchi o'zaro juft-juft aloqa qilishi uchun $n(n-1)/2$ ta kalit kerak bo'ladi.

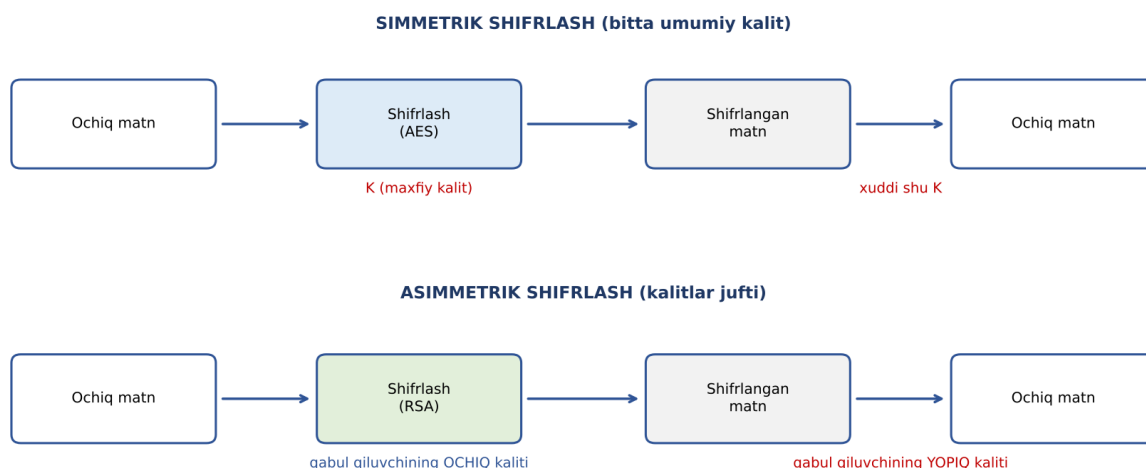
AES (Advanced Encryption Standard) – 2001-yilda AQSh NIST tomonidan standart sifatida qabul qilingan (Belgiya olimlari J. Daemen va V. Rijmen yaratgan Rijndael algoritmi) va hozirgi kunda dunyoda eng keng qo'llaniladigan simmetrik blokli shifr [2]:

- blok uzunligi – 128 bit; kalit uzunligi – 128, 192 yoki 256 bit;
- raundlar soni mos ravishda 10, 12 yoki 14;
- har bir raund almashtirish (SubBytes), qatorlarni siljitish (ShiftRows), ustunlarni aralashtirish (MixColumns) va raund kalitini qo'shish (AddRoundKey) amallaridan iborat;
- qo'llanilishi: HTTPS, Wi-Fi (WPA2/WPA3), BitLocker, VeraCrypt, arxivlarni shifrlash (7-Zip).

Eski DES algoritmi (56 bitli kalit) bugungi kunda to'liq tanlash orqali ochilishi mumkin va qo'llanilmaydi.

4. Asimmetrik shifrlash. RSA algoritmi

Asimmetrik (ochiq kalitli) shifrlash g'oyasi 1976-yilda U. Diffi va M. Hellman tomonidan taklif etilgan. Har bir foydalanuvchi matematik bog'langan **juft kalitga** ega: **ochiq kalit** hammaga e'lon qilinadi, **yopiq kalit** faqat egasida saqlanadi. Ochiq kalit bilan shifrlangan xabarni faqat mos yopiq kalit bilan ochish mumkin.



3-rasm. Simmetrik va asimmetrik shifrlash sxemasi

RSA algoritmi (1977, R. Rivest, A. Shamir, L. Adleman) katta sonlarni tub ko‘paytuvchilarga ajratish murakkabligiga asoslangan:

1. Ikkita katta tub son p va q tanlanadi, $n = p \cdot q$ hisoblanadi.
2. $\varphi(n) = (p - 1)(q - 1)$ hisoblanadi.
3. $\varphi(n)$ bilan o‘zaro tub e tanlanadi (odatda $e = 65537$).
4. $d \cdot e \equiv 1 \pmod{\varphi(n)}$ shartini qanoatlantiruvchi d topiladi.
5. Ochiq kalit – (e, n) , yopiq kalit – (d, n) .
6. Shifrlash: $C = M^e \bmod n$; deshifrlash: $M = C^d \bmod n$.

O‘quv misoli (kichik sonlar bilan): $p = 5, q = 11 \rightarrow n = 55, \varphi(n) = 40; e = 3, d = 27$ (chunki $3 \cdot 27 = 81 = 2 \cdot 40 + 1$). $M = 7$ bo‘lsa: $C = 7^3 \bmod 55 = 343 \bmod 55 = 13$; tekshirish: $13^{27} \bmod 55 = 7$. Real tizimlarda n kamida 2048 bit (taxminan 617 xonali o‘nlik son) bo‘ladi.

Mezon	Simmetrik (AES)	Asimmetrik (RSA)
Kalitlar	Bitta umumiy maxfiy kalit	Juft kalit: ochiq va yopiq
Tezlik	Juda yuqori	Sekin (yuzlab-minglab marta)
Kalit tarqatish	Muammoli	Ochiq kalitni erkin tarqatish mumkin
Asosiy qo‘llanishi	Katta hajmdagi ma’lumotni shifrlash	Kalit almashish, ERI

Amalda **gibrid shifrlash** qo‘llaniladi: ma’lumot tez simmetrik algoritm (AES) bilan shifrlanadi, AES kaliti esa qabul qiluvchining ochiq kaliti bilan shifrlanib yuboriladi (yoki Diffi–Xellman protokoli bilan kelishiladi). HTTPS (TLS) protokoli aynan shunday ishlaydi.

5. Xesh-funksiyalar

Kriptografik xesh-funksiya – ixtiyoriy uzunlikdagi ma'lumotdan qat'iy uzunlikdagi qiymat (xesh, "raqamli barmoq izi") hisoblaydigan funksiya. Masalan, **SHA-256** har qanday fayl uchun 256 bitli (64 ta o'n oltilik belgidan iborat) qiymat beradi.

Xesh-funksiyaga qo'yiladigan talablar

- **bir tomonlamalik:** xesh qiymatdan dastlabki ma'lumotni tiklab bo'lmaydi;
- **kolliziyaga chidamlilik:** bir xil xeshga ega ikki xil ma'lumotni topish amalda mumkin emas;
- **ko'chki effekti:** ma'lumotdagi bitta belgining o'zgarishi xeshni butunlay o'zgartiradi.

Ko'chki effekti misoli (A6 dagi dastur natijasi):

```
SHA-256("Salom") = 441f71d48aacacdc18293201da2bfda40a421c4f93d8e509fcd2d0440b007b46  
SHA-256("salom") = 038f270ca678c66f5bf393f958e8eebcf98b049e5a0d32a69cabf46b576cabbf
```

Qo'llanilishi

- fayl yaxlitligini tekshirish (yuklab olingan dastur saytda e'lon qilingan xeshga mosligi);
- parollarni saqlash: tizim parolning o'zini emas, uning "tuzlangan" xeshini saqlaydi (bcrypt, Argon2 kabi maxsus sekin funksiyalar bilan);
- elektron raqamli imzo va blokcheyn.

MD5 va SHA-1 algoritmlarida kolliziyalar topilgan, shuning uchun ular xavfsizlik maqsadlarida tavsiya etilmaydi. Hozirgi standart – SHA-256 va SHA-3 oilasi.

Xeshlash shifrlash emas: shifrlangan ma'lumotni kalit bilan ochish mumkin, xeshdan esa dastlabki ma'lumotni tiklab bo'lmaydi.

6. Elektron raqamli imzo va ochiq kalitlar infratuzilmasi

Elektron raqamli imzo (ERI) – elektron hujjatning muallifini tasdiqlash, unga imzolangandan keyin o'zgartirish kiritilmaganini tekshirish va imzolovchi imzodan tona olmasligini (inkor etib bo'lmasslik) ta'minlash uchun mo'ljallangan rekvizit. O'zbekistonda ERI dan foydalanish 2022-yil 12-oktabrdagi O'RQ-793-sonli "Elektron raqamli imzo to'g'risida"gi Qonun bilan tartibga solinadi [11].

ERI ning ishlash tamoyili

1. **Imzolash:** hujjatning xeshi hisoblanadi va u imzolovchining **yopiq kaliti** bilan imzolanadi.
2. Hujjat imzo bilan birga yuboriladi.

3. **Tekshirish:** qabul qiluvchi hujjat xeshini qayta hisoblaydi va imzoni imzolovchining **ochiq kaliti** bilan tekshiradi. Xeshlar mos kelsa – imzo haqiqiy va hujjat o‘zgarmagan.

Shifrlashda **qabul qiluvchining ochiq** kaliti, imzlashda esa **jo‘natuvchining yopiq** kaliti ishlatiladi. Bu farqni o‘quvchilar ko‘pincha chalkashtiradi.

Ochiq kalit sertifikat – ochiq kalitning aniq shaxsga tegishli ekanligini tasdiqlovchi, ishonchli **ro‘yxatga olish (sertifikatlash) markazi** tomonidan imzolangan elektron hujjat (X.509 formati). Unda egasi, ochiq kalit, amal qilish muddati va markaz imzosi bo‘ladi. Sertifikatlar, markazlar va ularni boshqarish qoidalari majmui **ochiq kalitlar infratuzilmasi (PKI)** deyiladi. Veb-saytlarning HTTPS sertifikatlari ham PKI ning bir qismi.

O‘zbekistonda jismoniy va yuridik shaxslar uchun ERI kalitlari **E-IMZO** tizimi orqali beriladi va my.gov.uz, soliq, bojxona va boshqa davlat axborot tizimlarida qo‘llaniladi (L2).

Mavzu bo‘yicha xulosa

Kriptografiya konfidensiallik (shifrlash), yaxlitlik (xesh) va haqiqiylik hamda inkor etib bo‘lmazlikni (ERI) ta‘minlaydi. Klassik shifrlar oddiy va oson ochiladi; zamonaviy simmetrik AES tez, ammo kalit tarqatish muammosiga ega; asimmetrik RSA bu muammoni hal qiladi, lekin sekin – shuning uchun amalda gibrid sxema ishlatiladi. Xesh-funksiyalar bir tomonlama va kolliziyaga chidamli. ERI yopiq kalit bilan imzlash va ochiq kalit bilan tekshirishga asoslanadi, ochiq kalitlarning haqiqiylikini PKI ta‘minlaydi.

Nazorat savollari

1. Kriptografiya va kriptotahlilning farqi nimada?
2. Kerkgooffs tamoyilini tushuntiring.
3. Sesar shifri qanday ishlaydi va nima uchun ishonchsiz?
4. Vijnier shifrining Sesar shifridan afzalligi nimada?
5. Simmetrik shifrlashning asosiy muammosi qaysi?
6. AES algoritmining asosiy parametrlarini sanang.
7. RSA algoritmidan kalitlar qanday hosil qilinadi?
8. Gibrid shifrlash nima va u qayerda qo‘llaniladi?
9. Xesh-funksiyaga qanday talablar qo‘yiladi?
10. ERI qanday yaratiladi va tekshiriladi?

7-MAVZU. TARMOQ XAVFSIZLIGI: TARMOQLARARO EKRANLAR, VPN, HUJUMLARNI ANIQLASH TIZIMLARI

Reja:

1. Tarmoq xavfsizligiga tahdidlar.
2. Tarmoqlararo ekranlar (firewall).
3. Virtual xususiy tarmoqlar (VPN).
4. Hujumlarni aniqlash va oldini olish tizimlari (IDS/IPS).
5. Tarmoqni segmentlash va simsiz tarmoq xavfsizligi.

Tayanch iboralar:

tarmoq hujumi, trafikni tinglash (sniffing), “o‘rtadagi odam” (MitM), soxtalashtirish (spoofing), DoS, DDoS, port skanerlash, tarmoqlararo ekran, paketli filtr, holatni kuzatuvchi ekran, NGFW, DMZ, VPN, tunnel, TLS, IPsec, WireGuard, IDS, IPS, signatura, anomaliya, VLAN, WPA2, WPA3.

1. Tarmoq xavfsizligiga tahdidlar

Hujum	Mazmuni
Trafikni tinglash (sniffing)	Tarmoqdagi paketlarni ushlab, shifrlanmagan ma’lumotlarni (parollar, xabarlar) o‘qish – passiv hujum
“O‘rtadagi odam” (Man-in-the-Middle)	Hujumchi ikki tomon orasiga kirib, trafikni o‘qiydi yoki o‘zgartiradi (masalan, soxta ochiq Wi-Fi nuqtasi)
Soxtalashtirish (spoofing)	IP manzil, MAC manzil, DNS javobi yoki elektron pochta jo‘natuvchisini soxtalashtirish
DoS va DDoS	Xizmatni so‘rovlar bilan to‘ldirib, qonuniy foydalanuvchilar uchun ishlamaydigan qilish; DDoS da botnet ishlatiladi
Port skanerlash	Ochiq portlar va xizmatlarni aniqlash – odatda hujumning razvedka bosqichi
Parollarni tanlash	SSH, RDP kabi masofaviy kirish xizmatlariga lug‘at hujumi

Tarmoqni skanerlash va trafikni tahlil qilish faqat **o‘z** tarmog‘ingizda yoki egasining yozma ruxsati bilan amalga oshiriladi. Ruxsatsiz skanerlash qonunga xilof harakat sifatida baholanishi mumkin.

2. Tarmoqlararo ekranlar (firewall)

Tarmoqlararo ekran (firewall) – belgilangan qoidalar asosida tarmoq trafikini filtrlaydigan, ya’ni ruxsat etilgan ulanishlarni o‘tkazib, qolganlarini to‘sadigan dasturiy yoki apparat vosita. U ichki (ishonchli) tarmoq va tashqi (ishonchsiz) tarmoq – Internet orasida “chegara posti” vazifasini bajaradi [2].

Turi	Mazmuni
Paketli filtr	Har bir paketni manzil, port va protokol bo'yicha alohida tekshiradi
Holatni kuzatuvchi (stateful) ekran	Ulanish holatini eslab qoladi: faqat ichkaridan boshlangan ulanishlarga javob paketlarini o'tkazadi
Ilova darajasidagi ekran (proksi, WAF)	HTTP kabi protokollar mazmunini tahlil qiladi; WAF veb-ilovalarni himoya qiladi
Keyingi avlod ekran (NGFW)	Ilovalarni aniqlash, IPS, URL-filtr va zararli dasturlarni tekshirishni birlashtiradi
Shaxsiy (xost) ekran	Alohida kompyuterda ishlaydi – Windows Defender Firewall, Linux'da ufw

Qoidalar namunasi (maktab tarmog'i uchun)

№	Manba	Manzil	Port/xizmat	Harakat
1	Ichki tarmoq	Internet	80, 443 (HTTP/HTTPS)	Ruxsat
2	Ichki tarmoq	Internet	53 (DNS)	Ruxsat
3	Internet	Maktab veb-serveri (DMZ)	443	Ruxsat
4	Internet	Ichki tarmoq	Har qanday	Taqiqlash
5	Har qanday	Har qanday	Har qanday	Taqiqlash (standart qoida)

Qoidalar yuqoridan pastga tekshiriladi; oxirgi “hammasini taqiqlash” qoidasi **standart bo'yicha rad etish** tamoyilini ifodalaydi. **DMZ (demilitarizatsiya zonasi)** – Internetdan ochiq bo'lishi kerak bo'lgan serverlar (vab-sayt) joylashtiriladigan, ichki tarmoqdan ajratilgan segment.

3. Virtual xususiy tarmoqlar (VPN)

VPN (Virtual Private Network) – ochiq tarmoq (Internet) orqali ikki nuqta yoki tarmoq o'rtasida shifrlangan “tunnel” hosil qilib, xavfsiz aloqani ta'minlovchi texnologiya. Asosiy protokollar: IPsec, TLS asosidagi VPN (OpenVPN), WireGuard.

- **tashkilot VPN i:** xodim uydan institut yoki maktab ichki tizimlariga xavfsiz ulanadi;
- **tarmoqlar orasidagi VPN:** ikki filialning tarmoqlari Internet orqali birlashtiriladi;
- **tijoriy VPN xizmatlari:** ochiq Wi-Fi da trafikni shifrlash; ammo bunda trafik VPN provayderiga ishonib topshiriladi, shuning uchun noma'lum “bepul VPN” ilovalari ma'lumotlarni yig'ishi mumkin.

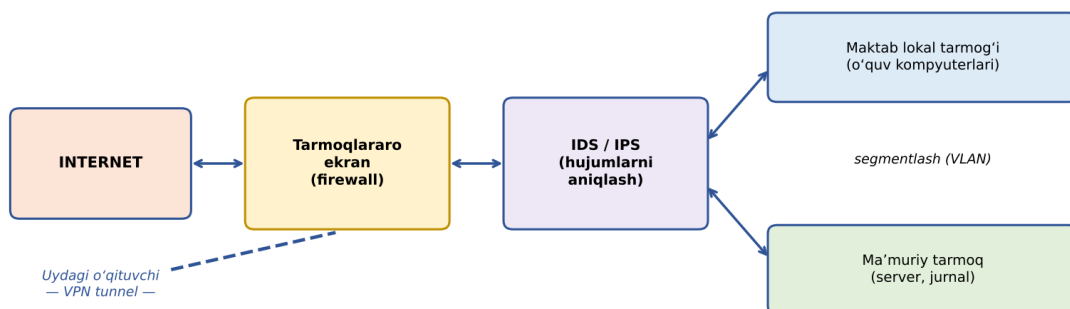
VPN anonimlik yoki zararli dasturlardan himoya kafolati emas. U faqat foydalanuvchi va VPN serveri orasidagi trafikni shifrlaydi.

4. Hujumlarni aniqlash va oldini olish tizimlari (IDS/IPS)

IDS (Intrusion Detection System) – tarmoq yoki xost faoliyatini kuzatib, shubhali harakatlar haqida **ogohlantiradigan** tizim. **IPS (Intrusion Prevention System)** – hujumni aniqlab, uni **avtomatik to‘shib qo‘yadigan** tizim.

Aniqlash usuli	Mazmuni
Signaturaga asoslangan	Ma’lum hujumlar namunalarini bilan solishtirish; aniq, lekin yangi hujumlarni topmaydi
Anomaliyaga asoslangan	Normal xulq-atvor modelidan chetlanishni aniqlash; yangi hujumlarni topishi mumkin, lekin yolg‘on signallar ko‘p

Ochiq kodli IDS/IPS ga Snort va Suricata misol bo‘ladi. Katta tashkilotlarda turli manbalardan kelgan jurnallar **SIEM** (xavfsizlik hodisalarini boshqarish) tizimida yig‘ilib tahlil qilinadi.



4-rasm. Maktab tarmog‘ini himoya qilish sxemasi

5. Tarmoqni segmentlash va simsiz tarmoq xavfsizligi

Segmentlash – tarmoqni mantiqiy qismlarga (VLAN) ajratish. Maktab tarmog‘i uchun namunaviy segmentlar: ma’muriyat (buxgalteriya, kadrlar) – o‘qituvchilar – kompyuter sinfi – mehmon Wi-Fi – kuzatuv kameralari. Segmentlar orasidagi trafik ekran qoidalari bilan cheklanadi: o‘quvchi kompyuteri buxgalteriya kompyuteriga ulana olmaydi, zararli dastur esa butun tarmoqqa tarqalmaydi.

Simsiz tarmoq (Wi-Fi) xavfsizligi

- **WPA3** (imkoniyat bo‘lmasa – WPA2-AES) shifrlash rejimidan foydalanish; WEP va WPA (TKIP) eskirgan;
- routerning standart administrator parolini o‘zgartirish va dasturiy ta’minotini yangilash;
- WPS funksiyasini o‘chirib qo‘yish;
- mehmonlar va o‘quvchilar uchun alohida Wi-Fi tarmog‘i;
- ochiq jamoat Wi-Fi tarmoqlarida faqat HTTPS saytlardan foydalanish, muhim operatsiyalarni mobil Internet yoki VPN orqali bajarish.

Mavzu bo'yicha xulosa

Tarmoq tinglash, MitM, soxtalashtirish va DoS hujumlariga duch keladi. Tarmoqlararo ekran trafikni qoidalar asosida filtrlaydi, VPN ochiq tarmoq orqali shifrlangan tunnel hosil qiladi, IDS/IPS esa hujumlarni aniqlaydi va to'sadi. Segmentlash va to'g'ri sozlangan Wi-Fi zararining tarqalishini cheklaydi. Bu vositalar birgalikda ko'p qatlamli himoyani tashkil etadi.

Nazorat savollari

1. Tarmoqqa qanday asosiy hujum turlari bor?
2. "O'rtadagi odam" hujumi qanday amalga oshiriladi?
3. DoS va DDoS ning farqi nimada?
4. Tarmoqlararo ekranning qanday turlari bor?
5. "Standart bo'yicha rad etish" tamoyilini tushuntiring.
6. DMZ nima uchun kerak?
7. VPN qanday vazifani bajaradi va uning cheklovlari qanday?
8. IDS va IPS ning farqi nimada?
9. Tarmoqni segmentlash qanday afzallik beradi?
10. Wi-Fi tarmog'ini xavfsiz sozlash qoidalarini sanang.

Adabiyotlar: [2], [3]

8-MAVZU. VEB-XAVFSIZLIK: OWASP TOP-10 ZAIFLIK LARI (SQL INJECTION, XSS) VA HIMOYALANISH USULLARI

Reja:

1. Veb-ilova arxitekturasini va HTTPS.
2. OWASP loyihasi va OWASP Top 10:2025 ro'yxati.
3. Injeksiya zaifliklari. SQL injection.
4. Saytlararo skripting (XSS).
5. Xavfsiz veb-dasturlash tamoyillari.

Tayanch iboralar:

vab-ilova, mijoz, server, HTTP, HTTPS, TLS, cookie, sessiya, OWASP, Top-10, kirishni boshqarishning buzilishi, noto'g'ri sozlash, yetkazib berish zanjiri, injeksiya, SQL injection, parametrlangan so'rov, XSS, kiritishni tekshirish, chiqishni ekranlash, CSP, xavfsiz dasturlash.

1. Veb-ilova arxitekturasini va HTTPS

Veb-ilova uch qismdan iborat: **mijoz** (brauzer – HTML, CSS, JavaScript), **server** (PHP, Python, Node.js dasturi) va **ma'lumotlar bazasi** (MySQL, PostgreSQL). Brauzer va server HTTP protokoli orqali so'rov-javob almashadi.

Foydalanuvchi tizimga kirgach, server unga **sessiya identifikatorini** beradi va u brauzerda **cookie** sifatida saqlanadi.

HTTPS – TLS protokoli yordamida shifrlangan HTTP. U trafikni tinglash va o‘zgartirishdan himoya qiladi va server sertifikatini orqali saytning domenini tasdiqlaydi. L3 laboratoriya ishida HTTP va HTTPS trafigi Wireshark yordamida taqqoslanadi.

2. OWASP loyihasi va OWASP Top 10:2025 ro‘yxati

OWASP (Open Worldwide Application Security Project) – veb-ilovalar xavfsizligini oshirishga qaratilgan xalqaro notijorat hamjamiyat. Uning eng mashhur hujjati – **OWASP Top 10**, veb-ilovalardagi eng muhim xavf toifalari ro‘yxati; u bir necha yilda bir marta real ma’lumotlar va mutaxassislar so‘rovi asosida yangilanadi. Eng so‘nggi tahriri – **OWASP Top 10:2025** [8].

Kod	Toifa	Qisqa mazmuni va himoya
A01	Kirishni boshqarishning buzilishi (Broken Access Control)	Foydalanuvchi ruxsat etilmagan ma’lumot yoki funksiyaga kira oladi (URL dagi id ni o‘zgartirib boshqa o‘quvchi bahosini ko‘rish). Himoya: har bir so‘rovda serverda huquqni tekshirish
A02	Xavfsizlik sozlamalaridagi xatolar (Security Misconfiguration)	Standart parollar, keraksiz xizmatlar, batafsil xato xabarlar. Himoya: xavfsiz sozlash andozalari
A03	Dasturiy ta’minot yetkazib berish zanjiridagi nosozliklar (Software Supply Chain Failures)	Zaif yoki zararlangan kutubxonalar va paketlar. Himoya: bog‘liqliklar ro‘yxati, yangilash, ishonchli manbalar
A04	Kriptografik nosozliklar (Cryptographic Failures)	Ma’lumotlarni shifrlamaslik, eskirgan algoritmlar, parollarni ochiq saqlash. Himoya: HTTPS, zamonaviy algoritmlar
A05	Injeksiya (Injection)	Foydalanuvchi kiritgan ma’lumot buyruq sifatida bajariladi (SQL, OS buyruqlari, XSS). Himoya: parametrlangan so‘rovlar, ekranlash
A06	Xavfsiz bo‘lmagan loyihalash (Insecure Design)	Loyihalash bosqichidagi mantiqiy xatolar. Himoya: tahdid modeli, xavfsiz loyihalash andozalari
A07	Autentifikatsiyadagi nosozliklar (Authentication Failures)	Kuchsiz parollar, tanlashdan himoya yo‘qligi, 2FA yo‘qligi. Himoya: 5-mavzudagi choralar
A08	Dasturiy ta’minot yoki ma’lumotlar yaxlitligidagi nosozliklar (Software or Data Integrity Failures)	Yangilanishlar va ma’lumotlarning yaxlitligi tekshirilmasligi. Himoya: imzolar, xeshlar
A09	Xavfsizlik jurnallari va ogohlantirishdagi nosozliklar (Security Logging & Alerting Failures)	Hujumlar qayd etilmaydi va aniqlanmaydi. Himoya: jurnallar, monitoring

Kod	Toifa	Qisqa mazmuni va himoya
A10	Istisno holatlarni noto'g'ri qayta ishlash (Mishandling of Exceptional Conditions)	Xatolar va kutilmagan holatlarda tizim xavfsiz bo'lmagan holatga o'tadi yoki ortiqcha ma'lumot beradi. Himoya: "xavfsiz holatda to'xtash", xatolarni to'g'ri qayta ishlash

Izoh: 2021-yilgi tahrirdagi "Server tomonidan so'rovlarni soxtalashtirish (SSRF)" toifasi 2025-yilda A01 tarkibiga qo'shilgan, "Zaif va eskirgan komponentlar" toifasi esa kengaytirilib A03 "Yetkazib berish zanjiri" toifasiga aylangan.

3. Injeksiya zaifliklari. SQL injection

SQL injection – foydalanuvchi kiritgan ma'lumot tekshirilmasdan SQL so'roviga **matn sifatida qo'shilganda** yuzaga keladigan zaiflik: hujumchi maxsus belgilar kiritib, so'rov mantiqini o'zgartiradi va ma'lumotlar bazasidagi axborotni o'qishi yoki o'zgartirishi mumkin. Quyidagi misol zaiflik **sababini** tushuntirish uchun keltirilgan:

```
# XAVFLI: foydalanuvchi kiritgan matn so'rovga bevosita qo'shilmoqda
sorov = "SELECT * FROM users WHERE login = '" + login + "'"
cur.execute(sorov)
```

Bu yerda **login** o'zgaruvchisidagi tirnoq (') belgisi so'rov tuzilishini buzadi va qo'shimcha shartlar SQL kodi sifatida bajarilishi mumkin. **To'g'ri yechim** – **parametrlangan so'rov** (prepared statement): ma'lumot va kod alohida uzatiladi, ma'lumotlar bazasi kiritilgan qiymatni hech qachon buyruq sifatida talqin qilmaydi.

```
# XAVFSIZ: parametrlangan so'rov
cur.execute("SELECT * FROM users WHERE login = ?", (login,))
```

SQL injection dan himoya choralari

- faqat parametrlangan so'rovlar yoki ORM vositalaridan foydalanish;
- kiritilgan ma'lumotni turi, uzunligi va formati bo'yicha tekshirish ("oq ro'yxat");
- ma'lumotlar bazasi foydalanuvchisiga minimal huquqlar berish;
- foydalanuvchiga batafsil SQL xato xabarlarini ko'rsatmaslik.

4. Saytlararo skripting (XSS)

XSS (Cross-Site Scripting) – hujumchi veb-sahifaga zararli JavaScript kodini joylashtirib, u boshqa foydalanuvchilar brauzerida bajarilishiga erishadigan zaiflik. Natijada sessiya cookie lari o'g'irlanishi, sahifa mazmuni o'zgartirilishi yoki foydalanuvchi soxta sahifaga yo'naltirilishi mumkin. OWASP Top 10:2025 da XSS injeksiya toifasiga (A05) kiritilgan.

XSS turi	Mazmuni
Saqlanadigan (stored)	Zararli kod serverda saqlanadi (forum xabari, izoh) va sahifani ochgan har bir foydalanuvchida bajariladi
Aks ettiriladigan (reflected)	Kod havola parametrda bo'ladi va server javobida qaytariladi; qurbon maxsus havolani bosishi kerak
DOM asosidagi	Zaiflik sahifadagi JavaScript kodida, ma'lumot server ishtirokisiz DOM ga qo'shiladi

XSS dan himoya choralari

- **chiqishni ekranlash (output encoding):** foydalanuvchi ma'lumoti HTML ga qo'shilishdan oldin `<`, `>`, `"`, `&` kabi belgilar mos HTML ob'ektlariga (`<`, `>`, ...) aylantiriladi;
- JavaScript da `innerHTML` o'rniga `textContent` dan foydalanish;
- zamonaviy shablon tizimlari va freymvorklarning avtomatik ekranlash imkoniyatlari;
- **Content Security Policy (CSP)** sarlavhasi bilan sahifada bajariladigan skriptlar manbalarini cheklash;
- sessiya cookie lari uchun `HttpOnly`, `Secure` va `SameSite` atributlari.

```
// XAVFLI: foydalanuvchi matni HTML sifatida talqin qilinadi
izoh.innerHTML = matn;
// XAVFSIZ: matn oddiy matn sifatida ko'rsatiladi
izoh.textContent = matn;
```

5. Xavfsiz veb-dasturlash tamoyillari

- **foydalanuvchi kiritgan har qanday ma'lumotga ishonmaslik** – serverda tekshirish (brauzerdagi tekshiruv osonlik bilan chetlab o'tiladi);
- kam huquqlar va standart bo'yicha rad etish tamoyillari;
- parollarni maxsus funksiyalar (bcrypt, Argon2) bilan xeshlab saqlash;
- barcha sahifalar uchun HTTPS;
- bog'liqliklar va freymvorklarni muntazam yangilash;
- xatolar haqida foydalanuvchiga umumiy xabar, batafsil ma'lumotni esa faqat jurnalga yozish;
- xavfsizlikni muntazam sinash – faqat o'z ilovangizda yoki ruxsat etilgan o'quv muhitida (OWASP Juice Shop, A9).

Mavzu bo'yicha xulosa

Veb-ilovalar mijoz, server va ma'lumotlar bazasidan iborat bo'lib, ularning xavfsizligi OWASP Top 10 ro'yxati asosida baholanadi. 2025-yilgi tahrirda birinchi o'rinda kirishni boshqarishning buzilishi turadi, yetkazib berish zanjiri va istisno holatlarni qayta ishlash yangi toifalar sifatida kiritilgan. SQL injection va XSS –

injeksiya toifasidagi klassik zaifliklar bo'lib, ulardan parametrlangan so'rovlar, kiritishni tekshirish, chiqishni ekranlash va CSP orqali himoyalaniadi.

Nazorat savollari

1. Veb-ilova qanday qismlardan iborat?
2. HTTPS qanday himoyani ta'minlaydi?
3. OWASP nima va Top 10 ro'yxati qanday tuziladi?
4. OWASP Top 10:2025 ning birinchi uchta toifasini tushuntiring.
5. Kirishni boshqarishning buzilishiga maktab elektron tizimidan misol keltiring.
6. SQL injection zaifligi qanday yuzaga keladi?
7. Parametrlangan so'rov SQL injection dan qanday himoya qiladi?
8. XSS ning qanday turlari bor?
9. Chiqishni ekranlash nima?
10. Xavfsiz veb-dasturlashning asosiy tamoyillarini sanang.

Adabiyotlar: [8], [13]

9-MAVZU. AXBOROT TIZIMLARI XAVFSIZLIGINI BOSHQARISH: XAVFLARNI BAHOLASH, ZAXIRA NUSXALASH, INSIDENTLARGA JAVOB BERISH

Reja:

1. Axborot xavfsizligini boshqarish tizimi.
2. Xavflarni baholash.
3. Xavfni boshqarish strategiyalari.
4. Zaxira nusxalash va ma'lumotlarni tiklash.
5. Insidentlarga javob berish.

Tayanch iboralar:

AXBT, PDCA sikli, aktivlar reyestri, xavflarni baholash, sifatli va miqdoriy baholash, xavf matritsasi, qoldiq xavf, xavfni kamaytirish, o'tkazish, qabul qilish, rad etish, zaxira nusxa, to'liq, ortib boruvchi, differensial nusxa, 3-2-1 qoidasi, RPO, RTO, insident, CSIRT, uzluksizlik rejasi.

1. Axborot xavfsizligini boshqarish tizimi

Axborot xavfsizligini boshqarish tizimi (AXBT) – tashkilotda axborot xavfsizligini rejalashtirish, joriy etish, nazorat qilish va takomillashtirishga qaratilgan siyosat, jarayonlar va choralar majmui (ISO/IEC 27001). AXBT uzluksiz takomillashtirish sikli – **PDCA (Plan – Do – Check – Act)** asosida ishlaydi [4]:

Bosqich	Mazmuni
Plan (Rejalashtirish)	Aktivlarni aniqlash, xavflarni baholash, siyosat va choralarni tanlash
Do (Bajarish)	Choralarni joriy etish, xodimlarni o‘qitish
Check (Tekshirish)	Monitoring, ichki audit, insidentlar tahlili
Act (Takomillashtirish)	Kamchiliklarni tuzatish, siyosatni yangilash

2. Xavflarni baholash

Xavflarni baholash quyidagi bosqichlardan iborat:

1. **Aktivlarni aniqlash** – aktivlar reyestrini tuzish va ularning qadrini (konfidensiallik, yaxlitlik, foydalanuvchanlik bo‘yicha) baholash.
2. **Tahdidlar va zaifliklarni aniqlash** – har bir aktiv uchun.
3. **Ehtimollik va ta’sirni baholash** – sifatli (past/o‘rta/yuqori) yoki miqdoriy (pul ko‘rinishida) usulda.
4. **Xavf darajasini hisoblash** va ustuvorlik bo‘yicha saralash.
5. **Choralarni tanlash** va qoldiq xavfni baholash.

Sifatli baholashda ehtimollik va ta’sir 1–3 (yoki 1–5) ballik shkalada baholanadi va xavf matritsasi tuziladi:

Ehtimollik	Yuqori	Yuqori	Kritik	Kritik
	O‘rtacha	O‘rta	Yuqori	Kritik
	Kam	Past	O‘rta	Yuqori
		Kichik	O‘rta	Katta
		Zarar hajmi (ta’sir)		

5-rasm. Xavf matritsasi (ehtimollik × ta’sir)

Maktab uchun xavflarni baholash namunasi

Aktiv	Tahdid / zaiflik	Ehtimol.	Ta'sir	Xavf	Chora
Elektron jurnal akkauntlari	Parolni fishing orqali o'g'irlash / 2FA yo'q	3	3	9 – yuqori	2FA, o'qitish
Kompyuter sinfi	Zararli dastur / USB disklar, admin huquqi	3	2	6 – yuqori	Cheklangan hisoblar, antivirus
O'quvchilar ma'lumotlari bazasi	Sizib chiqish / ochiq ulashilgan jadval	2	3	6 – yuqori	Kirish huquqlari, audit
Ma'muriyat kompyuteri	To'lov talab qiluvchi dastur / zaxira yo'q	2	3	6 – yuqori	3-2-1 zaxira
Maktab veb-sayti	Sozlashdagi xatolar / yangilanmagan CMS	2	2	4 – o'rta	Yangilash, kuchli parollar
Server xonasi	Elektr uzilishi / UPS yo'q	2	2	4 – o'rta	UPS o'rnatish

Miqdoriy baholashda yillik kutilayotgan zarar hisoblanadi: $ALE = SLE \times ARO$, bu yerda SLE – bitta hodisadan zarar, ARO – hodisaning yillik takrorlanish soni. Masalan, bir hodisadan zarar 5 mln so'm, hodisa 2 yilda bir marta ($ARO = 0,5$) bo'lsa, $ALE = 2,5$ mln so'm; himoya chorasining yillik narxi bundan kam bo'lsa, u iqtisodiy jihatdan asoslangan.

3. Xavfni boshqarish strategiyalari

Strategiya	Mazmuni	Misol
Kamaytirish	Himoya choralari bilan ehtimollik yoki ta'sirni pasaytirish	2FA joriy etish
O'tkazish	Xavfni boshqa tomonga o'tkazish	Sug'urta, bulutli xizmat provayderi
Qabul qilish	Xavf past bo'lsa yoki chora qimmat bo'lsa, ongli ravishda qabul qilish	Eski proyektor o'g'irlanishi xavfi
Rad etish (oldini olish)	Xavf manbai bo'lgan faoliyatdan voz kechish	Shaxsiy ma'lumotlarni ochiq messenjer guruhida saqlashdan voz kechish

Choralar ko'rilgandan keyin qolgan xavf **qoldiq xavf** deyiladi; u rahbariyat tomonidan qabul qilinadi.

4. Zaxira nusxalash va ma'lumotlarni tiklash

Zaxira nusxalash (backup) – ma'lumotlar yo'qolganda yoki buzilganda ularni tiklash uchun nusxalarini muntazam yaratish. Bu to'lov talab qiluvchi dasturlar, apparat nosozligi va inson xatosidan himoyaning asosiy usuli.

Nusxa turi	Mazmuni	Tiklash
To'liq	Barcha tanlangan ma'lumotlar nusxalanadi	Eng tez, lekin ko'p joy va vaqt talab qiladi
Ortib boruvchi (incremental)	Oxirgi har qanday nusxadan keyin o'zgarganlar	Nusxalash tez; tiklash uchun to'liq + barcha ortib boruvchi nusxalar kerak
Differensial	Oxirgi to'liq nusxadan keyin o'zgarganlar	To'liq + oxirgi differensial nusxa yetarli

3-2-1 qoidasi: ma'lumotlarning kamida 3 ta nusxasi bo'lishi, ular 2 xil turdagi tashuvchida saqlanishi va kamida 1 tasi boshqa joyda (bulutda yoki boshqa binoda) saqlanishi kerak. Zamonaviy talqinda yana bitta nusxa **oflayn yoki o'zgartirib bo'lmaydigan** (immutable) bo'lishi tavsiya etiladi (3-2-1-1-0: oxirgi "0" – tiklash sinovida xatolar yo'qligi).

- **RPO (Recovery Point Objective)** – qancha vaqtlik ma'lumot yo'qolishiga yo'l qo'yish mumkin (nusxalash davriyligini belgilaydi);
- **RTO (Recovery Time Objective)** – tizimni qancha vaqt ichida tiklash kerak.

Tiklab ko'rilmagan zaxira nusxa – ishonchli zaxira emas. Nusxalardan tiklash muntazam sinab turilishi kerak (L4).

5. Insidentlarga javob berish

Axborot xavfsizligi insidenti – axborot xavfsizligini buzgan yoki buzishi mumkin bo'lgan hodisa (akkaunt buzilishi, zararli dastur, ma'lumot sizib chiqishi, qurilma yo'qolishi). NIST va ISO yondashuvlariga ko'ra insidentga javob quyidagi bosqichlardan iborat [10]:

Bosqich	Maktab misolidagi harakatlar
Tayyorgarlik	Mas'ul shaxs, aloqa ro'yxati, yo'riqnoma, zaxira nusxalar, o'qitish
Aniqlash va tahlil	Belgilarni qayd etish (ekrandagi to'lov talabi, shubhali kirishlar), ko'lamini aniqlash
Cheklash	Zararlangan kompyuterni tarmoqdan uzish, buzilgan akkaunt parolini almashtirish
Bartaraf etish	Zararli dasturni yo'q qilish yoki tizimni qayta o'rnatish, zaiflikni yopish
Tiklash	Ma'lumotlarni zaxira nusxadan tiklash, ishni nazorat ostida qayta boshlash
Xulosa (saboqlar)	Sababni tahlil qilish, siyosat va choralarni yangilash, hisobot

Davlat darajasida kiberinsidentlarga javob berish uchun maxsus markazlar (CSIRT/CERT) faoliyat yuritadi. O'zbekistonda bu vazifani "Kiberxavfsizlik

markazi” bajaradi; “Kiberxavfsizlik to‘g‘risida”gi Qonunga muvofiq kiberinsidentlar haqida vakolatli organga xabar berilishi lozim.

Mavzu bo‘yicha xulosa

Xavfsizlikni boshqarish PDCA sikliga asoslangan AXBT orqali amalga oshiriladi. Xavflar aktivlar, tahdidlar va zaifliklar asosida ehtimollik va ta’sir bo‘yicha baholanadi va kamaytirish, o‘tkazish, qabul qilish yoki rad etish strategiyalari bilan boshqariladi. 3-2-1 qoidasi asosidagi va muntazam tekshiriladigan zaxira nusxalar foydalanuvchanlikning kafolatidir. Insidentlarga javob tayyorgarlik, aniqlash, cheklash, bartaraf etish, tiklash va xulosa bosqichlaridan iborat.

Nazorat savollari

1. AXBT nima va u qaysi standartga asoslanadi?
2. PDCA siklining bosqichlarini tushuntiring.
3. Xavflarni baholash qanday bosqichlardan iborat?
4. Xavf matritsasi qanday tuziladi?
5. ALE qanday hisoblanadi?
6. Xavfni boshqarishning to‘rt strategiyasini misollar bilan tushuntiring.
7. To‘liq, ortib boruvchi va differensial nusxalarning farqi nimada?
8. 3-2-1 qoidasini tushuntiring.
9. RPO va RTO nima?
10. Insidentga javob berish bosqichlarini sanang.

Adabiyotlar: [4], [10]

10-MAVZU. TA’LIM MUASSASASIDA AXBOROT XAVFSIZLIGI VA O‘QUVCHILARNING RAQAMLI XAVFSIZLIGI. KIBERXAVFSIZLIK MADANIYATINI SHAKLLANTIRISH

Reja:

1. Ta’lim muassasasining axborot aktivlari va xavflari.
2. O‘quvchilar va xodimlarning shaxsga doir ma’lumotlarini himoya qilish.
3. O‘quvchilarning raqamli xavfsizligi: asosiy xavflar.
4. Raqamli xavfsizlikni o‘qitish: mazmun va metodika.
5. Kiberxavfsizlik madaniyatini shakllantirish.

Tayanch iboralar:

ta’lim muassasasi aktivlari, AT mas’uli, qabul qilinadigan foydalanish qoidalari, raqamli iz, kiberbulling, onlayn tanishuvlar xavfi, maxfiylik sozlamalari, raqamli savodxonlik, raqamli fuqarolik, kiber-gigiyena, kiberxavfsizlik madaniyati, ota-onalar nazorati.

1. Ta'lim muassasasining axborot aktivlari va xavflari

Zamonaviy maktabda ko'plab axborot aktivlari mavjud: elektron jurnal va kundalik tizimi akkauntlari, o'quvchilar va ota-onalar ma'lumotlari, kadrlar va buxgalteriya hujjatlari, kompyuter sinfi, maktab veb-sayti va ijtimoiy tarmoq sahifalari, kuzatuv kameralari, nazorat ishlari materiallari. Ularga xos xavflar:

- ko'p foydalanuvchili kompyuterlar va umumiy parollar (“bitta parol butun sinfga”);
- o'qituvchilarning shaxsiy qurilmalaridan foydalanish;
- o'quvchilar ma'lumotlari bo'lgan jadvallarning ochiq havola orqali ulashilishi;
- messenger guruhlarida shaxsiy ma'lumotlarni tarqatish;
- yangilanmagan va litsenziyasiz dasturlar;
- AT bo'yicha mutaxassis yo'qligi – vazifa ko'pincha informatika o'qituvchisiga yuklanadi.

Shuning uchun informatika o'qituvchisi ham texnik choralarni (A8), ham tashkiliy choralarni (A10 – xavfsizlik siyosati) amalga oshira olishi kerak.

2. O'quvchilar va xodimlarning shaxsga doir ma'lumotlarini himoya qilish

“Shaxsga doir ma'lumotlar to'g'risida”gi Qonunga muvofiq (2-mavzu) maktab o'quvchilar va xodimlar ma'lumotlarining mulkdori va operatori hisoblanadi. Amaliy qoidalar:

- faqat zarur ma'lumotlarni yig'ish; tadbir suratlari va videolarini e'lon qilish uchun ota-ona roziligini olish;
- jadvallar va hujjatlarni faqat aniq shaxslarga ulashish (“havolasi bor har kim” rejimidan qochish);
- o'quvchilar ro'yxatlarini ochiq messenger guruhlarida tarqatmaslik;
- shaxsiy ma'lumotlar bor fayllarni shifrlangan tashuvchilarda saqlash (L1);
- xodim ishdan ketganda uning akkauntlarini o'chirish yoki bloklash;
- eski qurilmalarni utilizatsiya qilishdan oldin ma'lumotlarni ishonchli o'chirish.

3. O'quvchilarning raqamli xavfsizligi: asosiy xavflar

Xavf	Mazmuni
Akkauntlar buzilishi	Kuchsiz va takrorlanuvchi parollar, SMS-kodni “do'stga” aytish, fishing
Firibgarlik	“Bepul o'yin valyutasi”, soxta sovrinli o'yinlar, karta ma'lumotlarini so'rash
Zararli ilovalar	Norasmiy manbalardan .apk fayllar, “cheat”lar

Xavf	Mazmuni
Shaxsiy ma'lumotlarning oshkor bo'lishi va raqamli iz	Manzil, maktab, kun tartibi, geolokatsiyali suratlar; Internetga joylangan narsa abadiy saqlanib qolishi mumkin
Kiberbulling	Internetda tahqirlash, masxara qilish, shaxsiy surat va yozishmalarni tarqatish
Xavfli onlayn tanishuvlar	Notanish kishilar o'zini tengdosh qilib ko'rsatib ishonchga kirishi, shaxsiy ma'lumot yoki suratlar so'rashi
Noto'g'ri axborot	Soxta xabarlar, manipulyatsiya, SI yaratgan soxta tasvir va videolar (dipfeyk)

O'quvchi tashvishli vaziyatga (kiberbulling, tahdid, shubhali notanish odam) duch kelsa, uni ayblamasdan tinglash, dalillarni saqlash (screenshot), sinf rahbari, maktab psixologi va ota-onalarga xabar berish, zarur hollarda vakolatli organlarga murojaat qilish lozim. O'quvchiga "kattalarga aytish – xiyonat emas" ekanini tushuntirish muhim.

4. Raqamli xavfsizlikni o'qitish: mazmun va metodika

Raqamli xavfsizlik informatika darslarida (masalan, "Kompyuter tarmoqlari va Internet", "Axborot xavfsizligi" mavzulari), sinf soatlarida va maxsus tadbirlarda o'qitiladi. Yoshga mos mazmun:

Sinflar	Asosiy mazmun
1–4	Shaxsiy ma'lumot nima; notanishlarga ma'lumot bermaslik; noqulay vaziyatda kattalarga aytish; parolni sir saqlash
5–7	Kuchli parol va parol iborasi; fishing va firibgarlik belgilari; ilovalarni rasmiy do'kondan o'rnatish; maxfiylik sozlamalari; kiberbulling va unga qarshi turish
8–9	2FA; raqamli iz va obro'; axborotni tanqidiy baholash, dipfeyklar; shifrlash va HTTPS asoslari; qonuniy javobgarlik
10–11	Kriptografiya asoslari; xavfsizlik siyosati; kiberxavfsizlik kasblari; axloqiy xakerlik va qonun chegaralari; CTF musobaqalari

Metodik tavsiyalar

- qo'rqitish o'rniga **amaliy ko'nikma** berish: "nima qilish kerak" degan aniq harakatlar;
- real (anonimlashtirilgan) keyslar, rolly o'yinlar, fishing xatlarini "topish" o'yinlari (A3);
- "Unplugged" mashg'ulotlar: qog'ozda Sezar shifri, parol kuchliligini taqqoslash;
- o'quvchilar o'zlari ota-onalar uchun eslatma tayyorlashi (6-mustaqil topshiriq) – "o'qitish orqali o'rganish";
- xalqaro bepul resurslardan foydalanish: Harvard CS50 Cybersecurity kursi [12], CISA tavsiyalari [9], CTF o'quv musobaqalari.

5. Kiberxavfsizlik madaniyatini shakllantirish

Kiberxavfsizlik madaniyati – tashkilot a'zolarining xavfsizlikka oid qadriyatlari, bilimlari va kundalik xatti-harakatlari majmui. Madaniyat texnik choralardan kam emas: hatto eng yaxshi texnik himoya ham bitta e'tiborsiz foydalanuvchi tufayli yengib o'tilishi mumkin.

Maktabda madaniyatni shakllantirish yo'llari

- rahbariyatning shaxsiy namunasi (direktorning o'zi 2FA dan foydalanishi);
- barcha xodimlar uchun yiliga kamida bir marta qisqa trening;
- kompyuter sinfida va o'qituvchilar xonasida “kiber-gigiyena” eslatmalari;
- “Xavfsiz Internet kuni” (har yili fevral oyida o'tkaziladigan xalqaro tadbir) va oktabr – kiberxavfsizlik xabardorligi oyi doirasida tadbirlar;
- xatoga yo'l qo'ygan xodim yoki o'quvchini ayblamasdan, tez xabar berishni rag'batlantirish;
- ota-onalar bilan hamkorlik: ota-onalar yig'ilishlarida qisqa chiqishlar, eslatmalar.

Mavzu bo'yicha xulosa

Ta'lim muassasasi ko'plab qimmatli axborot aktivlariga ega va ularni himoya qilishda informatika o'qituvchisining roli katta. O'quvchilar va xodimlarning shaxsga doir ma'lumotlari qonun talablariga muvofiq himoya qilinishi shart. O'quvchilarga akkauntlar xavfsizligi, firibgarlik, raqamli iz, kiberbulling va xavfli tanishuvlar bo'yicha yoshga mos, amaliy yo'naltirilgan ta'lim beriladi. Kiberxavfsizlik madaniyati rahbariyat namunasi, muntazam o'qitish va ayblamaslik muhiti orqali shakllanadi.

Nazorat savollari

1. Maktabning asosiy axborot aktivlarini sanang.
2. Ta'lim muassasasiga xos xavfsizlik xavflari qaysilar?
3. Maktab o'quvchilar ma'lumotlarini himoya qilish uchun qanday qoidalarga amal qiladi?
4. Raqamli iz nima va u nima uchun muhim?
5. Kiberbulling holatida o'qituvchi qanday harakat qilishi kerak?
6. 5–7-sinflar uchun raqamli xavfsizlik mazmunini tavsiflang.
7. Raqamli xavfsizlikni o'qitishda qanday metodlar samarali?
8. Kiberxavfsizlik madaniyati nima?
9. Maktabda kiberxavfsizlik madaniyatini shakllantirish yo'llarini sanang.
10. Ota-onalar bilan raqamli xavfsizlik bo'yicha hamkorlik qanday tashkil etiladi?

Adabiyotlar: [6], [9], [12]

V. AMALIY MASHG‘ULOT MATERIALLARI

Amaliy mashg‘ulotlar kompyuter sinfida o‘tkaziladi. Har bir mashg‘ulot quyidagi tuzilishga ega: mavzu, maqsad, kutilayotgan natijalar, kerakli jihozlar, ishni bajarish tartibi (namunaviy ishlanmalar va dastur kodlari bilan), mustaqil bajarish uchun variantli topshiriqlar va nazorat savollari. A1 da tuzilgan tahdid modeli va A2–A9 natijalari A10 dagi maktab xavfsizlik siyosati loyihasiga asos bo‘ladi.

Amaliy ishni topshirish tartibi. Tinglovchi namunaviy topshiriqni bajaradi, so‘ngra o‘z variantidagi topshiriqni mustaqil bajaradi va natijani (jadval, dastur, skrinshotlar bilan hisobot) namoyish etib, nazorat savollariga javob beradi. Barcha natijalar tinglovchining “familiya_AX” papkasida saqlanadi. Variant raqami tinglovchining jurnaldagi tartib raqami bo‘yicha aniqlanadi (raqam 10 dan katta bo‘lsa, 10 ga bo‘lgandagi qoldiq olinadi; qoldiq 0 bo‘lsa – 10-variant).

Xavfsizlik qoidalar: amaliy ishlarda faqat o‘z kompyuteringiz, o‘quv virtual mashinasi va o‘qituvchi bergan o‘quv fayllari bilan ishlanadi. Haqiqiy akkauntlarda 2FA ni sozlashda zaxira kodlar xavfsiz saqlanadi. Real shaxsiy ma’lumotlar o‘rniga o‘ylab topilgan ma’lumotlar ishlatiladi.

Amaliy ishlar uchun umumiy baholash mezon:

Baho	Mezon
5	Topshiriq to‘liq va to‘g‘ri bajarilgan; dastur ishlaydi; xavfsizlik nuqtayi nazaridan asoslangan xulosalar chiqarilgan; himoyada barcha savollarga javob berilgan
4	Topshiriq bajarilgan, 1–2 ta kichik kamchilik bor
3	Topshiriq qisman bajarilgan, jiddiy kamchiliklar bor
2	Topshiriq bajarilmagan yoki ko‘chirilgan

1-AMALIY MASHG‘ULOT. AXBOROT TIZIMI UCHUN TAHDID VA ZAIFLIK MODELINI TUZISH

Maqsad: axborot tizimining aktivlarini aniqlash, ularga tahdid va zaifliklarni tahlil qilish hamda xavflarni baholab, ustuvor himoya choralarini tanlash ko‘nikmasini shakllantirish.

Kutilayotgan natijalar (TN1): tinglovchi aktivlar reyestrini tuzadi; har bir aktiv uchun CIA bo‘yicha qadrni belgilaydi; tahdid–zaiflik juftliklarini aniqlaydi; xavf matritsasi asosida ustuvorlikni belgilaydi.

Kerakli jihozlar: elektron jadval (Excel yoki Google Sheets), M1 va M9 materiallari.

Ishni bajarish tartibi

1-qadam. Tizim chegarasini aniqlash. Namunaviy tizim – “Maktab elektron jurnali va kompyuter sinfi”. Tizim tarkibi: elektron jurnal akkauntlari (o‘qituvchilar, sinf rahbarlari, direktor o‘rinbosari), 15 ta kompyuterli informatika sinfi, o‘qituvchi kompyuteri, Wi-Fi router, o‘quvchilar ro‘yxati jadvali, maktab Telegram kanali.

2-qadam. Aktivlar reyestri. Har bir aktiv uchun konfidensiallik (K), yaxlitlik (Y), foydalanuvchanlik (F) bo‘yicha qadr 1–3 ballda baholanadi:

№	Aktiv	Turi	K	Y	F
1	Elektron jurnaldagi baholar	Axborot	2	3	2
2	O‘qituvchilarning jurnal akkauntlari	Axborot	3	3	2
3	O‘quvchilar ro‘yxati (ism, telefon, manzil)	Axborot	3	2	1
4	Kompyuter sinfi kompyuterlari	Qurilma	1	2	3
5	Wi-Fi router	Qurilma	2	2	3
6	Nazorat ishi variantlari	Axborot	3	2	2

3-qadam. Tahdid–zaiflik juftliklari va xavfni baholash (ehtimollik va ta’sir 1–3 ball, $xavf = ehtimollik \times ta'sir$):

№	Aktiv	Tahdid	Zaiflik	E	T	X
1	Jurnal akkauntlari	Parolni fishing orqali o‘g‘irlash	2FA yo‘q, o‘qitilmagan xodimlar	3	3	9
2	Kompyuter sinfi	Zararli dastur	Hamma admin huquqida, USB nazorat qilinmaydi	3	2	6
3	O‘quvchilar ro‘yxati	Ma’lumotlar sizib chiqishi	Jadval “havolasi bor har kim” rejimida ulashilgan	2	3	6
4	Wi-Fi router	Ruxsatsiz ulanish	Standart admin paroli, WPA2 paroli devorga yozilgan	2	2	4
5	Nazorat ishi variantlari	Oldindan tarqalishi	O‘qituvchi kompyuteri qulflanmaydi	2	2	4

4-qadam. Choralarini tanlash. Xavfi 6 va undan yuqori bo‘lgan qatorlar uchun aniq chora, mas’ul shaxs va muddat belgilanadi (masalan: “Barcha o‘qituvchilar jurnal akkauntiga 2FA ni yoqadi – mas’ul: informatika o‘qituvchisi – 2 hafta”).

5-qadam. Xulosa. Eng yuqori uchta xavf va ularga qarshi choralar 5–6 jumlada yoziladi.

Mustaqil bajarish uchun variantlar

Quyidagi tizimlardan biri uchun kamida 6 ta aktiv va 6 ta tahdid–zaiflik juftligidan iborat model tuzing, xavf matritsasini chizing va choralarni tanlang.

Variant	Tizim
1	Maktab kutubxonasining elektron katalogi va o‘quvchi formulyarlari
2	Maktab veb-sayti va Telegram kanali
3	O‘qituvchining shaxsiy noutbuki va bulutli disk
4	Maktab buxgalteriyasi kompyuteri
5	Onlayn dars o‘tkaziladigan videokonferensiya tizimi
6	Kuzatuv kameralari tizimi
7	Maktabning ota-onalar bilan aloqa guruhi
8	Olimpiada natijalari va nazorat ishlari bazasi
9	O‘quv markazining onlayn ro‘yxatdan o‘tish formasi
10	Maktab psixologining elektron hujjatlari

Nazorat savollari

1. Aktivning qadri qanday baholanadi?
2. Tahdid va zaiflikka modelingizdan misol keltiring.
3. Nima uchun bir xil tahdid turli tashkilotlarda turli darajadagi xavf tug‘diradi?
4. Xavf matritsasining qaysi kataklaridagi xavflar birinchi navbatda bartaraf etiladi?
5. Qoldiq xavf nima?

2-AMALIY MASHG‘ULOT. KUCHLI PAROLLAR YARATISH, PAROL MENEJERLARI VA IKKI FAKTORLI AUTENTIFIKATSIYANI SOZLASH

Maqsad: parol kuchliligini baholash, parol iboralari yaratish, parol menejeri va autentifikator ilovasi bilan ishlash ko‘nikmalarini shakllantirish.

Kutilayotgan natijalar (TN7): tinglovchi parol entropiyasini hisoblaydi; KeePassXC (yoki Bitwarden) da parollar bazasini yaratadi; o‘quv akkauntida TOTP asosidagi 2FA ni yoqadi; maktab uchun parol siyosati qoidalarini tuzadi.

Kerakli jihozlar: kompyuter, Python 3, KeePassXC, smartfonda Google Authenticator yoki Microsoft Authenticator, o‘quv Google akkaunti.

Ishni bajarish tartibi

1-qadam. Entropiyani qo‘lda hisoblash. M5 dagi formula ($H = L \cdot \log_2 N$) bo‘yicha quyidagi parollar entropiyasini hisoblang: **sinf7a**, **Sinf7A2026**, **S!nf7#A_2026**, **quyosh-daftar-olma-bulut**. Natijalarni jadvalga yozing.

2-qadam. Parolni baholovchi dastur. Quyidagi dastur parol entropiyasini taxminan hisoblaydi, keng tarqalgan parollarni aniqlaydi va **secrets** moduli yordamida tasodifiy parol iborasini yaratadi (**random** moduli kriptografik maqsadlar uchun yaroqsiz):

```
import math, secrets, string

KENG_TARQALGAN = {"123456", "12345678", "qwerty", "password", "parol", "111111",
                  "123123", "admin", "iloveyou", "toshkent2026"}

def alifbo_hajmi(parol):
    n = 0
    if any(b.islower() for b in parol): n += 26
    if any(b.isupper() for b in parol): n += 26
    if any(b.isdigit() for b in parol): n += 10
    if any(b in string.punctuation for b in parol): n += 32
    return n

def baholash(parol):
    if parol.lower() in KENG_TARQALGAN:
        return 0, "juda kuchsiz (keng tarqalgan parol)"
    h = len(parol) * math.log2(alifbo_hajmi(parol))
    if h < 40: daraja = "kuchsiz"
    elif h < 60: daraja = "o'rtacha"
    elif h < 80: daraja = "kuchli"
    else: daraja = "juda kuchli"
    return round(h), daraja

def parol_iborasi(sozlar, n=5):
    return "-".join(secrets.choice(sozlar) for _ in range(n))

for p in ["qwerty", "Salom12", "Maktab#2026", "kitob-daraxt-quyosh-daftar-olma"]:
    print(f"{p:35} {baholash(p)}")

sozlar = ["kitob", "daraxt", "quyosh", "daftar", "olma", "bulut", "tog", "daryo",
          "qalam", "yulduz"]
print(parol_iborasi(sozlar))
```

Natija:

qwerty	(0, 'juda kuchsiz (keng tarqalgan parol)')
Salom12	(42, "o'rtacha")
Maktab#2026	(72, 'kuchli')
kitob-daraxt-quyosh-daftar-olma	(182, 'juda kuchli')
kitob-quyosh-daryo-bulut-yulduz	

Dastur natijasini tanqidiy tahlil qiling: **Maktab#2026** formal ravishda “kuchli” chiqdi, ammo u soʻz + yil + belgi andozasiga mos va lugʻat hujumlarida tez topiladi. Parol iborasi uchun haqiqiy entropiya belgilar soni boʻyicha emas, **soʻzlar soni** boʻyicha hisoblanadi: 10 soʻzli lugʻatdan 5 ta soʻz – atigi $5 \cdot \log_2 10 \approx 17$ bit, 7776 soʻzli lugʻatdan 5 ta soʻz – ≈ 65 bit. Shuning uchun real parol iboralari katta lugʻatlardan (masalan, EFF Diceware roʻyxati) tanlanadi.

3-qadam. Parol menejeri. KeePassXC da yangi baza yarating (Database → New Database), uzun asosiy parol iborasini o‘rnating. Uchta o‘quv yozuvi qo‘shing va parol generatori yordamida 20 belgili parollar yarating. Baza fayli (.kdbx) shifrlangan holda saqlanishini, asosiy parolsiz ochilmasligini tekshiring.

4-qadam. 2FA ni yoqish. O‘quv Google akkauntida: Akkaunt boshqaruvi → Xavfsizlik → 2 bosqichli tasdiqlash → Autentifikator ilovasi. QR-kodni smartfondagi ilova bilan skanerlang, 6 xonali kodni kiriting. Zaxira kodlarni yuklab olib, xavfsiz joyda saqlang. Chiqib, qayta kirish orqali 2FA ishlashini tekshiring.

5-qadam. Parol siyosati. M5 dagi NIST tavsiyalari asosida maktab uchun 6–8 banddan iborat parol siyosatini yozing.

Mustaqil bajarish uchun variantlar

Variant	Topshiriq
1	1–4-sinf o‘quvchilari uchun “Parolim – sirim” mavzusida 5 ta oddiy qoida va o‘yin topshirig‘ini tuzing
2	Dasturni kengaytiring: parolda foydalanuvchi ismi yoki tug‘ilgan yil bo‘lsa, ogohlantirsin
3	8, 10, 12, 16 belgili parollar uchun ($N = 94$) entropiya va to‘liq tanlash vaqtini (sekundiga 10^{10} urinish) hisoblang
4	Bitwarden va KeePassXC parol menejerlarini 6 ta mezon bo‘yicha taqqoslang
5	SMS, TOTP, push va passkey 2FA usullarini xavfsizlik va qulaylik bo‘yicha jadvalda baholang
6	Dasturga takrorlanuvchi belgilar (aaaa, 1111) va ketma-ketliklarni (abcd, 1234) aniqlash funksiyasini qo‘shing
7	O‘qituvchilar uchun “Telefon yo‘qolsa 2FA akkauntini qanday tiklash” yo‘riqnomasini tuzing
8	5 ta tasodifiy so‘zli parol iborasini yaratuvchi va uning so‘zlar bo‘yicha entropiyasini hisoblovchi dastur yozing
9	Credential stuffing hujumi oqibatlarini tushuntiruvchi 5 slaydli taqdimot tayyorlang
10	Maktab elektron jurnali uchun parol siyosati va hisoblarni bloklash qoidalarini ishlab chiqing

Nazorat savollari

1. Nima uchun parol uzunligi tarkibidagi belgilar xilma-xilligidan muhimroq?
2. secrets va random modullarining farqi nimada?
3. Parol menejeri buzilsa nima bo‘ladi va bu xavf qanday kamaytiriladi?
4. TOTP kodi nima uchun Internet aloqasiz ham ishlaydi?
5. Zaxira kodlar nima uchun kerak?

3-AMALIY MASHG'ULOT. FISHING XATLARINI ANIQLASH VA TAHLIL QILISHGA DOIR KEYSLAR

Maqsad: fishing xatlari, SMS va saytlarning belgilarini aniqlash, havolalarni tahlil qilish va to'g'ri harakat algoritmini ishlab chiqish ko'nikmasini shakllantirish.

Kutilayotgan natijalar (TN9): tinglovchi xatlarni "fishing / ishonchli / shubhali" deb tasniflaydi va asoslaydi; URL dagi asosiy domenni aniqlaydi; xodimlar uchun eslatma tuzadi.

Kerakli jihozlar: o'qituvchi tayyorlagan xatlar to'plami (bosma yoki PDF), M4 materiallari.

Mashg'ulotda faqat o'quv xatlari ishlatiladi. Haqiqiy shubhali xatlardagi havolalar bosilmaydi va ilovalar ochilmaydi – ular faqat skrinshot sifatida tahlil qilinadi.

Ishni bajarish tartibi

1-qadam. Xatlar to'plami bilan tanishish. Quyidagi 6 ta xat (keys) tahlil qilinadi:

№	Xat yoki xabar mazmuni
1	Jo'natuvchi: xavfsizlik@uzcard-support.info . "Kartangiz bloklandi! 2 soat ichida ma'lumotlaringizni tasdiqlang: karta raqami, amal qilish muddati va SMS-kod." Havola: http://uzcard-verify.info/login
2	Jo'natuvchi: direktorning familiyasi, lekin manzil direktor.maktab21@gmail.com (maktab rasmiy pochta boshqa). "Shoshilinch! Uchrashuvdaman, qo'ng'iroq qila olmayman. Sovg'a uchun 5 ta 100 000 so'mlik 'Payme' to'lov kartasini sotib olib, kodlarini yuboring."
3	Telegram xabari tanishdan: "Salom, mana bu ovozga qatnashib yuboring, sinfimiz g'olib bo'lsin □", havola t.mega o'xshash, lekin telegram-vote.top saytiga olib boradi va telefon raqami hamda kodni so'raydi
4	Jo'natuvchi: no-reply@accounts.google.com . "Yangi qurilmadan kirish aniqlandi. Agar bu siz bo'lmasangiz, akkauntingizni tekshiring." Havola https://myaccount.google.com/notifications ga olib boradi
5	SMS: "Pochta: posilkangiz yetkazilmadi, manzilni yangilang va 3 900 so'm to'lang: https://uzpost.delivery-track.cc "
6	Elektron pochta: "Yangi o'quv yili dars jadvali" mavzusi, ilova Dars_jadvali_2026.xlsm , matnda "Ochish uchun 'Tahrirlashni yoqish' va 'Kontentni yoqish' tugmalarini bosing"

2-qadam. Tahlil jadvali. Har bir xat uchun quyidagi jadval to'ldiriladi:

№	Belgilar	Haqiqiy domen / jo'natuvchi	Xulosa	To'g'ri harakat
1	Shoshilinchlik, SMS-kod so'rash, HTTP	uzcard-verify.info – rasmiy emas	Fishing	Javob bermaslik, bankka rasmiy raqam orqali murojaat

№	Belgilar	Haqiqiy domen / jo‘natuvchi	Xulosa	To‘g‘ri harakat
2	Avtoritet, shoshilinchlik, sovg‘a kartalari, tashqi pochta	Shaxsiy Gmail manzil	Fishing (BEC)	Direktorga shaxsan yoki rasmiy raqam orqali qo‘ng‘iroq
3	Tanishning buzilgan akkaunti, kod so‘rash	telegram-vote.top	Fishing	Kodni kiritmaslik, tanishni boshqa kanal orqali ogohlantirish
4	Odatiy xabarnoma, hech narsa so‘ramaydi	google.com – rasmiy	Ishonchli (lekin havolani bosmasdan, akkauntga o‘zi kirib tekshirish yaxshiroq)	Akkauntga o‘zi kirib, faollikni tekshirish
5	Kichik to‘lov, soxta yetkazib berish	delivery-track.cc	Smishing	E‘tiborsiz qoldirish, spam deb belgilash
6	Makrosli ilova, makroslarni yoqishga undash	Jo‘natuvchi tekshirilishi kerak	Zararli dastur yuborish urinishi	Ochmaslik, AT mas‘uliga xabar berish

3-qadam. URL lar bilan mashq. Quyidagi havolalar uchun asosiy domenni yozing va “ishonchli / soxta” deb belgilang: <https://kundalik.com.login.uz-edu.net>, <https://my.gov.uz/oz>, <https://lex.uz/docs/123>, <https://paypal.com-secure.account-check.ru>, <https://edu.uz.pass-reset.org>.

4-qadam. Eslatma. O‘qituvchilar uchun bir sahifalik “Fishingni qanday aniqlash mumkin” eslatmasini (7–10 band, “To‘xta – o‘yla – tekshir” qoidasi bilan) Canva yoki Word da tayyorlang.

Mustaqil bajarish uchun variantlar

Variant	Topshiriq
1	Bank nomidan vishing qo‘ng‘irog‘i ssenariysini tahlil qiling va to‘g‘ri javob algoritmini tuzing
2	5–6-sinflar uchun “Fishing ovchisi” o‘yini kartochkalarini tayyorlang (8 ta xabar)
3	QR-kod orqali fishing (kvishing) bo‘yicha 3 ta vaziyat va himoya qoidalarini yozing
4	Elektron pochta sarlavhasini (Received, From, Reply-To, SPF natijasi) o‘quv namunasi asosida tahlil qiling

Variant	Topshiriq
5	Messenjer akkauntini o'g'irlash usullari va himoya (2 bosqichli parol) bo'yicha yo'riqnoma tuzing
6	"Sovg'a yutdingiz" turidagi firibgarlik saytlari belgilarini o'quvchilar uchun infografika qiling
7	Sun'iy intellekt yordamida yaratilgan fishing xatlari xavfi haqida 1 sahifalik tahlil yozing
8	Ota-onalar uchun "Bolangiz nomidan pul so'rasa" vaziyati bo'yicha eslatma tuzing
9	Maktab uchun fishing xatini olganda xabar berish tartibini (kimga, qanday, qachon) ishlab chiqing
10	Tayposkvotting misollarini (5 ta mashhur domen uchun) tuzing va ularni aniqlash usullarini tushuntiring

Nazorat savollari

1. Fishing xatining eng ishonchli belgilari qaysilar?
2. URL ning asosiy domeni qanday aniqlanadi?
3. BEC hujumi qanday amalga oshiriladi?
4. Makrosli hujjatlar qanday xavf tug'diradi?
5. Adashib fishing havolasini bosgan xodim nima qilishi kerak?

4-AMALIY MASHG'ULOT. KLASSIK SHIFRLASH USULLARI (SEZAR, VIJINER) BO'YICHA MASALALAR YECHISH

Maqsad: o'rniga qo'yish shifrlarining ishlash tamoyilini tushunish, ularni qo'lda va dasturiy amalga oshirish, kriptotahlil usullari (to'liq tanlash, chastota tahlili) bilan tanishish.

Kutilayotgan natijalar (TN5): tinglovchi Sezar va Vijiner shifrlarida qo'lda shifrlaydi va ochadi; Python dasturini yozadi; Sezar shifrnini to'liq tanlash bilan ochadi; harflar chastotasini hisoblaydi.

Kerakli jihozlar: kompyuter, Python 3, Vijiner jadvali (bosma), M6 materiallari.

Ishni bajarish tartibi

1-qadam. Qo'lda shifrlash. Lotin alifbosi harflarini 0–25 raqamlariga mos qo'yib ($A = 0, B = 1, \dots, Z = 25$), quyidagilarni bajaring:

- **ALGORITM** so'zini Sezar shifri bilan $k = 5$ kalit bilan shifrlang (javob: **FQLTWNRY**);
- **WONDOE** shifmatnini **KOD** kaliti bilan Vijiner usulida oching (javob: **MAKTAB**).

2-qadam. Shifrlash dasturi. Quyidagi dastur ikkala shifrnini ham amalga oshiradi; alifbodan tashqari belgilar (bo'shliq, tinish belgilari) o'zgarmaydi:

```

ALIFBO = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

def sezar(matn, k):
    natija = ""
    for belgi in matn.upper():
        if belgi in ALIFBO:
            natija += ALIFBO[(ALIFBO.index(belgi) + k) % 26]
        else:
            natija += belgi
    return natija

def vijiner(matn, kalit, ochish=False):
    natija, j = "", 0
    kalit = kalit.upper()
    for belgi in matn.upper():
        if belgi in ALIFBO:
            siljish = ALIFBO.index(kalit[j % len(kalit)])
            if ochish:
                siljish = -siljish
            natija += ALIFBO[(ALIFBO.index(belgi) + siljish) % 26]
            j += 1
        else:
            natija += belgi
    return natija

if __name__ == "__main__":
    shifr = sezar("INFORMATIKA", 3)
    print(shifr)                                # LQIRUPDWLND
    print(sezar(shifr, -3))                     # INFORMATIKA
    v = vijiner("MAKTAB", "KOD")
    print(v)                                    # WONDOE
    print(vijiner(v, "KOD", ochish=True))      # MAKTAB

```

Natija:

```

LQIRUPDWLND
INFORMATIKA
WONDOE
MAKTAB

```

3-qadam. Kriptotahlil. Sezar shifrida atigi 25 ta kalit bo‘lgani uchun uni barcha kalitlarni sinab ochish mumkin. Harflar chastotasini hisoblash esa bir alifboli shifrlarni kalitsiz ochishga yordam beradi:

```

from klassik import sezar
from collections import Counter

shifr = "LQIRUPDWLND"
for k in range(1, 26):
    print(k, sezar(shifr, -k))                # to'liq tanlash: barcha 25 kalit

matn = "AXBOROT XAVFSIZLIGI MAKTABDA MUHIM AHAMIYATGA EGA"
print(Counter(b for b in matn if b.isalpha()).most_common(3))

```

Natija (qisqartirilgan):

```
1 KPHQTOCVKMC
2 JOGPSNBUJLB
3 INFORMATIKA      <- ma'noli so'z: kalit topildi
...
25 MRJSVQEXMOE
[('A', 10), ('I', 5), ('M', 4)]
```

O'zbek tilidagi matnlarda "A" va "I" harflari eng ko'p uchraydi; agar Sezar shifratnida eng ko'p uchragan harf "D" bo'lsa, kalit katta ehtimol bilan $k = 3$ ($A \rightarrow D$).

Mustaqil bajarish uchun variantlar

Har bir variantda: a) Sezar shifri bilan qo'lda shifrlang; b) Vijiner shifri bilan qo'lda shifrlang; c) natijalarni dastur bilan tekshiring; d) dasturni ko'rsatilgan funksiya bilan kengaytiring.

Variant	Ochiq matn	Sezar k	Vijiner kaliti	Dasturni kengaytirish
1	XAVFSIZLIK	4	DARS	Kirill alifbosi uchun Sezar shifri
2	KOMPYUTER	7	SINF	Shifratnni 5 belgili guruhlariga bo'lib chiqarish
3	PAROL	11	KALIT	Matnni fayldan o'qib, shifrlangan faylga yozish
4	TARMOQ	13	OLMA	ROT13: ikki marta qo'llash dastlabki matnni berishini isbotlash
5	DASTUR	9	BAHO	Chastota tahlili asosida Sezar kalitini avtomatik topish
6	SERVER	15	KITOB	Atbash shifri ($A \leftrightarrow Z$, $B \leftrightarrow Y$, ...)
7	MAKTAB	21	QALAM	Kichik va katta harflarni saqlab shifrlash
8	INTERNET	6	YULDUZ	O'zbek lotin alifbosidagi O', G', SH, CH harflarini hisobga olish
9	SHIFR	17	DAFTAR	Vijiner shifrida kalit uzunligini kiritish va tekshirish
10	ALGORITM	19	QUYOSH	Affin shifri: $C = (a \cdot P + b) \bmod 26$, $a = 5$, $b = 8$

Nazorat savollari

1. Sezar shifrida nechta kalit bor va nima uchun?
2. Chastota tahlili qanday ishlaydi?
3. Vijiner shifri nima uchun chastota tahliliga chidamlir?
4. Dasturda **% 26** amali nima uchun kerak?
5. Klassik shifrlarni maktabda o'qitishning pedagogik ahamiyati nimada?

5-AMALIY MASHG'ULOT. ZAMONAVIY SHIFRLASH: AES VA RSA ALGORITMLARINI DASTURIY VOSITALARDA QO'LLASH

Maqsad: zamonaviy simmetrik va asimmetrik shifrlash algoritmlarini tayyor kutubxonalar va dasturlar yordamida qo'llash, paroldan kalit hosil qilish va raqamli imzo tamoyillarini amalda ko'rish.

Kutilayotgan natijalar (TN5, TN8): tinglovchi 7-Zip da AES-256 bilan arxivni shifrlaydi; Python **cryptography** kutubxonasida simmetrik shifrlash, RSA va imzolashni bajaradi; fayllarni parol asosida shifrlovchi dastur bilan ishlaydi.

Kerakli jihozlar: kompyuter, Python 3, **cryptography** kutubxonasi (**pip install cryptography**), 7-Zip, OpenSSL (ixtiyoriy).

Kriptografik algoritmlarni o'zingiz "noldan" yozmang: real tizimlarda faqat tekshirilgan kutubxonalar ishlatiladi. Quyidagi dasturlar o'quv maqsadida, tayyor kutubxona funksiyalari asosida yozilgan.

Ishni bajarish tartibi

1-qadam. 7-Zip bilan shifrlash. Faylni tanlab: o'ng tugma → 7-Zip → Arxivga qo'shish → Format: 7z, Shifrlash usuli: AES-256, kuchli parol kiriting va "Fayl nomlarini shifrlash" belgisini qo'ying. Arxivni parolsiz ochishga urinib ko'ring.

2-qadam. Simmetrik va asimmetrik shifrlash, imzo. **Fernet** – **cryptography** kutubxonasidagi oson va xavfsiz simmetrik shifrlash usuli (AES-128 CBC rejimida + HMAC-SHA256 yaxlitlik nazorati). RSA bilan esa OAEP to'ldirish sxemasi qo'llaniladi:

```

from cryptography.fernet import Fernet
from cryptography.hazmat.primitives.asymmetric import rsa, padding
from cryptography.hazmat.primitives import hashes

# 1. Simmetrik shifrlash (Fernet: AES-128 + HMAC)
kalit = Fernet.generate_key()
f = Fernet(kalit)
shifrlangan = f.encrypt("Nazorat ishi javoblari".encode("utf-8"))
print(shifrlangan[:30], "...")
print(f.decrypt(shifrlangan).decode("utf-8"))

# 2. Asimmetrik shifrlash (RSA-2048, OAEP)
yopiq = rsa.generate_private_key(public_exponent=65537, key_size=2048)
ochiq = yopiq.public_key()
oaep = padding.OAEP(mgf=padding.MGF1(algorithm=hashes.SHA256()),
                    algorithm=hashes.SHA256(), label=None)
xabar = ochiq.encrypt(b"Maxfiy xabar", oaep)
print(len(xabar), "bayt")
print(yopiq.decrypt(xabar, oaep))

# 3. Raqamli imzo (RSA-PSS)
pss = padding.PSS(mgf=padding.MGF1(hashes.SHA256()),
                  salt_length=padding.PSS.MAX_LENGTH)
hujjat = b"Buyruq: 7-A sinf baholari tasdiqlandi"
imzo = yopiq.sign(hujjat, pss, hashes.SHA256())
ochiq.verify(imzo, hujjat, pss, hashes.SHA256()) # xato bo'lsa istisno chiqadi
print("Imzo to'g'ri")

```

Natija:

```

b'gAAAAABo...' ...
Nazorat ishi javoblari
256 bayt
b'Maxfiy xabar'
Imzo to'g'ri

```

2048 bitli RSA kaliti bilan shifrlangan har qanday qisqa xabar 256 bayt (2048 bit) uzunlikka ega bo'ladi. RSA katta fayllarni shifrlash uchun ishlatilmaydi – buning uchun gibril sxema qo'llaniladi (M6). Imzolangan **hujjat** dagi bitta belgi o'zgartirilsa, **verify** funksiyasi **InvalidSignature** xatosini chiqaradi – buni o'zingiz tekshirib ko'ring.

3-qadam. Faylni parol bilan shifrlash. Inson eslab qoladigan parol to'g'ridan to'g'ri kalit sifatida ishlatilmaydi: undan **PBKDF2** funksiyasi yordamida tasodifiy “tuz” (salt) va ko'p sonli iteratsiyalar bilan kalit hosil qilinadi. Bu parollarni tanlash hujumini sekinlashtiradi:

```

import base64, os
from cryptography.fernet import Fernet
from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC
from cryptography.hazmat.primitives import hashes

def kalit_hosil_qil(parol, tuz):
    kdf = PBKDF2HMAC(algorithm=hashes.SHA256(), length=32, salt=tuz,
iterations=600_000)
    return base64.urlsafe_b64encode(kdf.derive(parol.encode("utf-8")))

def shifrla(fayl, parol):
    tuz = os.urandom(16)
    f = Fernet(kalit_hosil_qil(parol, tuz))
    with open(fayl, "rb") as fin:
        malumot = fin.read()
    with open(fayl + ".enc", "wb") as fout:
        fout.write(tuz + f.encrypt(malumot))

def deshifrla(fayl_enc, parol):
    with open(fayl_enc, "rb") as fin:
        tuz, token = fin.read(16), fin.read()
    f = Fernet(kalit_hosil_qil(parol, tuz))
    return f.decrypt(token) # parol noto'g'ri bo'lsa InvalidToken xatosi

with open("baholar.txt", "w", encoding="utf-8") as t:
    t.write("Aliyev Bobur - 5\nKarimova Dilnoza - 4\n")
shifrla("baholar.txt", "kitob-daraxt-quyosh-daftar")
print(deshifrla("baholar.txt.enc", "kitob-daraxt-quyosh-daftar").decode("utf-8"))
try:
    deshifrla("baholar.txt.enc", "notogri-parol")
except Exception as e:
    print("Xato:", type(e).__name__)

```

Natija:

```

Aliyev Bobur - 5
Karimova Dilnoza - 4

Xato: InvalidToken

```

Mustaqil bajarish uchun variantlar

Variant	Topshiriq
1	<code>fayl_shifr.py</code> ni papkadagi barcha <code>.txt</code> fayllarni shifrlaydigan qilib kengaytiring
2	Iteratsiyalar soni 1 000, 100 000 va 600 000 bo'lganda kalit hosil qilish vaqtini o'lchang va xulosa yozing
3	RSA kalitlarini PEM faylga saqlash va o'qish dasturini yozing (yopiq kalit parol bilan himoyalansin)
4	Gibrid shifrlash: faylni Fernet bilan, Fernet kalitini RSA ochiq kaliti bilan shifrllovchi dastur yozing
5	Imzolangan hujjatga bitta belgi qo'shilganda tekshiruv natijasini ko'rsating va tushuntiring
6	7-Zip, VeraCrypt va BitLocker shifrlash vositalarini 6 ta mezon bo'yicha taqqoslang

Variant	Topshiriq
7	OpenSSL buyruqlari bilan faylni AES-256 da shifrlang va oching (<code>openssl enc -aes-256-cbc -pbkdf2</code>)
8	Bir xil matnni Fernet bilan ikki marta shifrlang; shifmatnlar nima uchun farq qilishini tushuntiring
9	Tkinter oynali “Matnni shifrlash/ochish” dasturini yarating (parol asosida)
10	O‘quvchilar uchun “Ochiq va yopiq kalit” tushunchasini qulf va kalit misolida tushuntiruvchi dars fragmentini tuzing

Nazorat savollari

1. Fernet qanday algoritmlardan foydalanadi?
2. Nima uchun paroldan kalit PBKDF2 orqali hosil qilinadi?
3. “Tuz” (salt) nima uchun kerak?
4. RSA da shifrlash va imzolashda qaysi kalitlar ishlatiladi?
5. Nima uchun RSA bilan katta fayllar shifrlanmaydi?

6-AMALIY MASHG‘ULOT. XESH-FUNKSIYALAR VA FAYL YAXLITLIGINI TEKSHIRISH

Maqsad: xesh-funksiyalarning xossalarini amalda o‘rganish, fayllarning nazorat yig‘indilarini hisoblash va ular asosida fayl yaxlitligini tekshirish.

Kutilayotgan natijalar (TN5, TN8): tinglovchi OS buyruqlari va Python yordamida SHA-256 xeshini hisoblaydi; ko‘chki effektini ko‘rsatadi; yuklab olingan dastur xeshini rasmiy qiymat bilan solishtiradi; papka yaxlitligini nazorat qiluvchi dastur bilan ishlaydi.

Kerakli jihozlar: kompyuter, Python 3, PowerShell yoki Linux terminali.

Ishni bajarish tartibi

1-qadam. OS vositalari bilan xesh hisoblash.

```
# Windows PowerShell
Get-FileHash .\dastur.exe -Algorithm SHA256
# Windows buyruq qatori
certutil -hashfile dastur.exe SHA256
# Linux / macOS
sha256sum dastur.iso
```

Rasmiy saytdan biror ochiq dastur (masalan, 7-Zip yoki Python o‘rnatuvchisi) yuklab olib, uning SHA-256 xeshini saytda e‘lon qilingan qiymat bilan solishtiring.

2-qadam. Ko‘chki effekti.

```
import hashlib

def fayl_xeshi(yol):
    h = hashlib.sha256()
    with open(yol, "rb") as f:
        for qism in iter(lambda: f.read(65536), b''):
            h.update(qism)
    return h.hexdigest()

print(hashlib.sha256("Salom".encode()).hexdigest())
print(hashlib.sha256("salom".encode()).hexdigest()) # bitta harf farqi - butunlay
boshqa xesh
```

Natija:

```
441f71d48aacacdc18293201da2bfda40a421c4f93d8e509fcd2d0440b007b46
038f270ca678c66f5bf393f958e8eebcf98b049e5a0d32a69cabf46b576cabbf
```

Bitta harfning ($S \rightarrow s$) o'zgarishi xeshni butunlay o'zgartirdi. **fayl_xeshi** funksiyasi katta fayllarni ham xotiraga to'liq yuklamasdan, 64 KB lik qismlarda o'qiydi.

3-qadam. Papka yaxlitligini nazorat qilish. Quyidagi dastur papkadagi fayllar xeshlarini JSON faylga yozadi, keyinroq esa qaysi fayllar o'zgartirilgan yoki o'chirilganini aniqlaydi. Bu yondashuv yaxlitlikni nazorat qilish tizimlarining (masalan, nazorat ishlari, buyruqlar arxivi uchun) soddalashtirilgan modeli:

```

import hashlib, json, os

def fayl_xeshi(yol):
    h = hashlib.sha256()
    with open(yol, "rb") as f:
        for qism in iter(lambda: f.read(65536), b''):
            h.update(qism)
    return h.hexdigest()

def royxat_tuz(papka, natija="xeshlar.json"):
    xeshlar = {n: fayl_xeshi(os.path.join(papka, n)) for n in
sorted(os.listdir(papka))}
    with open(natija, "w") as f:
        json.dump(xeshlar, f, indent=2)
    return xeshlar

def tekshir(papka, natija="xeshlar.json"):
    with open(natija) as f:
        eski = json.load(f)
    for nom, xesh in eski.items():
        yol = os.path.join(papka, nom)
        if not os.path.exists(yol):
            print(nom, "- O'CHIRILGAN")
        elif fayl_xeshi(yol) != xesh:
            print(nom, "- O'ZGARTIRILGAN")
        else:
            print(nom, "- o'zgarmagan")

os.makedirs("hujjatlar", exist_ok=True)
for i in range(1, 4):
    with open(f"hujjatlar/test{i}.txt", "w") as f:
        f.write(f"Nazorat ishi {i}-variant\n")
royxat_tuz("hujjatlar")
with open("hujjatlar/test2.txt", "a") as f:
    f.write("javob: B\n") # faylga o'zgartirish kiritamiz
tekshir("hujjatlar")

```

Natija:

```

test1.txt - o'zgarmagan
test2.txt - O'ZGARTIRILGAN
test3.txt - o'zgarmagan

```

Mustaqil bajarish uchun variantlar

Variant	Topshiriq
1	<code>yaxlitlik.py</code> ga papkaga qoʻshilgan yangi fayllarni aniqlash funksiyasini qoʻshing
2	Bir xil fayl uchun MD5, SHA-1, SHA-256, SHA-3-256 xeshlarini hisoblang va uzunliklarini taqqoslang
3	Ikki faylning bir xilligini (nomidan qat'i nazar) xesh orqali aniqlaydigan, takroriy fayllarni topuvchi dastur yozing
4	<code>hashlib.pbkdf2_hmac</code> yordamida parolni tuz bilan xeshlab saqlash va tekshirish dasturini yozing

Variant	Topshiriq
5	Rasmiy dastur saytidan 2 ta fayl yuklab, ularning xeshlarini tekshirish bo'yicha qadamma-qadam yo'riqnoma tuzing
6	hmac moduli yordamida xabar autentifikatsiya kodini hisoblang va oddiy xeshdan farqini tushuntiring
7	"Tug'ilgan kunlar paradoksi"ni 16 bitli qisqartirilgan xesh misolida dastur bilan modellashtiring
8	Xeshlash va shifrlashning farqini 6 ta mezon bo'yicha jadvalda ko'rsating
9	Tkinter oynali "Fayl xeshini hisoblash va solishtirish" dasturini yarating
10	8–9-sinf o'quvchilari uchun "Raqamli barmoq izi" mavzusida 15 daqiqalik dars fragmenti tuzing

Nazorat savollari

1. Xesh-funksiya qanday xossalarga ega bo'lishi kerak?
2. Ko'chki effekti nimani bildiradi?
3. Nima uchun MD5 xavfsizlik maqsadlarida ishlatilmaydi?
4. Yuklab olingan fayl xeshi rasmiy qiymatga mos kelmasa, nima qilish kerak?
5. Parollarni saqlashda oddiy SHA-256 o'rniga nima uchun maxsus funksiyalar ishlatiladi?

7-AMALIY MASHG'ULOT. ANTIVIRUS VA ZARARLI DASTURLARNI ANIQLASH VOSITALARI BILAN ISHLASH

Maqsad: antivirus dasturlarini sozlash, tekshiruv turlarini qo'llash, karantin va hisobotlar bilan ishlash, shubhali fayllarni xavfsiz baholash ko'nikmalarini shakllantirish.

Kutilayotgan natijalar (TN8): tinglovchi Microsoft Defender sozlamalarini tahlil qiladi; tez, to'liq va maxsus tekshiruvlarni bajaradi; EICAR sinov fayli yordamida antivirus reaksiyasini tekshiradi; karantin va tahdidlar tarixini o'rganadi; zararlanish belgilarini sanaydi.

Kerakli jihozlar: Windows 10/11 o'rnatilgan kompyuter yoki virtual mashina, Microsoft Defender, Internet.

Ishni bajarish tartibi

1-qadam. Defender holatini tekshirish. Windows xavfsizligi (Windows Security) → Viruslar va tahdidlardan himoya. Quyidagilar yoqilganini tekshiring va skrinshot oling: real vaqtdagi himoya, bulutli himoya, namunalarni avtomatik yuborish, buzib kirishdan himoya (Tamper Protection). "Ransomware himoyasi" bo'limida "Boshqariladigan papkalarga kirish" funksiyasi bilan tanishing.

2-qadam. Tekshiruv turlari. Tez tekshiruvni bajaring; “Tekshiruv parametrlari” bo‘limida to‘liq, maxsus (bitta papka yoki USB disk) va **Microsoft Defender Offline** tekshiruvlarining farqini jadvalga yozing.

3-qadam. EICAR sinov fayli. EICAR – Yevropa kompyuter antivirus tadqiqotlari instituti tomonidan ishlab chiqilgan, **zararsiz** standart sinov fayli: u hech qanday zararli harakat qilmaydi, lekin barcha antiviruslar uni “virus” deb aniqlashga kelishib olgan. Faylni rasmiy sahifadan (<https://www.eicar.org>, “Anti Malware Testfile” bo‘limi) yuklab olishga urinib ko‘ring va Defender reaksiyasini kuzating: bildirishnoma, fayl karantinga olinishi, “Himoya tarixi”dagi yozuv.

Real zararli dasturlar bilan o‘quv kompyuterida tajriba qilish taqiqlanadi. EICAR fayli antivirus ishlashini tekshirishning xavfsiz va qabul qilingan usuli.

4-qadam. Shubhali faylni baholash. Noma’lum faylni ochmasdan baholash usullari: fayl kengaytmasini tekshirish (Explorer’da “Fayl nomi kengaytmalari” ni yoqish: **hujjat.pdf.exe** kabi qo‘sh kengaytmalar), raqamli imzo (Xususiyatlar → Raqamli imzolar), fayl xeshini hisoblash (A6) va uni VirusTotal xizmatida xesh bo‘yicha qidirish.

VirusTotal’ga **maxfiy ma’lumotlar bo‘lgan** hujjatlarni yuklamang: yuklangan fayllar xavfsizlik tadqiqotchilariga ochiq bo‘lishi mumkin. Avval faqat xesh bo‘yicha qidiring.

5-qadam. Zararlanish belgilari va harakatlar. Kompyuter zararlanganining belgilarini (sekinlashish, noma’lum jarayonlar, brauzerda o‘zgargan bosh sahifa, fayllar kengaytmasi o‘zgarishi, antivirus o‘chib qolishi) va harakatlar ketma-ketligini (tarmoqdan uzish → offline tekshiruv → parollarni boshqa qurilmadan almashtirish → mas’ulga xabar → zarurat bo‘lsa qayta o‘rnatish va zaxiradan tiklash) yozing.

Mustaqil bajarish uchun variantlar

Variant	Topshiriq
1	Microsoft Defender va ClamAV ning imkoniyatlarini 6 ta mezon bo‘yicha taqqoslang
2	Kompyuter sinfi uchun haftalik antivirus tekshiruvi rejasini (vazifalar rejalashtiruvchisi bilan) tuzing
3	“Boshqariladigan papkalarga kirish” funksiyasini sozlang va uning to‘lov talab qiluvchi dasturlardan himoyasini tushuntiring
4	USB-flesh diskni avtomatik tekshirish va autorun xavfini kamaytirish bo‘yicha yo‘riqnoma tuzing
5	Vazifalar dispetcheri (Task Manager) va “Avtoyuklash” bo‘limi orqali shubhali dasturlarni aniqlash bo‘yicha qo‘llanma tuzing
6	Android smartfonda ilova ruxsatlarini tekshirish va Google Play Protect bo‘yicha yo‘riqnoma tuzing
7	Brauzer kengaytmalari xavfi va ularni tekshirish bo‘yicha eslatma tayyorlang

Variant	Topshiriq
8	Signatura, evristik va xulq-atvor tahlili usullarini misollar bilan tushuntiruvchi taqdimot tayyorlang
9	Kompyuter zararlanganida o'qituvchi uchun 1 sahifalik harakatlar algoritmini (blok-sxema) tuzing
10	O'quvchilar uchun "Cheat va krekdan ehtiyot bo'ling" mavzusida infografika tayyorlang

Nazorat savollari

1. Real vaqtdagi himoya va rejalashtirilgan tekshiruvning farqi nimada?
2. Defender Offline tekshiruvi qachon kerak?
3. EICAR fayli nima uchun xavfsiz?
4. Karantin nima va undan faylni qachon tiklash mumkin?
5. Kompyuter zararlanganda birinchi navbatda nima qilinadi?

8-AMALIY MASHG'ULOT. OPERATSION TIZIM XAVFSIZLIK SOZLAMALARI: FOYDALANUVCHI HUQUQLARI, YANGILANISHLAR, TARMOQLARARO EKRAN

Maqsad: operatsion tizimni xavfsiz sozlash: foydalanuvchi hisoblari va huquqlarini boshqarish, yangilanishlar, tarmoqlararo ekran, ekranni qulflash va diskni shifrlash holatini tekshirish.

Kutilayotgan natijalar (TN7): tinglovchi standart va administrator hisoblarini yaratadi; UAC va yangilanishlar sozlamalarini tekshiradi; Windows Defender Firewall qoidalarini ko'rib chiqadi; kompyuter sinfi uchun xavfsizlik nazorat varag'ini (checklist) tuzadi.

Kerakli jihozlar: Windows 10/11 virtual mashinasi (administrator huquqi bilan), ixtiyoriy – Ubuntu virtual mashinasi.

Ishni bajarish tartibi

1-qadam. Foydalanuvchi hisoblari. Sozlamalar → Hisoblar → Boshqa foydalanuvchilar orqali "Oquvchi" nomli **standart** hisob yarating. Yoki administrator PowerShell'da:

```
net user Oquvchi * /add
net localgroup Administrators
```

Standart hisobga kirib, dastur o'rnatishga urinib ko'ring – UAC administrator parolini so'raydi. Bu kam huquqlar tamoyilining amaldagi ko'rinishi (M5).

2-qadam. Yangilanishlar. Sozlamalar → Windows Update: oxirgi yangilanish sanasi, kutilayotgan yangilanishlar, "Faol soatlar" sozlamasini tekshiring. Brauzer va boshqa dasturlarning yangilanishini ham tekshiring.

3-qadam. Tarmoqlararo ekran. Windows xavfsizligi → Tarmoqlararo ekran va tarmoq himoyasi: domen, xususiy va ommaviy profillar holatini yozing. “Kengaytirilgan sozlamalar” (**wf.msc**) da kiruvchi qoidalar ro‘yxatini ko‘ring. Holatni buyruq bilan tekshirish:

```
netsh advfirewall show allprofiles state
```

Linux’da (Ubuntu) oddiy ekran **ufw** bilan boshqariladi: **sudo ufw enable**, **sudo ufw status verbose**.

4-qadam. Qo‘shimcha sozlamalar. Ekranni avtomatik qulflash (5–10 daqiqa), **Win + L** bilan qulflash odati, fayl kengaytmalarini ko‘rsatish, olinadigan qurilmalar uchun avtomatik ishga tushishni o‘chirish, BitLocker holati (L1), keraksiz dasturlarni o‘chirish.

5-qadam. Nazorat varag‘i. Natijalarni quyidagi shaklda rasmiylashtiring:

№	Tekshiruv bandi	Holat	Izoh
1	O‘quvchilar standart hisobda ishlaydi	✓ / ✗	
2	Administrator paroli kuchli va faqat mas’ulda	✓ / ✗	
3	Avtomatik yangilanishlar yoqilgan, oxirgi yangilanish 30 kundan eski emas	✓ / ✗	
4	Real vaqtdagi antivirus himoyasi yoqilgan	✓ / ✗	
5	Tarmoqlararo ekran barcha profillarda yoqilgan	✓ / ✗	
6	Ekran avtomatik qulflanadi	✓ / ✗	
7	Olinadigan qurilmalar uchun avtomatik ishga tushirish o‘chirilgan	✓ / ✗	
8	Litsenziyasiz va keraksiz dasturlar yo‘q	✓ / ✗	
9	O‘qituvchi kompyuteri diski shifrlangan	✓ / ✗	
10	Muhim ma’lumotlarning zaxira nusxasi mavjud	✓ / ✗	

Mustaqil bajarish uchun variantlar

Variant	Topshiriq
1	Ubuntu’da standart foydalanuvchi yaratish, sudo guruhi va ufw sozlamalari bo‘yicha hisobot
2	Windows’da mehmon hisoblari va avtomatik tizimga kirishni o‘chirish bo‘yicha yo‘riqnoma
3	Kompyuter sinfidagi 15 ta kompyuterni bir xil sozlash uchun reja (Local Group Policy, tasvir nusxasi)
4	Windows Update va dasturlarni yangilash (winget upgrade --all) bo‘yicha qo‘llanma
5	Muayyan dasturga Internetga chiqishni taqiqlovchi chiquvchi qoida yarating va tekshiring

Variant	Topshiriq
6	Android smartfon xavfsizlik sozlamalari nazorat varag'i (ekran qulfi, yangilanishlar, noma'lum manbalar)
7	Windows hodisalar jurnalida (Event Viewer) muvaffaqiyatsiz kirish urinishlarini topish bo'yicha yo'riqnoma
8	Routerning xavfsizlik sozlamalari nazorat varag'i (admin paroli, WPA3/WPA2, WPS, mehmon tarmog'i)
9	Maktab o'qituvchilari uchun "Shaxsiy noutbukni xavfsiz sozlash" bir sahifalik eslatma
10	Kompyuter sinfi uchun "Qabul qilinadigan foydalanish qoidolari" (o'quvchilar uchun 10 band)

Nazorat savollari

1. Nima uchun kundalik ish administrator hisobida bajarilmasligi kerak?
2. UAC qanday vazifani bajaradi?
3. Tarmoqlararo ekranning domen, xususiy va ommaviy profillari nimasi bilan farq qiladi?
4. Yangilanishlarni o'rnatmaslik qanday xavf tug'diradi?
5. Kompyuter sinfi xavfsizligini ta'minlashning eng muhim 5 ta qoidasini ayting.

9-AMALIY MASHG'ULOT. VEB-ILOVALARDAGI ZAIFLIK LARNI O'QUV MUHITIDA (OWASP JUICE SHOP) TAHLIL QILISH

Maqsad: OWASP Top 10 zaiflik toifalarini ataylab zaif qilib yaratilgan o'quv ilovasi misolida tanib olish va har bir toifa uchun himoya choralarini asoslash.

Kutilayotgan natijalar (TN6): tinglovchi OWASP Juice Shop ni lokal kompyuterda ishga tushiradi; ilovaning "Score Board" sahifasidagi topshiriqlarni OWASP Top 10:2025 toifalariga moslashtiradi; ikkita oddiy topshiriqni o'qituvchi rahbarligida bajaradi; har bir toifa uchun himoya choralarini jadvalda asoslaydi.

Kerakli jihozlar: kompyuter yoki virtual mashina, Docker (yoki Node.js), brauzer, M8 materiallari.

Muhim: OWASP Juice Shop – OWASP tomonidan o'qitish uchun ataylab zaif qilib yaratilgan ochiq kodli ilova. U faqat o'z kompyuteringizda (**localhost**) ishga tushiriladi. Mashg'ulotda o'rganilgan usullarni haqiqiy saytlarda, jumladan maktab yoki institut saytlarida sinash qat'iy tan taqiqlanadi va qonunga xilof (M2).

Ishni bajarish tartibi

1-qadam. Ilovani ishga tushirish. Docker o'rnatilgan bo'lsa:

```
docker pull bkimminich/juice-shop
docker run --rm -p 127.0.0.1:3000:3000 bkimminich/juice-shop
```

Brauzerda <http://localhost:3000> manzilini oching. Port faqat **127.0.0.1** ga bog‘langani uchun ilova tarmoqdagi boshqa kompyuterlardan ko‘rinmaydi.

2-qadam. Ilova bilan tanishish. Oddiy foydalanuvchi sifatida ro‘yxatdan o‘ting, mahsulotlarni ko‘ring, savatga qo‘shing, izoh qoldiring. Brauzerning dasturchi vositalari (F12) da Network bo‘limini oching va HTTP so‘rovlari, cookie va JSON javoblarni kuzating. Bu veb-ilova arxitekturasini (M8) amalda ko‘rishga yordam beradi.

3-qadam. Score Board va toifalar. Juice Shop dagi topshiriqlar ro‘yxati (“Score Board”) sahifasini toping (u ham o‘quv topshiriqlaridan biri; ko‘rsatma o‘qituvchidan olinadi). Topshiriqlar qiyinlik darajasi (1–6 yulduz) va toifalar (Injection, XSS, Broken Access Control, Sensitive Data Exposure va boshqalar) bo‘yicha guruhlangan. 1–2 yulduzli 10 ta topshiriq nomi va tavsifini o‘qib, ularni OWASP Top 10:2025 toifalariga moslashtiring.

4-qadam. O‘qituvchi rahbarligida ikkita topshiriq. O‘qituvchi ekranda 1 yulduzli ikkita topshiriqni namoyish etadi (masalan, xato xabari orqali ortiqcha ma’lumot oshkor bo‘lishi – A10/A02 toifalari va sahifada foydalanuvchi matnining HTML sifatida talqin qilinishi – A05 toifasi), tinglovchilar esa takrorlaydi. Har bir holat uchun **zaiflik sababi** va **dasturchi qanday tuzatishi kerakligi** muhokama qilinadi. Ilova o‘rnatilgan qo‘llanmasi va rasmiy “Pwning OWASP Juice Shop” kitobi topshiriqlar uchun ko‘rsatmalar beradi.

5-qadam. Tahlil jadvali. Natijalar quyidagi shaklda rasmiylashtiriladi:

№	Juice Shop topshirig‘i	OWASP Top 10:2025 toifasi	Sabab va himoya chorasi
1	Xato xabarida server texnologiyasi va ichki ma’lumotlar ko‘rinishi	A02, A10	Batafsil xatolar faqat jurnalga yoziladi; foydalanuvchiga umumiy xabar
2	Qidiruv yoki izoh maydonidagi matn HTML sifatida bajarilishi	A05 (XSS)	Chiqishni ekranlash, textContent , CSP
3	...	...	...

Mustaqil bajarish uchun variantlar

Har bir variantda ko‘rsatilgan toifa bo‘yicha: a) toifa mazmunini tushuntiring; b) Juice Shop dagi mos topshiriqni (tavsifi bo‘yicha) toping; c) zaiflik sababini va dasturchi uchun 3 ta himoya chorasini yozing; d) maktab elektron tizimi misolida xavfni tushuntiring.

Variant	OWASP Top 10:2025 toifasi
1	A01 – Kirishni boshqarishning buzilishi

Variant	OWASP Top 10:2025 toifasi
2	A02 – Xavfsizlik sozlamalaridagi xatolar
3	A03 – Dasturiy ta’minot yetkazib berish zanjiridagi nosozliklar
4	A04 – Kriptografik nosozliklar
5	A05 – Injeksiya (SQL injection)
6	A05 – Injeksiya (XSS)
7	A06 – Xavfsiz bo‘lmagan loyihalash
8	A07 – Autentifikatsiyadagi nosozliklar
9	A09 – Xavfsizlik jurnallari va ogohlantirishdagi nosozliklar
10	A10 – Istisno holatlarni noto‘g‘ri qayta ishlash

Nazorat savollari

1. Nima uchun xavfsizlik ko‘nikmalari ataylab zaif qilingan ilovalarda o‘rganiladi?
2. Juice Shop ni ishga tushirishda portni **127.0.0.1** ga bog‘lash nima uchun muhim?
3. Batafsil xato xabarlarini qanday xavf tug‘diradi?
4. XSS dan himoyaning asosiy usullari qaysilar?
5. Axloqiy xakerlik (ethical hacking) va qonunga xilof buzib kirishning farqi nimada?

10-AMALIY MASHG‘ULOT. MAKTAB UCHUN AXBOROT XAVFSIZLIGI SIYOSATI LOYIHASINI ISHLAB CHIQISH

Maqsad: oldingi mashg‘ulotlar natijalariga tayanib, umumta’lim maktabi uchun axborot xavfsizligi siyosati loyihasini ishlab chiqish va himoya qilish.

Kutilayotgan natijalar (TN10): tinglovchilar guruhi 4–6 sahifalik siyosat hujjati loyihasini tayyorlaydi; unda rollar, qoidalar, insidentlarga javob tartibi aniq yoziladi; loyiha 5 daqiqalik taqdimot bilan himoya qilinadi.

Kerakli jihozlar: matn muharriri yoki Google Docs, A1 dagi tahdid modeli, M2 dagi siyosat tuzilmasi, “Shaxsga doir ma’lumotlar to‘g‘risida” va “Kiberxavfsizlik to‘g‘risida”gi qonunlar (lex.uz).

Ishni bajarish tartibi

1-qadam. Guruhlarga bo‘linish va maktab profilini tanlash. 3–4 kishilik guruhlar maktab profilini belgilaydi: o‘quvchilar soni, kompyuterlar soni, qo‘llaniladigan tizimlar (elektron jurnal, Telegram kanal, Google Workspace va boshqalar).

2-qadam. Siyosat tuzilmasini to'ldirish. M2 dagi 12 bo'limli tuzilma asosida hujjat yoziladi. Har bir bo'lim **aniq va tekshirib bo'ladigan** qoidalaridan iborat bo'lishi kerak. Namuna:

Bo'lim	Namunaviy qoidalar
Rollar va mas'uliyat	Direktor siyosatni tasdiqlaydi; AT mas'uli (informatika o'qituvchisi) hisoblarni boshqaradi va yiliga 2 marta tekshiruv o'tkazadi; har bir xodim insidentlar haqida 1 soat ichida xabar beradi
Kirishni boshqarish va parollar	Har bir xodim shaxsiy hisobga ega; umumiy parollar taqiqlanadi; elektron jurnal va pochta uchun 2FA majburiy; parol kamida 12 belgi yoki 4 so'zli parol iborasi
Qurilmalardan foydalanish	O'quvchilar standart hisobda ishlaydi; dastur o'rnatish faqat AT mas'uli orqali; noma'lum USB disklar avval tekshiriladi
Shaxsga doir ma'lumotlar	O'quvchilar ro'yxatlari faqat aniq shaxslarga ulashiladi; suratlar ota-onalar roziligi bilan e'lon qilinadi; ma'lumotlar shaxsiy pochtaga yuborilmaydi
Zaxira nusxalash	Ma'muriyat hujjatlari har hafta 3-2-1 qoidasi bo'yicha nusxalanadi; har chorakda tiklash sinovi o'tkaziladi
Insidentlarga javob	Zararlangan kompyuter darhol tarmoqdan uziladi; AT mas'uli va direktorga xabar beriladi; jurnalga qayd etiladi; zarur hollarda vakolatli organlarga xabar beriladi
O'qitish	Xodimlar uchun yiliga 2 marta trening; o'quvchilar uchun har chorakda raqamli xavfsizlik bo'yicha sinf soati

3-qadam. Ilovalar. Hujjatga ilovalar qo'shiladi: insident haqida xabar berish shakli, kompyuter sinfi qoidalar (A8), ota-onalar roziligi shakli namunasi.

4-qadam. Himoya. Guruh 5 daqiqada siyosatning asosiy qoidalarini taqdim etadi; boshqa guruhlar "auditor" sifatida savol beradi va qoidalarining aniqligi, bajarilishi mumkinligi va qonunchilikka mosligini baholaydi.

Mustaqil bajarish uchun variantlar

Guruhlar quyidagi muassasa turlaridan biri uchun siyosat loyihasini tayyorlaydi:

Variant	Muassasa
1	Qishloqdagi 400 o'quvchili umumta'lim maktabi, 1 ta kompyuter sinfi
2	Shahardagi 1500 o'quvchili ixtisoslashtirilgan maktab, 3 ta kompyuter sinfi va Wi-Fi
3	Masofaviy va aralash ta'lim tashkil etgan maktab (Google Classroom, Zoom)
4	Xususiy o'quv markazi (to'lovlar, onlayn ro'yxatdan o'tish)
5	Maktabgacha ta'lim tashkiloti (ota-onalar bilan messenjer aloqasi, kameralar)
6	Maktab internati (o'quvchilarning shaxsiy smartfonlari va Wi-Fi)
7	IT yo'nalishidagi maktab (robototexnika, o'quvchilar serverlari)
8	Inklyuziv ta'lim maktabi (maxsus ma'lumotlar toifalari, psixolog hujjatlari)
9	Kasb-hunar maktabi (amaliyot korxonalari bilan ma'lumot almashinuvi)

Variant	Muassasa
10	Tuman maktabgacha va maktab ta'limi bo'limi (bir necha maktab ma'lumotlari)

Nazorat savollari

1. Xavfsizlik siyosati nima uchun rahbariyat tomonidan tasdiqlanishi kerak?
2. Yaxshi siyosat qoidasining belgilari qanday (aniqlik, tekshiriluvchanlik)?
3. Siyosatda qonunchilik talablari qanday aks ettiriladi?
4. Siyosat qanchalik tez-tez qayta ko'rib chiqilishi kerak?
5. Siyosat bajarilishini qanday nazorat qilish mumkin?

VI. LABORATORIYA MASHG'ULOTLARI MATERIALLARI

Laboratoriya ishlari amaliy mashg'ulotlardan farqli ravishda real xavfsizlik vositalari bilan qadamma-qadam tajriba o'tkazish, natijalarni o'lchash va hisobot shaklida rasmiylashtirishga qaratilgan. Ishlar virtual mashinada yoki o'quv USB-flesh disklarida bajariladi, shunda xato harakatlar asosiy tizim va shaxsiy ma'lumotlarga ta'sir qilmaydi.

Laboratoriya hisobotining tuzilishi

1. Ish nomi, maqsadi, foydalanilgan vositalar (versiyalari bilan).
2. Bajarilgan qadamlar va har bir qadam natijasi (screenshotlar bilan).
3. O'lchov natijalari jadvali (vaqt, hajm, xesh qiymatlar va h.k.).
4. Xulosa: nimani o'rgandim, maktab amaliyotida qanday qo'llayman.
5. Nazorat savollariga javoblar.

Baholash: hisobot va uning himoyasi amaliy ishlar uchun umumiy mezon (V bo'lim) bo'yicha baholanadi.

1-LABORATORIYA ISHI. MA'LUMOTLARNI SHIFRLASH VOSITALARI (VERACRYPT, BITLOCKER) BILAN ISHLASH

Maqsad: disk va konteynerlarni shifrlash vositalari yordamida ma'lumotlarni yo'qolish yoki o'g'irlanish holatida himoya qilish ko'nikmasini shakllantirish.

Kutilayotgan natijalar (TN8): tinglovchi VeraCrypt shifrlangan konteynerini yaratadi va ulaydi; BitLocker To Go bilan USB-flesh diskni shifrlaydi; tiklash kalitini to'g'ri saqlaydi; shifrlash vositalarini taqqoslaydi.

Kerakli jihozlar: Windows 10/11 Pro yoki Enterprise (BitLocker uchun), VeraCrypt (rasmiy sayt: veracrypt.io), o'quv USB-flesh disk (ichidagi ma'lumotlar o'chiriladi).

Shifrlash parolini yoki tiklash kalitini yo'qotish ma'lumotlarning **butunlay** yo'qolishiga olib keladi – “parolni tiklash” imkoniyati yo'q. Laboratoriyada faqat o'quv ma'lumotlari ishlatiladi.

1-qism. VeraCrypt konteyneri

1. VeraCrypt ni o'rnatish va ishga tushirish. **Create Volume → Create an encrypted file container → Standard VeraCrypt volume.**
2. Konteyner fayli joylashuvini tanlang: **D:\AX\maxfiy.hc** (fayl nomi va kengaytmasi ixtiyoriy).
3. Shifrlash algoritmi: **AES**, xesh algoritmi: **SHA-512** (standart sozlamalar).
4. Hajm: 200 MB. Parol: kamida 20 belgili parol iborasi.
5. Fayl tizimi: exFAT yoki NTFS; “Format” oynasida sichqonchani tasodifiy harakatlantirib entropiya to'plang va **Format** tugmasini bosing.

6. Asosiy oynada bo'sh disk harfini (masalan, X:) tanlang → **Select File** → konteyner faylini tanlang → **Mount** → parolni kiriting. Endi X: disk oddiy disk kabi ishlaydi.

7. Diskka o'quv fayllarini (masalan, "o'quvchilar ro'yxati" namunasi) nusxalang. **Dismount** tugmasini bosing va konteyner fayli (maxfiy.hc) ni oddiy matn muharririda ochib ko'ring – faqat tasodifiy belgilar ko'rinadi.

2-qism. BitLocker To Go bilan USB diskni shifrlash

1. USB diskni ulang. Explorer'da disk ustida o'ng tugma → **BitLocker'ni yoqish** (Turn on BitLocker).

2. **Diskni ochish uchun parol ishlatish** ni tanlang va kuchli parol kiriting.

3. **Tiklash kalitini** saqlang: faylga (boshqa diskka!) yoki chop eting. 48 raqamli tiklash kaliti parol unutilganda yagona chora.

4. Shifrlash rejimi: **Mos keluvchi rejim** (boshqa kompyuterlarda ham ochilishi uchun); "Faqat ishlatilgan joyni shifrlash".

5. Shifrlash tugagach, diskni chiqarib qayta ulang – parol so'raladi. Boshqa kompyuterda ochib ko'ring.

6. Holatni buyruq bilan tekshiring (administrator huquqida): **manage-bde -status**.

3-qism. O'lchovlar va taqqoslash

Mezon	VeraCrypt	BitLocker	7-Zip (AES-256)
Shifrlash obyekti	Konteyner, bo'lim, tizim diski	Butun disk, USB	Arxiv fayli
Platforma	Windows, Linux, macOS	Windows (Pro/Enterprise)	Asosan Windows
Ochiq kodli	Ha	Yo'q	Ha
Shaffof ishlash	Ha (ulangandan keyin)	Ha	Yo'q (har safar ochish)
Maktabda qo'llanishi	Shaxsiy ma'lumotlar konteyneri	O'qituvchi noutbuki va USB disklar	Fayllarni pochta orqali yuborish

Konteynerni yaratish vaqtini va 100 MB faylni shifrlangan va oddiy diskka nusxalash vaqtlarini o'lchab, jadvalga yozing.

Nazorat savollari

1. Disk shifrlash qanday tahdiddan himoya qiladi va qaysisidan himoya qilmaydi?

2. Konteyner ulangan holatda ma'lumotlar himoyalanganmi?

3. BitLocker tiklash kaliti qayerda saqlanishi kerak?

4. VeraCrypt da sichqoncha harakati nima uchun kerak?

5. Maktab o‘qituvchisining noutbuki nima uchun shifrlanishi kerak?

2-LABORATORIYA ISHI. ELEKTRON RAQAMLI IMZO VA SERTIFIKATLAR BILAN ISHLASH

Maqsad: ochiq kalit sertifikatlari tuzilishini o‘rganish, hujjatni imzolash va imzoni tekshirish jarayonini amalda bajarish, O‘zbekistondagi E-IMZO tizimi bilan tanishish.

Kutilayotgan natijalar (TN5): tinglovchi veb-sayt sertifikatini tahlil qiladi; OpenSSL yordamida o‘quv kalit juftligi va o‘z-o‘zini imzolagan sertifikat yaratadi; faylni imzolab tekshiradi; E-IMZO dan foydalanish tartibini tushuntiradi.

Kerakli jihozlar: brauzer, OpenSSL (Git for Windows tarkibida yoki Linux), Python 3 (**cryptography**), lex.uz dagi “Elektron raqamli imzo to‘g‘risida”gi Qonun (O‘RQ-793).

Laboratoriyada **haqiqiy** E-IMZO kalitlaringizdan foydalanmang va ularni boshqa kompyuterlarga nusxalamang. Barcha imzolash tajribalari o‘quv kalitlari bilan bajariladi.

1-qism. Veb-sayt sertifikatini tahlil qilish

Brauzerda **https://my.gov.uz** saytini oching → manzil qatoridagi belgi → “Ulanish xavfsiz” → “Sertifikat”. Quyidagilarni jadvalga yozing: kimga berilgan (Subject, CN), kim bergan (Issuer), amal qilish muddati, ochiq kalit algoritmi va uzunligi, sertifikatlar zanjiri (ildiz – oraliq – sayt sertifikati). Xuddi shu tahlilni yana ikkita sayt (**lex.uz**, **google.com**) uchun bajaring.

2-qism. OpenSSL bilan o‘quv kalitlari va imzo

```
# 1. RSA-2048 kalit juftligini yaratish
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out yopiq.pem
openssl pkey -in yopiq.pem -pubout -out ochiq.pem
# 2. O‘z-o‘zini imzolagan o‘quv sertifikati (365 kun)
openssl req -new -x509 -key yopiq.pem -out sertifikat.crt -days 365 -subj "/CN=Oquv
Oqituvchi/O=NamDPI/C=UZ"
openssl x509 -in sertifikat.crt -text -noout
# 3. Hujjatni imzolash va tekshirish
openssl dgst -sha256 -sign yopiq.pem -out buyruq.sig buyruq.txt
openssl dgst -sha256 -verify ochiq.pem -signature buyruq.sig buyruq.txt
```

Oxirgi buyruq **Verified OK** natijasini beradi. **buyruq.txt** fayliga bitta belgi qo‘shib, tekshiruvni takrorlang – **Verification failure** chiqadi. Bu ERI yaxlitlik va haqiqiylikni qanday ta’minlashini ko‘rsatadi.

3-qism. Python’da imzo

A5 dagi **zamonaviy.py** dasturining 3-qismi (RSA-PSS imzosi) yordamida hujjat imzolanadi va tekshiriladi. Hujjat o‘zgartirilganda **InvalidSignature** istisnosi ushlanadigan qilib dasturni o‘zgartiring:

```
from cryptography.exceptions import InvalidSignature
try:
    ochiq.verify(imzo, hujjat + b"!", pss, hashes.SHA256())
    print("Imzo to'g'ri")
except InvalidSignature:
    print("Imzo yaroqsiz: hujjat o'zgartirilgan yoki imzo boshqa kalitga tegishli")
```

4-qism. E-IMZO tizimi bilan tanishish

E-IMZO – O‘zbekistonda jismoniy va yuridik shaxslarga ERI kalitlarini berish va ulardan davlat axborot tizimlarida foydalanish tizimi. Rasmiy sayt (e-imzo.uz) materiallari asosida quyidagilarni yozing: ERI kalitini olish tartibi va joyi; kalit fayli qanday tashuvchida saqlanadi; kalitning amal qilish muddati; kalitni yo‘qotganda yoki parolni unutganda qanday harakat qilinadi; ERI qo‘llaniladigan 5 ta davlat xizmati. “Elektron raqamli imzo to‘g‘risida”gi Qonundan ERI kalitini saqlash bo‘yicha egasining majburiyatlarini toping.

Nazorat savollari

1. Sertifikatda qanday asosiy maydonlar bor?
2. Sertifikatlar zanjiri nima va ildiz sertifikat qayerda saqlanadi?
3. O‘z-o‘zini imzolagan sertifikatga brauzer nima uchun ishonmaydi?
4. Imzolash va tekshirishda qaysi kalitlar ishlatiladi?
5. ERI kaliti egasi qanday majburiyatlarga ega?

3-LABORATORIYA ISHI. WIRESHARK YORDAMIDA SHIFRLANMAGAN VA SHIFRLANGAN TRAFIKNI SOLISHTIRISH

Maqsad: tarmoq protokollari analizatori yordamida shifrlanmagan (HTTP) va shifrlangan (HTTPS/TLS) trafikni taqqoslash orqali shifrlashning ahamiyatini amalda ko‘rsatish.

Kutilayotgan natijalar (TN6): tinglovchi Wireshark da o‘z trafigini yozib oladi; filtrlardan foydalanadi; HTTP so‘rovida ochiq ko‘rinadigan ma’lumotlarni va TLS da shifrlangan ma’lumotlarni aniqlaydi; DNS so‘rovlarini tahlil qiladi.

Kerakli jihozlar: Wireshark (wireshark.org), brauzer, Python 3 (lokal sinov serveri uchun).

Wireshark bilan **faqat o‘z kompyuteringiz** trafigi yoziladi. Boshqa foydalanuvchilar trafigini ushlab shaxsiy hayot daxlsizligi va yozishmalar sirini buzish hisoblanadi.

Ishni bajarish tartibi

1-qadam. Lokal sinov serveri. Shifrlanmagan trafikni xavfsiz ko‘rish uchun o‘z kompyuteringizda HTTP serverini ishga tushiramiz. Quyidagi dastur oddiy kirish formasini ko‘rsatadi va yuborilgan ma’lumotlarni qabul qiladi:

```

from http.server import HTTPServer, BaseHTTPRequestHandler
from urllib.parse import parse_qs

FORMA = """<html><body><h3>O'quv kirish sahifasi (HTTP)</h3>
<form method="post"><input name="login" placeholder="login"><br>
<input name="parol" type="password" placeholder="parol"><br>
<button>Kirish</button></form></body></html>"""

class Ishlovchi(BaseHTTPRequestHandler):
    def do_GET(self):
        self.send_response(200)
        self.send_header("Content-Type", "text/html; charset=utf-8")
        self.end_headers()
        self.wfile.write(FORMA.encode("utf-8"))

    def do_POST(self):
        uzunlik = int(self.headers.get("Content-Length", 0))
        malumot = parse_qs(self.rfile.read(uzunlik).decode("utf-8"))
        self.send_response(200)
        self.send_header("Content-Type", "text/html; charset=utf-8")
        self.end_headers()
        javob = f"<p>Qabul qilindi: {len(malumot)} ta maydon</p>"
        self.wfile.write(javob.encode("utf-8"))

# faqat lokal kompyuterda (127.0.0.1) ishlaydi
HTTPServer(("127.0.0.1", 8080), Ishlovchi).serve_forever()

```

Dasturni ishga tushiring va brauzerda <http://127.0.0.1:8080> manzilini oching.

2-qadam. Trafikni yozish. Wireshark da **Adapter for loopback traffic capture** (Windows, Npcap) yoki **lo** (Linux) interfeysini tanlang va yozishni boshlang. Formaga o'quv login va parolini (**test_oqituvchi / Sinov-Parol-123**) kiritib yuboring. Yozishni to'xtating.

3-qadam. HTTP trafigini tahlil qilish. Filtr: **http.request.method == "POST"**. Paketni tanlab, **HTML Form URL Encoded** qismini oching – login va parol ochiq matnda ko'rinadi. **Follow** → **HTTP Stream** orqali butun so'rov va javobni ko'ring.

4-qadam. HTTPS trafigi. Yangi yozuvni Wi-Fi yoki Ethernet interfeysida boshlang va istalgan HTTPS saytni (masalan, <https://lex.uz>) oching. Filtr: **tls.Client Hello** paketida Server Name Indication (SNI) maydonida sayt nomi ko'rinadi, lekin **Application Data** paketlari mazmuni shifrlangan – sahifa matni, cookie va parollar ko'rinmaydi. Filtr **dns** orqali qaysi domen nomlari so'ralganini ham ko'ring.

5-qadam. Natijalar jadvali.

Nima ko'rinadi?	HTTP	HTTPS (TLS)
Server IP manzili va porti	Ha	Ha

Nima ko‘rinadi?	HTTP	HTTPS (TLS)
Sayt domen nomi	Ha (Host sarlavhasi)	Ha (DNS va SNI orqali)
So‘ralgan sahifa yo‘li (URL)	Ha	Yo‘q
Login va parol	Ha	Yo‘q
Cookie va sessiya	Ha	Yo‘q
Sahifa mazmuni	Ha	Yo‘q
Trafik hajmi va vaqti	Ha	Ha

Xulosa: HTTPS mazmunni himoya qiladi, ammo **qaysi saytga** ulanilgani (metama’lumotlar) tarmoq administratoriga yoki provayderga ko‘rinib qolishi mumkin.

Nazorat savollari

1. Nima uchun parol HTTP da ochiq ko‘rindi?
2. TLS da qaysi ma’lumotlar shifrlanmaydi?
3. DNS so‘rovlari qanday ma’lumotni oshkor qiladi?
4. Ochiq Wi-Fi tarmog‘ida HTTP saytga kirish qanday xavf tug‘diradi?
5. Wireshark dan qonuniy foydalanish chegaralari qanday?

4-LABORATORIYA ISHI. ZAXIRA NUSXA OLIISH VA MA’LUMOTLARNI TIKLASH STRATEGIYASINI AMALDA QO‘LLASH

Maqsad: 3-2-1 qoidasi asosida zaxira nusxalash strategiyasini ishlab chiqish, OS vositalari va skript yordamida nusxa olish hamda tiklashni sinab ko‘rish.

Kutilayotgan natijalar (TN9): tinglovchi maktab ma’muriyati hujjatlari uchun zaxira strategiyasini (RPO, RTO, jadval) tuzadi; Windows “Fayl tarixi” yoki **robocopy** bilan nusxa oladi; Python skripti bilan sanali arxiv yaratadi va xesh orqali tekshiradi; faylni tiklash sinovini bajaradi.

Kerakli jihozlar: Windows kompyuter yoki virtual mashina, tashqi disk yoki USB-flesh disk, bulutli disk (Google Drive), Python 3.

Ishni bajarish tartibi

1-qadam. Strategiya. Quyidagi jadvalni maktab ma’muriyati uchun to‘ldiring:

Parametr	Qiymat (namuna)
Nusxalanadigan ma’lumotlar	D:\Maktab\Buyruqlar, D:\Maktab\Kadrlar, D:\Maktab\Hisobotlar
RPO	1 kun (bir kunlik ishdan ko‘p yo‘qotishga yo‘l qo‘yilmaydi)
RTO	4 soat
Nusxa turlari va jadval	Har kuni ortib boruvchi (Fayl tarixi), har juma to‘liq arxiv

Parametr	Qiymat (namuna)
3-2-1	1) asl fayllar; 2) tashqi disk (har juma uziladi va seyfda saqlanadi); 3) shifrlangan arxiv bulutli diskda
Tiklash sinovi	Har oyda tasodifiy 3 ta faylni tiklash
Mas'ul	AT mas'uli, nazorat – direktor o‘rinbosari

2-qadam. Windows vositalari. Sozlamalar (yoki Boshqaruv paneli) → **Fayl tarixi** (File History): tashqi diskni tanlang, papkalarni qo‘shing, davriylikni belgilang va birinchi nusxani oling. Muqobil sifatida **robocopy** buyrug‘i:

```
robocopy D:\Maktab E:\Zaxira\Maktab /MIR /R:1 /W:1 /LOG:E:\Zaxira\log.txt
```

/MIR kaliti manba papkani ko‘zgu kabi takrorlaydi – manbada o‘chirilgan fayllar zaxirada ham o‘chiriladi. Shuning uchun u yagona zaxira usuli bo‘la olmaydi; versiyali nusxalar (Fayl tarixi, sanali arxivlar) ham kerak.

3-qadam. Sanali arxiv va tekshiruv skripti. Quyidagi dastur papkadan sanali ZIP arxiv yaratadi, uning SHA-256 xeshini yozadi va eng so‘nggi 7 ta arxivni qoldirib, eskilarini o‘chiradi:

```
import hashlib, os, shutil
from datetime import datetime

MANBA = "Maktab" # nusxalanadigan papka
ZAXIRA = "Zaxira" # tashqi disk yoki boshqa joy
SAQLASH_SONI = 7 # nechta oxirgi arxiv saqlanadi

def sha256(yol):
    h = hashlib.sha256()
    with open(yol, "rb") as f:
        for qism in iter(lambda: f.read(65536), b''):
            h.update(qism)
    return h.hexdigest()

os.makedirs(ZAXIRA, exist_ok=True)
nom = os.path.join(ZAXIRA, "maktab_" + datetime.now().strftime("%Y-%m-%d_%H%M%S"))
arxiv = shutil.make_archive(nom, "zip", MANBA)
with open(arxiv + ".sha256", "w") as f:
    f.write(sha256(arxiv))
print("Yaratildi:", os.path.basename(arxiv))

arxivlar = sorted(a for a in os.listdir(ZAXIRA) if a.endswith(".zip"))
for eski in arxivlar[:-SAQLASH_SONI]:
    os.remove(os.path.join(ZAXIRA, eski))
    os.remove(os.path.join(ZAXIRA, eski + ".sha256"))
    print("O'chirildi:", eski)
```

4-qadam. Tiklash sinovi. Manba papkadan bitta faylni o‘chiring va bittasini o‘zgartiring. Fayl tarixi (“Shaxsiy fayllarni tiklash”) va ZIP arxivdan ularni tiklang.

Tiklash vaqtini o‘lchang va RTO bilan solishtiring. Arxiv xeshini **.sha256** fayldagi qiymat bilan solishtirib, arxiv buzilmaganini tekshiring.

5-qadam. Bayonnoma. Tiklash sinovi bayonnomasini rasmiylashtiring: sana, tiklangan fayllar, manba (qaysi nusxadan), sarflangan vaqt, natija, aniqlangan muammolar.

Nazorat savollari

1. RPO va RTO zaxira strategiyasini qanday belgilaydi?
2. Nima uchun bitta tashqi disk ishonchli zaxira emas?
3. To‘lov talab qiluvchi dasturdan himoya uchun zaxira qanday saqlanishi kerak?
4. Bulutli diskdagi zaxirani nima uchun shifrlash kerak?
5. Tiklash sinovi nima uchun majburiy?

5-LABORATORIYA ISHI. YAKUNIY LOYIHA: O‘QUVCHILAR UCHUN “RAQAMLI XAVFSIZLIK” DARS VA TRENING MATERIALLARINI TAYYORLASH VA HIMOYA QILISH

Maqsad: fan davomida egallangan bilim va ko‘nikmalarni umumlashtirib, o‘quvchilar (yoki o‘qituvchilar va ota-onalar) uchun raqamli xavfsizlik bo‘yicha dars yoki trening materiallarini ishlab chiqish va himoya qilish.

Kutilayotgan natijalar (TN10): tinglovchilar guruhi tanlangan auditoriya uchun 40–45 daqiqalik dars ishlanmasi, taqdimot, kamida bitta interaktiv topshiriq va eslatma (6-mustaqil topshiriq) tayyorlaydi; darsdan 10 daqiqalik fragmentni namoyish etib himoya qiladi.

Kerakli jihozlar: taqdimot dasturi, Canva, Kahoot/Quizizz yoki LearningApps, M10 materiallari, CS50 Cybersecurity [12] va CISA [9] resurslari.

Loyiha mavzulari (guruhlar tanlaydi)

№	Mavzu	Auditoriya
1	“Parolim – qal’am”: kuchli parol va 2FA	5–6-sinflar
2	“Fishing ovchisi”: soxta xabarlarini aniqlash	7–8-sinflar
3	“Raqamli izim”: maxfiylik sozlamalari va obro‘	8–9-sinflar
4	“Kiberbullingga yo‘q!”: Internetda hurmat va yordam so‘rash	5–7-sinflar
5	“Shifrlash sirlari”: Sezar shifridan HTTPS gacha	9–11-sinflar
6	“Dipfeyk va soxta xabarlar”: axborotni tekshirish	9–11-sinflar
7	“Maktabimiz xavfsizligi”: o‘qituvchilar uchun trening	Pedagoglar
8	“Farzandingiz Internetda”: ota-onalar uchun trening	Ota-onalar

Dars ishlanmasining tuzilishi

Bosqich	Vaqt	Mazmun va metod
Tashkiliy qism va motivatsiya	3 daq	Hayotiy vaziyat (qisqa video yoki keys), muammoli savol
Bilimlarni faollashtirish	5 daq	“BBB” jadvali yoki aqliy hujum
Yangi mavzu	12 daq	Interaktiv tushuntirish, misollar, taqdimot
Amaliy topshiriq	15 daq	Juftlikda yoki guruhda: parollarni baholash, fishing xatlarini topish, Sesar shifri o‘yini
Mustahkamlash	5 daq	Kahoot/Quizizz viktorinasi
Xulosa va refleksiya	3 daq	“Bugun men ... ni o‘rgandim va ... qilaman”; eslatma tarqatish
Uyga vazifa	2 daq	Oilada akkauntlarni tekshirish, ota-onalarga eslatmani tushuntirish

Himoya tartibi

1. Guruh 2 daqiqada dars maqsadi, auditoriya va natijalarni taqdim etadi.
2. 10 daqiqalik fragmentni boshqa tinglovchilarni “o‘quvchi” sifatida jalb qilib o‘tkazadi.
3. 3 daqiqa savol-javob va hamkasblar baholashi.

Baholash mezonlari

Mezon	Ball	Izoh
Mazmunning ilmiy to‘g‘riligi va dolzarbligi	25	Atamalar va maslahatlar to‘g‘ri, eskirgan tavsiyalar yo‘q
Auditoriya yoshiga mosligi	20	Til, misollar va topshiriqlar mos
Interaktivlik va amaliy yo‘nalganlik	20	O‘quvchilar faol, aniq harakatlar o‘rgatiladi
Materiallar sifati (taqdimot, eslatma, test)	20	Dizayn, o‘qilishi, manbalar ko‘rsatilgan
Himoya va savollarga javob	15	Asoslangan javoblar, jamoaviy ish
Jami	100	86–100 – “5”; 71–85 – “4”; 55–70 – “3”; 55 dan kam – “2”

Nazorat savollari

1. Raqamli xavfsizlikni o‘qitishda qo‘rqitish yondashuvi nima uchun samarasiz?
2. Tanlagan auditoriyangizning asosiy xavflari qaysilar?
3. Darsingizda qaysi interaktiv metodlardan foydalandingiz va nima uchun?
4. Dars natijalarini qanday baholaysiz?

5. Ota-onalarni bu jarayonga qanday jalb qilish mumkin?

VII. MUSTAQIL TA'LIM TOPSHIRIQLARI

Mustaqil ta'lim topshiriqlari auditoriya mashg'ulotlarida olingan bilimlarni chuqurlashtirish, me'yoriy hujjatlar va xalqaro manbalar bilan ishlash hamda maktab amaliyoti uchun tayyor materiallar yaratishga qaratilgan. Topshiriqlar variativ: har bir topshiriq uchun bir nechta variant berilgan va variant tinglovchining jurnalidagi tartib raqami bo'yicha aniqlanadi. 3- va 6-topshiriqlar kichik guruhlarda (3–4 kishi) hamkorlikda bajariladi – bu mustaqil ish topshiriqlarining 1/3 qismini tashkil etadi.

Umumiy talablar

- matnli ishlar: Times New Roman, 14 pt, 1,5 interval; manbalar ro'yxati va havolalar majburiy;
- me'yoriy hujjatlarga havola lex.uz dagi amaldagi tahrir bo'yicha beriladi (hujjat raqami va sanasi bilan);
- sun'iy intellekt vositalaridan foydalanilgan bo'lsa, bu ochiq ko'rsatiladi va barcha faktlar birlamchi manba bo'yicha tekshiriladi;
- ko'chirmachilik (plagiat) aniqlansa, topshiriq "2" bilan baholanadi.

1-topshiriq. "Kiberxavfsizlik to'g'risida"gi Qonunning asosiy qoidalari bo'yicha tahliliy referat (individual)

Maqsad: kiberxavfsizlik sohasidagi milliy qonunchilik bilan chuqur tanishish va uni ta'lim muassasasi faoliyatiga tatbiq etish.

Hajmi: 8–10 sahifa. **Bog'liq mavzu:** M2.

Tuzilishi: kirish (qonunning qabul qilinish sabablari) → asosiy tushunchalar → kiberxavfsizlik subyektlari va ularning vakolatlari → kiberinsidentlarga javob berish tartibi → ta'lim muassasalari uchun ahamiyati → xulosa va takliflar → manbalar.

Variant	Tahlil yo'nalishi
1	Qonundagi asosiy tushunchalar va ularning xalqaro standartlardagi (ISO/IEC 27000, NIST) atamalar bilan taqqoslanishi
2	Kiberxavfsizlik sohasidagi vakolatli davlat organi va subyektlarning huquq va majburiyatlari
3	Muhim axborot infratuzilmasi obyektlarini himoya qilish talablari
4	Kiberinsidentlar haqida xabar berish va ularga javob qaytarish tartibi
5	"Kiberxavfsizlik to'g'risida"gi va "Shaxsga doir ma'lumotlar to'g'risida"gi qonunlarning o'zaro bog'liqligi
6	Qonun talablari asosida maktab uchun majburiyatlar ro'yxatini ishlab chiqish
7	O'zbekiston va boshqa bir davlat (Qozog'iston, Estoniya yoki boshqa) kiberxavfsizlik qonunchiligini taqqoslash

Variant	Tahlil yo‘nalishi
8	Jinoyat kodeksidagi axborot texnologiyalari sohasidagi jinoyatlar va qonunning o‘zaro bog‘liqligi

2-topshiriq. Zararli dasturlar bo‘yicha taqdimot (individual)

Maqsad: zararli dasturlarning turi, tarqalish usuli va himoya choralari tizimli bayon qilish.

Hajmi: 12–15 slayd, 7–10 daqiqalik chiqish. **Bog‘liq mavzular:** M3, A7.

Tarkibi: zararli dastur turi va tarixi → ishlash mexanizmi (umumiy darajada) → tarqalish yo‘llari → mashhur hodisa misoli va oqibatlar → aniqlash belgilari → himoya choralari → maktab uchun tavsiyalar → manbalar.

Variant	Mavzu
1	Fayl viruslari va makroviruslar
2	Chuvalchanglar: Morris (1988) dan zamonaviy chuvalchanglarga
3	Trojanlar va masofadan boshqarish dasturlari (RAT)
4	To‘lov talab qiluvchi dasturlar: WannaCry hodisasi va saboqlar
5	Josus dasturlar va keyloggerlar
6	Botnetlar va DDoS hujumlari
7	Mobil qurilmalar uchun zararli dasturlar (Android .apk fayllari)
8	Parol o‘g‘rilari (stealer) va “cheat”/“krek” orqali tarqalish
9	Rootkit va fayl qoldirmaydigan (fileless) zararli dasturlar
10	Kriptomaynerlar va brauzer orqali yashirin mayning

3-topshiriq. Ijtimoiy muhandislik hujumlariga doir real keyslar to‘plami (kichik guruhda)

Maqsad: ijtimoiy muhandislik hujumlarining real holatlarini to‘plash, tahlil qilish va o‘qitish uchun keyslar to‘plamini yaratish.

Hajmi: guruh uchun 8–10 ta keys. **Bog‘liq mavzular:** M4, A3.

Har bir keysning tuzilishi: vaziyat bayoni (shaxsiy ma’lumotlar anonimlashtirilgan) → qo‘llanilgan usul va psixologik omil → qurbonning xatosi → oqibatlar → to‘g‘ri harakat → muhokama uchun 2–3 savol.

Rollar taqsimoti: koordinator; manbalar bo‘yicha mas’ul (rasmiy xabarlar, CISA, bank ogohlantirishlari); muharrir; dizayner (to‘plamni bir xil shaklga keltiradi). Har bir a’zoning hissasi hujjat tarixida yoki alohida jadvalda ko‘rsatiladi.

Variant	Keyslar yo‘nalishi
1	Bank kartalari va to‘lov tizimlari nomidan firibgarlik
2	Messenjer akkauntlarini o‘g‘irlash (SMS-kod, “ovoz berish” havolalari)

Variant	Keyslar yo‘nalishi
3	Tashkilot rahbari nomidan soxta topshiriqlar (BEC)
4	O‘quvchilar va o‘smirlarga qaratilgan firibgarliklar (o‘yinlar, sovg‘alar)
5	Telefon orqali firibgarlik (vishing) va “qarindosh muammoda” ssenariylari
6	Soxta ish va stipendiya takliflari

4-topshiriq. Shifrlash algoritmlari bo‘yicha qiyosiy jadval (individual)

Maqsad: klassik va zamonaviy kriptografik algoritmlarni tizimlashtirish.

Hajmi: jadval va 1–2 sahifalik tahliliy izoh. **Bog‘liq mavzular:** M6, A4–A6.

Jadval ustunlari: algoritmi → turi (klassik / simmetrik / asimmetrik / xesh) → yaratilgan yili va muallifi → kalit (yoki xesh) uzunligi → ishlash tamoyili (1–2 jumla) → afzalliklari → kamchiliklari yoki ma’lum hujumlar → hozirgi holati (tavsiya etiladi / eskirgan) → qo‘llanish sohasi.

Variant	Algoritmlar to‘plami (kamida 8 ta)
1	Sezar, Atbash, Vijnier, Playfair, DES, 3DES, AES, RSA
2	AES, ChaCha20, Blowfish, Twofish, RSA, ECC, Diffi–Xellman, ElGamal
3	MD5, SHA-1, SHA-256, SHA-512, SHA-3, BLAKE2, bcrypt, Argon2
4	RSA, DSA, ECDSA, Ed25519 imzo algoritmlari va ularning ERI da qo‘llanishi
5	Wi-Fi shifrlash protokollari: WEP, WPA (TKIP), WPA2 (AES-CCMP), WPA3 (SAE) va TLS 1.2/1.3
6	Kvantdan keyingi kriptografiya: NIST tomonidan standartlashtirilgan algoritmlar va an’anaviy algoritmlar

5-topshiriq. OWASP Top-10 zaifliklari bo‘yicha qisqacha qo‘llanma (individual)

Maqsad: veb-ilovalar zaifliklari va himoya choralari bo‘yicha o‘qituvchilar va boshlovchi dasturchilar uchun qo‘llanma yaratish.

Hajmi: 6–8 sahifa. **Bog‘liq mavzular:** M8, A9.

Tuzilishi: OWASP loyihasi haqida → OWASP Top 10:2025 ro‘yxati (jadval) → variantdagi uchta toifa bo‘yicha batafsil: mazmuni, sabablari, oqibatlari, himoya choralari (xavfsiz kod namunasi bilan) → maktab veb-sayti va elektron tizimlari uchun nazorat varag‘i → manbalar (owasp.org).

Variant	Batafsil yoritiladigan toifalar
1	A01, A05, A07
2	A02, A04, A09
3	A03, A06, A08
4	A01, A02, A10

Variant	Batafsil yoritiladigan toifalar
5	A04, A05, A07
6	A03, A08, A09
7	A05 (SQL injection va XSS), A06
8	A01, A07, A10

Qo‘llanmada faqat himoya yo‘nalishidagi ma’lumotlar beriladi: hujum usullari umumiy darajada tushuntiriladi, real saytlarga qarshi qo‘llanadigan buyruqlar yoki ko‘rsatmalar keltirilmaydi.

6-topshiriq. O‘quvchilar va ota-onalar uchun “Internetda xavfsiz yurish” eslatmasi (kichik guruhda)

Maqsad: maqsadli auditoriya uchun tushunarli, amaliy va vizual jihatdan sifatli raqamli xavfsizlik materiali yaratish.

Hajmi: 2 sahifalik bosma eslatma (yoki buklet) + 1 ta ijtimoiy tarmoq posti yoki qisqa video (60–90 soniya). **Bog‘liq mavzular:** M10, L5.

Talablar: 8–12 ta aniq maslahat (“nima qilish kerak” shaklida); yoshga mos til va tasvirlar; yordam uchun murojaat qilish yo‘llari; QR-kod orqali qo‘shimcha ishonchli manbaga havola; materiallar mualliflik huquqiga rioya qilgan holda tayyorlanadi.

Variant	Auditoriya va urg‘u
1	1–4-sinf o‘quvchilari: shaxsiy ma’lumot, notanishlar, kattalarga aytish
2	5–7-sinf o‘quvchilari: parollar, o‘yinlar va firibgarlik, kiberbulling
3	8–11-sinf o‘quvchilari: raqamli iz, 2FA, dipfeyklar, qonuniy javobgarlik
4	Ota-onalar: bolaning qurilmalarini sozlash, ota-ona nazorati, muloqot
5	O‘qituvchilar: o‘quvchilar ma’lumotlari, onlayn darslar, akkauntlar xavfsizligi
6	Bobo-buvilar va katta yoshdagilar: telefon firibgarligi, SMS-kodlar

Mustaqil ta’lim topshiriqlarini baholash mezonlari

Baho	Mezon
5	Topshiriq talablarga to‘liq mos; mazmun ilmiy aniq va dolzarb; me’yoriy hujjatlar va manbalar to‘g‘ri ko‘rsatilgan; maktab amaliyoti bilan bog‘langan; mustaqil xulosalar bor; himoyada savollarga to‘liq javob berilgan; guruh ishida har bir a’zoning hissasi aniq
4	Topshiriq asosan to‘liq, 1–2 ta kichik kamchilik (manbalar to‘liq emas, misollar kam)
3	Topshiriq qisman bajarilgan; mazmunda noaniqliklar yoki eskirgan ma’lumotlar bor; xulosalar umumiy
2	Topshiriq bajarilmagan, mavzuga mos emas yoki ko‘chirilgan

VIII. KEYSLAR BANKI

Keyslar ma'ruza va amaliy mashg'ulotlarda "Keys-stadi" metodi (III bo'lim) asosida tahlil qilinadi. Har bir keys uchun tinglovchilar: 1) aktiv, tahdid va zaiflikni aniqlaydi; 2) qaysi CIA xususiyati buzilganini belgilaydi; 3) darhol ko'riladigan choralarni; 4) kelajakda takrorlanmasligi uchun choralarni taklif qiladi. Keyslardagi barcha nomlar va vaziyatlar o'ylab topilgan.

1-keys. "Umumiy parol" (M1, M5)

Maktabning kompyuter sinfidagi 15 ta kompyuterning barchasida bitta **admin** hisobi va bitta parol (**maktab2020**) ishlatiladi. Parol informatika xonasi doskasining burchagida yozilgan. Bir kuni 9-sinf o'quvchisi o'qituvchi kompyuteriga kirib, nazorat ishi variantlarini telefoniga suratga oladi.

Savollar: 1. Qaysi zaifliklar mavjud? 2. CIA ning qaysi xususiyati buzildi? 3. Hodisadan keyin darhol nima qilish kerak? 4. Qanday tashkiliy va texnik choralar zarur?

Yechim yo'nalishi: har bir o'quvchi va o'qituvchi uchun alohida standart hisoblar, administrator hisobi faqat AT mas'ulida; parollarni ochiq yozmaslik; o'qituvchi kompyuterini qulflash; nazorat ishlari fayllarini shifrlangan konteynerda saqlash; nazorat ishi variantlarini almashtirish; o'quvchi bilan tarbiyaviy suhbat va qonuniy javobgarlik haqida tushuntirish.

2-keys. "Ochiq jadval" (M2, M10)

Sinf rahbari ota-onalar bilan aloqa uchun o'quvchilar ro'yxatini (F.I.Sh., tug'ilgan sana, manzil, ota-onalar telefon raqamlari) Google Sheets da tuzib, havolasini ota-onalar Telegram guruhiga "havolasi bor har kim ko'ra oladi" rejimida yuboradi. Guruhda 120 kishi bor, bir necha oydan keyin ota-onalarga notanish kishilardan "kredit" takliflari kela boshlaydi.

Savollar: 1. Qaysi qonun talablari buzilgan? 2. Bu holatda subyekt, mulkdor va operator kimlar? 3. Darhol qanday choralar ko'rish kerak? 4. Ota-onalar bilan xavfsiz aloqa qanday tashkil etiladi?

Yechim yo'nalishi: havola orqali ulashishni darhol o'chirish, kirish tarixini tekshirish; ma'muriyatga xabar berish; zarur minimal ma'lumotlarni yig'ish; faqat aniq shaxslarga ulashish; xodimlarni "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun bo'yicha o'qitish.

3-keys. "Shoshilinch buyruq" (M4)

Juma kuni kechqurun o'qituvchilarga "direktor" nomidan xat keladi: "Vazirlik tekshiruvi! Ilovadagi jadvalni ochib, o'z ma'lumotlaringizni 1 soat ichida

to'ldiring." Ilova – **Tekshiruv_jadvali.xlsm**. Uchta o'qituvchi faylni ochib, "Kontentni yoqish" tugmasini bosadi. Dushanba kuni ularning kompyuterlarida fayllar ochilmay qoladi.

Savollar: 1. Qanday ijtimoiy muhandislik usullari qo'llanilgan? 2. Qaysi belgilar shubha uyg'otishi kerak edi? 3. Insidentga javob bosqichlarini rejalashtiring. 4. Bunday hodisalarni oldini olish uchun nima qilish kerak?

Yechim yo'nalishi: avtoritet va shoshilinchlik omillari, makrosli ilova; zararlangan kompyuterlarni tarmoqdan uzish, tarqalish ko'lamini aniqlash, zaxiradan tiklash; makroslarni markazlashgan holda o'chirish; ikki kanalli tekshiruv qoidasi; o'quv fishing mashqlari.

4-keys. "Elektron jurnalda baholar" (M5, M9)

O'qituvchi elektron jurnal paroli sifatida tug'ilgan yilini ishlatadi va uni bir nechta saytda qo'llaydi. Chorak oxirida bir necha o'quvchining baholari o'zgartirilgani aniqlanadi. Tizim jurnalida o'zgartirishlar o'qituvchi hisobidan, kechasi soat 23:40 da kiritilgani ko'rinadi.

Savollar: 1. Hujumchi parolni qanday bilishi mumkin edi? 2. Tizim jurnali qaysi xususiyatni ta'minladi? 3. Yaxlitlikni qanday tiklash mumkin? 4. Qanday texnik choralar bunday hodisaning oldini oladi?

Yechim yo'nalishi: taxmin qilinadigan va takrorlanuvchi parol, credential stuffing yoki tanish odam tomonidan taxmin; hisobdorlik (audit); qog'oz manbalar yoki zaxira asosida baholarni tiklash; noyob uzun parol, parol menejeri, 2FA, g'ayrioddiy vaqtdagi kirishlar haqida ogohlantirish.

5-keys. "Fayllar shifrlandi" (M3, M9)

Maktab buxgalteriyasi kompyuterida ekranda to'lov talabi chiqadi: barcha hujjatlar shifrlangan, 72 soat ichida kriptovalyutada to'lov talab qilinmoqda. Zaxira nusxa shu kompyuterga doimiy ulangan tashqi diskda saqlangan va u ham shifrlangan. Kompyuterda OS yangilanishlari bir yildan beri o'rnatilmagan.

Savollar: 1. Qaysi xatolar hodisaga sabab bo'ldi? 2. To'lov to'lash kerakmi? Asoslang. 3. Hodisaga javob bosqichlarini tuzing. 4. To'g'ri zaxira strategiyasini taklif qiling.

Yechim yo'nalishi: yangilanishlarning yo'qligi, doimiy ulangan zaxira, ehtimoliy admin huquqlari; to'lov kafolat bermaydi va jinoyatchilarni rag'batlantiradi – mutaxassislar va vakolatli organlarga murojaat; kompyuterni ajratish, qayta o'rnatish; 3-2-1 qoidasi, oflayn nusxa, tiklash sinovlari.

6-keys. “Bepul Wi-Fi” (M7)

O‘qituvchi kafeda “Free_WiFi_Cafe” nomli parolsiz tarmoqqa ulanib, maktab pochta-siga va elektron jurnalga kiradi. Kafedagi tarmoqlardan biri soxta (hujumchi tomonidan yaratilgan) bo‘lgani keyinroq ma’lum bo‘ladi.

Savollar: 1. Qanday hujum turi amalga oshirilgan bo‘lishi mumkin? 2. HTTPS bunday holatda qanday himoya beradi va qaysi xavflar saqlanib qoladi? 3. Ochiq Wi-Fi da xavfsiz ishlash qoidalarini tuzing.

Yechim yo‘nalishi: soxta kirish nuqtasi va “o‘rtadagi odam” hujumi; HTTPS mazmunni himoya qiladi, ammo soxta sahifalar va sertifikat ogohlantirishlarini e‘tiborsiz qoldirish xavfli; mobil Internet yoki ishonchli VPN, 2FA, sertifikat ogohlantirishlarida to‘xtash.

7-keys. “Kiberbulling” (M10)

7-sinf o‘quvchisining surati uning roziligisiz tahrirlanib, masxara qiluvchi izohlar bilan sinf chatiga va ijtimoiy tarmoqqa joylanadi. O‘quvchi darslarga kelmay qo‘yadi. Ota-ona informatika o‘qituvchisi va sinf rahbariga murojaat qiladi.

Savollar: 1. O‘qituvchi qanday ketma-ketlikda harakat qilishi kerak? 2. Dalillar qanday saqlanadi? 3. Kimlar jarayonga jalb qilinadi? 4. Sinfda qanday profilaktik ishlar olib boriladi?

Yechim yo‘nalishi: o‘quvchini tinglash va qo‘llab-quvvatlash; skrinshotlar va havolalarni saqlash; platformaga shikoyat qilish; sinf rahbari, maktab psixologi, ma‘muriyat va ota-onalarni jalb etish, zarur hollarda vakolatli organlarga murojaat; raqamli odob va empatiya bo‘yicha sinf soatlari, aniq maktab qoidalari.

8-keys. “Maktab sayti o‘zgardi” (M8)

Maktab veb-saytining bosh sahifasida begona matn va havolalar paydo bo‘ladi. Sayt bir necha yil oldin tayyor CMS asosida yaratilgan, administrator paroli **admin123**, pluginlar hech qachon yangilanmagan. Saytni qo‘llab-quvvatlovchi mas‘ul shaxs yo‘q.

Savollar: 1. OWASP Top 10:2025 ning qaysi toifalari bu holatga mos keladi? 2. Saytni qanday tiklash kerak? 3. Kelajakda qanday tashkiliy va texnik choralar zarur?

Yechim yo‘nalishi: A02 (sozlashdagi xatolar), A03 (yetkazib berish zanjiri, eskirgan pluginlar), A07 (kuchsiz parol); saytni vaqtincha o‘chirish, toza zaxiradan tiklash, barcha parollarni almashtirish, CMS va pluginlarni yangilash; mas‘ul shaxs tayinlash, 2FA, muntazam yangilash va zaxira nusxalash.

9-keys. “Yo‘qolgan noutbuk” (M6, L1)

Direktor o‘rinbosarining noutbuki taksida qoldirilib yo‘qoladi. Unda o‘quvchilar va xodimlar ro‘yxatlari, buyruqlar va attestatsiya hujjatlari bor edi. Noutbukka faqat oddiy Windows paroli o‘rnatilgan, disk shifrlanmagan.

Savollar: 1. Oddiy Windows paroli nima uchun ma’lumotlarni himoya qilmaydi? 2. Qanday zarar yetishi mumkin? 3. Hodisadan keyin darhol nima qilinadi? 4. Qanday choralar oldindan ko‘rilishi kerak edi?

Yechim yo‘nalishi: diskni boshqa kompyuterga ulab o‘qish mumkin; shaxsga doir ma’lumotlarning sizib chiqishi xavfi; akkauntlar parollarini almashtirish, bulutli seanslarni tugatish, ma’muriyatga xabar berish; BitLocker bilan disk shifrlash, zaxira nusxa, qurilmani masofadan topish va bloklash funksiyalari.

10-keys. “Ovoz berish havolasi” (M4, M5)

O‘quvchi sinfdoshidan “tanlovda ovoz bering” degan havola oladi, ochilgan sahifada telefon raqami va keyin SMS orqali kelgan kodni kiritadi. Bir necha daqiqadan so‘ng uning messenjer akkaunti boshqa qurilmadan boshqarila boshlaydi va uning nomidan barcha kontaktlarga xuddi shu havola yuboriladi.

Savollar: 1. Hujum qanday ishladi? 2. Nima uchun xabar ishonchli tuyuldi? 3. Akkauntni qanday tiklash kerak? 4. O‘quvchilarga qanday qoidalarini o‘rgatish kerak?

Yechim yo‘nalishi: fishing sahifasi orqali tasdiqlash kodini qo‘lga kiritish; tanish odamdan kelgan xabar – ishonch omili; rasmiy ilova orqali boshqa seanslarni tugatish, qayta kirish, 2 bosqichli parolni yoqish, kontaktlarni ogohlantirish; “SMS-kodni hech qayerga kiritmaslik va hech kimga aytmasslik” qoidasi.

IX. GLOSSARIY

Glossariyda fanning asosiy atamaları o‘zbek, ingliz va rus tillarida izohi bilan keltirilgan. Atamalar o‘zbek alifbosi tartibida joylashtirilgan; raqam bilan boshlanuvchi atamalar ro‘yxat oxirida berilgan.

№	O‘zbekcha	Inglizcha	Ruscha	Izoh
1	AES	Advanced Encryption Standard	Стандарт шифрования AES	2001-yilda qabul qilingan, 128 bitli bloklar va 128/192/256 bitli kalitlar bilan ishlaydigan simmetrik shifr
2	Aktiv	Asset	Актив	Tashkilot uchun qadrli bo‘lgan axborot, dastur, qurilma, xizmat yoki inson
3	Antivirus	Antivirus	Антивирус	Zararli dasturlarni aniqlash, bloklash va yo‘q qilish dasturi
4	Asimmetrik shifrlash	Asymmetric encryption	Асимметричное шифрование	Ochiq va yopiq kalitlar juftligidan foydalanuvchi shifrlash
5	Autentifikatsiya	Authentication	Аутентификация	Foydalanuvchi yoki obyekt haqiqiyligini tekshirish
6	Autentiklik	Authenticity	Подлинность	Axborot yoki foydalanuvchi o‘zini kim deb ko‘rsatsa, aynan shu ekanligi
7	Avtorizatsiya	Authorization	Авторизация	Autentifikatsiyadan o‘tgan foydalanuvchiga huquqlar berish
8	Botnet	Botnet	Ботнет	Masofadan boshqariladigan zararlangan kompyuterlar tarmog‘i
9	DDoS	Distributed Denial of Service	Распределённая атака отказа в обслуживании	Ko‘plab manbalardan xizmatni so‘rovlar bilan to‘ldirib ishdan chiqarish hujumi
10	Deshifrlash	Decryption	Расшифрование	Shifratmdan kalit yordamida ochiq matnni tiklash
11	DMZ	Demilitarized zone	Демилитаризованная зона	Internetdan ochiq serverlar joylashtiriladigan, ichki tarmoqdan ajratilgan segment

№	O'zbekcha	Inglizcha	Ruscha	Izoh
12	E-IMZO	E-IMZO	E-IMZO	O'zbekistonda ERI kalitlarini berish va ulardan foydalanish tizimi
13	Elektron raqamli imzo (ERI)	Digital signature	Электронная цифровая подпись	Hujjat muallifi, yaxlitligi va inkor etib bo'lmashligini tasdiqlovchi rekvizit
14	Fishing	Phishing	Фишинг	Ishonchli tashkilot nomidan soxta xabar orqali maxfiy ma'lumotlarni olish
15	Foydalanuvchanlik	Availability	Доступность	Ruxsati bor foydalanuvchilar axborotdan kerakli vaqtda foydalana olishi
16	Gibrid shifrlash	Hybrid encryption	Гибридное шифрование	Ma'lumot simmetrik, kalit esa asimmetrik algoritmi bilan shifrlanadigan sxema
17	Hisobdorlik	Accountability	Подотчётность	Har bir harakatni aniq foydalanuvchiga bog'lash imkoniyati
18	HTTPS	HTTP Secure	HTTPS	TLS yordamida shifrlangan HTTP protokoli
19	Identifikatsiya	Identification	Идентификация	Foydalanuvchining o'zini identifikator orqali tanishtirishi
20	IDS	Intrusion Detection System	Система обнаружения вторжений	Shubhali tarmoq faolligini aniqlab ogohlantiruvchi tizim
21	Ijtimoiy muhandislik	Social engineering	Социальная инженерия	Inson psixologiyasidan foydalanib maxfiy ma'lumot yoki harakatni qo'lga kiritish
22	Inkor etib bo'lmashlik	Non-repudiation	Неотказуемость	Harakatni bajargan shaxs undan tona olmasligi
23	Insident	Security incident	Инцидент безопасности	Axborot xavfsizligini buzgan yoki buzishi mumkin bo'lgan hodisa
24	IPS	Intrusion Prevention System	Система предотвращения вторжений	Hujumlarni aniqlab avtomatik to'sib qo'yuvchi tizim
25	Kalit	Key	Ключ	Shifrlash va deshifrlash algoritmini boshqaruvchi maxfiy parametr

№	O'zbekcha	Inglizcha	Ruscha	Izoh
26	Kam huquqlar tamoyili	Principle of least privilege	Принцип минимальных привилегий	Foydalanuvchiga faqat vazifasi uchun zarur minimal huquqlar berish
27	Keylogger	Keylogger	Кейлоггер	Klaviatura bosishlarini yashirincha yozib oluvchi dastur
28	Kiberbulling	Cyberbullying	Кибербуллинг	Internet va raqamli vositalar orqali tahqirlash, ta'qib qilish
29	Kiberhujum	Cyberattack	Кибератака	Axborot tizimlariga dasturiy-texnik vositalar bilan qasddan ta'sir
30	Kiberxavfsizlik	Cybersecurity	Кибербезопасность	Shaxs, jamiyat va davlat manfaatlarining kibermakondagi tahdidlardan himoyalanganligi
31	Konfidensiallik	Confidentiality	Конфиденциальность	Axborotdan faqat ruxsati bor shaxslar foydalana olishi
32	Kriptografiya	Cryptography	Криптография	Axborotni shifrlash, yaxlitligi va haqiqiyligini ta'minlash haqidagi fan
33	Kriptotahlil	Cryptanalysis	Криптоанализ	Kalitni bilmasdan shifrni ochish usullari haqidagi fan
34	Ko'p faktorli autentifikatsiya (MFA)	Multi-factor authentication	Многофакторная аутентификация	Ikki yoki undan ortiq har xil turdagi omillardan foydalanuvchi autentifikatsiya
35	Ko'p qatlamli himoya	Defense in depth	Эшелонированная защита	Bir necha mustaqil himoya qatlamlarini birgalikda qo'llash tamoyili
36	OWASP	Open Worldwide Application Security Project	OWASP	Veb-ilovalar xavfsizligi bo'yicha xalqaro notijorat hamjamiyat
37	Ochiq kalit	Public key	Открытый ключ	Asimmetrik juftlikdagi hammaga e'lon qilinadigan kalit
38	Parametrlangan so'rov	Parameterized query	Параметризованный запрос	Ma'lumot va SQL kodi alohida uzatiladigan, injeksiyadan himoyalangan so'rov

№	O'zbekcha	Inglizcha	Ruscha	Izoh
39	Parol iborasi	Passphrase	Парольная фраза	Bir nechta tasodifiy so'zlardan iborat uzun parol
40	Parol menejeri	Password manager	Менеджер паролей	Parollarni shifrlangan bazada saqlovchi va yaratuvchi dastur
41	PKI	Public Key Infrastructure	Инфраструктура открытых ключей	Sertifikatlar, markazlar va ularni boshqarish qoidolari majmui
42	Qoldiq xavf	Residual risk	Остаточный риск	Himoya choralari ko'rilgandan keyin qolgan xavf
43	Rootkit	Rootkit	Руткит	Zararli dastur mavjudligini OS darajasida yashiruvchi vosita
44	RSA	RSA	RSA	Katta sonlarni ko'paytuvchilarga ajratish murakkabligiga asoslangan asimmetrik algoritim
45	Sertifikat	Certificate	Сертификат	Ochiq kalitning egasiga tegishligini tasdiqlovchi elektron hujjat
46	Simmetrik shifrlash	Symmetric encryption	Симметричное шифрование	Shifrlash va deshifrlash uchun bitta kalit ishlatiladigan usul
47	SQL injection	SQL injection	SQL-инъекция	Kiritilgan ma'lumot SQL so'roviga kod sifatida qo'shilishidan kelib chiqadigan zaiflik
48	Tahdid	Threat	Угроза	Aktivga zarar yetkazishi mumkin bo'lgan potentsial hodisa yoki harakat
49	Tarmoqlararo ekran	Firewall	Межсетевой экран	Trafikni qoidalar asosida filtrlovchi vosita
50	TOTP	Time-based One-Time Password	Одноразовый пароль на основе времени	Vaqt va maxfiy kalit asosida hisoblanadigan bir martalik kod
51	Trojan	Trojan horse	Троянская программа	Foydali dastur qiyofasida niqoblangan zararli dastur
52	To'lov talab qiluvchi dastur	Ransomware	Программа-вымогатель	Fayllarni shifrlab, to'lov talab qiluvchi zararli dastur

№	O'zbekcha	Inglizcha	Ruscha	Izoh
53	Virus	Computer virus	Компьютерный вирус	O'z kodini boshqa fayllarga yozib ko'payadigan zararli dastur
54	VPN	Virtual Private Network	Виртуальная частная сеть	Ochiq tarmoq orqali shifrlangan tunnel hosil qiluvchi texnologiya
55	Xavf	Risk	Риск	Tahdid zaiflikdan foydalanib zarar yetkazish ehtimoli va ta'sirining birikmasi
56	Xavfsizlik siyosati	Security policy	Политика безопасности	Axborotni himoya qilish maqsadlari, qoidalari va mas'uliyatini belgilovchi hujjat
57	Xesh-funksiya	Hash function	Хеш-функция	Ixtiyoriy ma'lumotdan qat'iy uzunlikdagi qiymat hisoblovchi bir tomonlama funksiya
58	XSS	Cross-Site Scripting	Межсайтовый скриптинг	Sahifaga zararli skript joylashtirilib, boshqa foydalanuvchilarda bajarilishi
59	Yaxlitlik	Integrity	Целостность	Axborotning to'g'riligi va unga ruxsatsiz o'zgartirish kiritilmaganligi
60	Yopiq kalit	Private key	Закрытый ключ	Asimmetrik juftlikdagi faqat egasida saqlanadigan kalit
61	Zaiflik	Vulnerability	Уязвимость	Tahdid amalga oshishiga imkon beruvchi kamchilik
62	Zararli dastur	Malware	Вредоносная программа	Tizimga zarar yetkazish yoki ma'lumot o'g'irlash uchun yaratilgan dastur
63	Zaxira nusxa	Backup	Резервная копия	Ma'lumotlarni tiklash uchun yaratiladigan nusxa
64	Zero-day (nol kunlik) zaiflik	Zero-day vulnerability	Уязвимость нулевого дня	Ishlab chiquvchiga noma'lum yoki tuzatish chiqarilmagan zaiflik
65	Shaxsga doir ma'lumotlar	Personal data	Персональные данные	Jismoniy shaxsga taalluqli yoki uni identifikatsiya qilish imkonini beradigan axborot

№	O‘zbekcha	Inglizcha	Ruscha	Izoh
66	Shifrlash	Encryption	Шифрование	Ochiq matnni kalit yordamida o‘qib bo‘lmaydigan shaklga keltirish
67	Shifrmtn	Ciphertext	Шифртекст	Shifrlangandan keyingi axborot
68	Chuvalchang	Worm	Сетевой червь	Tarmoq orqali mustaqil tarqaladigan zararli dastur
69	2FA	Two-factor authentication	Двухфакторная аутентификация	Ikki har xil turdagi omildan foydalanuvchi autentifikatsiya

X. TEST SAVOLLARI

Test savollari tinglovchilarning nazariy bilimlarini joriy nazorat va o‘z-o‘zini tekshirish maqsadida baholash uchun mo‘ljallangan. Har bir mavzu bo‘yicha 10 tadan, jami 100 ta savol berilgan. Har bir savolga to‘rtta javob varianti berilgan, ulardan faqat bittasi to‘g‘ri. Javoblar kaliti bo‘lim oxirida keltirilgan. Testdan joriy nazoratda foydalanilganda 30 ta savoldan iborat variant tuziladi (har bir mavzudan 3 tadan); to‘g‘ri javoblar ulushi 86% va undan yuqori – “5”, 71–85% – “4”, 55–70% – “3”, 55% dan kam – “2”.

M1. Axborot xavfsizligi asosiy tushunchalari

1. CIA uchligi qaysi xususiyatlardan iborat?
 - A) Tezkorlik, ishonchlilik, arzonlik
 - B) Nazorat, identifikatsiya, audit
 - C) Konfidensiallik, yaxlitlik, foydalanuvchanlik
 - D) Shifrlash, autentifikatsiya, avtorizatsiya
2. Axborotdan faqat ruxsati bor shaxslar foydalana olishi qaysi xususiyat?
 - A) Foydalanuvchanlik
 - B) Yaxlitlik
 - C) Hisobdorlik
 - D) Konfidensiallik
3. O‘quvchi o‘qituvchi parolini bilib, elektron jurnaldagi bahoni o‘zgartirdi. Qaysi xususiyat buzildi?
 - A) Autentiklik
 - B) Yaxlitlik
 - C) Faqat konfidensiallik
 - D) Foydalanuvchanlik
4. To‘lov talab qiluvchi dastur fayllarni shifrlab qo‘ydi. Avvalo qaysi xususiyat buziladi?
 - A) Foydalanuvchanlik
 - B) Konfidensiallik
 - C) Inkori etib bo‘lmaslik
 - D) Identifikatsiya
5. Tahdid amalga oshishiga imkon beruvchi kamchilik nima deb ataladi?
 - A) Aktiv
 - B) Xavf
 - C) Zaiflik
 - D) Hujum

6. Xavf qanday baholanadi?
- A) Hujumlar soni $\div$ himoya choralari
 - B) Tahdidlar soni + zaifliklar soni
 - C) Aktivlar soni $\times$ narxi
 - D) Ehtimollik $\times$ ta'sir
7. Quyidagilardan qaysi biri aktivga misol bo'ladi?
- A) Oddiy parol
 - B) Virus
 - C) Fishing xati
 - D) O'quvchilar ma'lumotlari bazasi
8. Harakatni bajargan shaxs keyinchalik undan tona olmasligi qaysi xususiyat?
- A) Foydalanuvchanlik
 - B) Inkori etib bo'lmaslik
 - C) Yaxlitlik
 - D) Konfidensiallik
9. Zaxira nusxalash himoya choralarining qaysi turiga kiradi (vazifasi bo'yicha)?
- A) Huquqiy
 - B) Oldini oluvchi
 - C) Tiklovchi
 - D) Faqat aniqlovchi
10. "Ko'p qatlamli himoya" tamoyilining mazmuni nima?
- A) Faqat bitta, eng kuchli vositaga tayanish
 - B) Himoyani faqat tarmoq chegarasida tashkil etish
 - C) Barcha kompyuterlarni bitta parol bilan himoyalash
 - D) Bir necha mustaqil himoya qatlamlarini birgalikda qo'llash

M2. Axborot xavfsizligining huquqiy asoslari

11. "Kiberxavfsizlik to'g'risida"gi Qonun qachon qabul qilingan (imzolangan)?
- A) 2019-yil 2-iyul
 - B) 2003-yil 11-dekabr
 - C) 2020-yil 23-sentabr
 - D) 2022-yil 15-aprel
12. "Shaxsga doir ma'lumotlar to'g'risida"gi Qonunning raqami qaysi?
- A) O'RQ-547
 - B) O'RQ-793
 - C) 560-II
 - D) O'RQ-764

- 13.** Amaldagi “Elektron raqamli imzo to‘g‘risida”gi Qonun qaysi?
- A) 2022-yil 12-oktabrdagi O‘RQ-793
 - B) 2022-yil 15-apreldagi O‘RQ-764
 - C) 2003-yil 11-dekabrdagi 562-II
 - D) 2019-yil 2-iyuldagi O‘RQ-547
- 14.** Kiberxavfsizlik sohasidagi vakolatli davlat organi qaysi?
- A) Markaziy bank
 - B) Maktabgacha va maktab ta’limi vazirligi
 - C) Adliya vazirligi
 - D) Davlat xavfsizlik xizmati
- 15.** Shaxsga doir ma’lumotlari ishlov berilayotgan jismoniy shaxs qonunda qanday ataladi?
- A) Uchinchi shaxs
 - B) Subyekt
 - C) Mulkdor
 - D) Operator
- 16.** Maktab o‘quvchilar ma’lumotlar bazasiga nisbatan kim hisoblanadi?
- A) Mulkdor
 - B) Provayder
 - C) Subyekt
 - D) Uchinchi shaxs
- 17.** O‘zbekiston qonunchilik hujjatlarining rasmiy matni qaysi saytda e’lon qilinadi?
- A) uzedu.uz
 - B) owasp.org
 - C) csrc.nist.gov
 - D) lex.uz
- 18.** Axborot xavfsizligini boshqarish tizimiga talablarni belgilovchi xalqaro standart qaysi?
- A) ISO 639
 - B) IEEE 802.11
 - C) ISO/IEC 27001
 - D) ISO 9001
- 19.** NIST CSF 2.0 da nechta asosiy funksiya bor?
- A) Uchta
 - B) O‘nta
 - C) To‘rtta
 - D) Oltita

20. Xavfsizlik siyosati kim tomonidan tasdiqlanadi?

- A) Internet provayderi
- B) Tashkilot rahbariyati
- C) Har bir xodim o'zi uchun
- D) Faqat antivirus ishlab chiqaruvchisi

M3. Tahdidlar tasnifi. Zararli dasturlar

21. Tarmoq orqali foydalanuvchi harakatisiz mustaqil tarqaladigan zararli dastur qaysi?

- A) Reklama dasturi
- B) Chuvalchang
- C) Trojan
- D) Keylogger

22. Foydali dastur qiyofasida niqoblanadigan va o'zi ko'paymaydigan zararli dastur qaysi?

- A) Trojan
- B) Chuvalchang
- C) Botnet
- D) Virus

23. Klaviatura bosishlarini yashirincha yozib oluvchi dastur qanday ataladi?

- A) Keylogger
- B) Rootkit
- C) Kriptomayner
- D) Firewall

24. WannaCry hujumi qaysi yilda sodir bo'lgan?

- A) 2023
- B) 2017
- C) 1988
- D) 2000

25. WannaCry zararlanishidan qaysi chora eng samarali himoya qilar edi?

- A) Brauzer tarixini tozalash
- B) Ekran fon rasmini o'zgartirish
- C) OS yangilanishlarini o'z vaqtida o'rnatish
- D) Monitorni o'chirib qo'yish

26. Trafikni faqat kuzatish va nusxalashdan iborat hujum qanday ataladi?

- A) Ijtimoiy hujum
- B) Faol hujum

- C) DoS hujumi
 - D) Passiv hujum
27. Zararli dastur mavjudligini OS darajasida yashiruvchi vosita qaysi?
- A) VPN
 - B) Parol menejeri
 - C) Antivirus
 - D) Rootkit
28. Antivirusning ma'lum zararli dasturlarni "barmoq izlari" bazasi bilan solishtirish usuli qaysi?
- A) Signatura usuli
 - B) Qum qutisi
 - C) Evristik tahlil
 - D) Xulq-atvor tahlili
29. Ishlab chiquvchiga hali noma'lum bo'lgan zaiflik qanday ataladi?
- A) Ma'lum zaiflik
 - B) Nol kunlik (zero-day) zaiflik
 - C) Jismoniy zaiflik
 - D) Tashkiliy zaiflik
30. To'lov talab qiluvchi dasturdan himoyaning asosiy usuli qaysi?
- A) To'lovni darhol to'lash
 - B) Antivirusni o'chirib qo'yish
 - C) Barcha foydalanuvchilarga administrator huquqi berish
 - D) Tarmoqdan ajratilgan muntazam zaxira nusxalar

M4. Ijtimoiy muhandislik va fishing

31. Ijtimoiy muhandislik nimaga asoslanadi?
- A) Faqat dasturiy zaifliklarga
 - B) Kriptografik algoritmlarni buzishga
 - C) Apparat nosozliklariga
 - D) Inson psixologiyasidan foydalanishga
32. Telefon qo'ng'irog'i orqali aldash qanday ataladi?
- A) Smishing
 - B) Vishing
 - C) Baiting
 - D) Kvishing
33. QR-kod orqali soxta saytga yo'naltirish qanday ataladi?
- A) Tailgating

- B) Pretexting
 - C) Kvishing
 - D) Vishing
34. Yo‘lakda “Maoshlar 2026” yozuvli USB-flesh disk qoldirish qaysi usulga misol?
- A) Whaling
 - B) Baiting
 - C) Vishing
 - D) Tailgating
35. Aniq shaxs haqida oldindan ma’lumot yig‘ib tuzilgan fishing xati qanday ataladi?
- A) Ommaviy fishing
 - B) Smishing
 - C) Nishonli fishing (spear phishing)
 - D) Spam
36. <https://my.gov.uz.login-check.com/oz> havolasidagi haqiqiy (asosiy) domen qaysi?
- A) uz.login
 - B) gov.uz
 - C) my.gov.uz
 - D) login-check.com
37. Saytda HTTPS va qulf belgisi borligi nimani bildiradi?
- A) Ulanish shifrlanganini
 - B) Saytda virus yo‘qligini
 - C) Sayt davlat tomonidan tekshirilganini
 - D) Sayt albatta rasmiy va ishonchli ekanini
38. Shubhali so‘rovni boshqa kanal orqali (rasmiy telefon, shaxsan) tasdiqlash qanday ataladi?
- A) Pretexting
 - B) Ikki kanalli tekshiruv
 - C) Ikki faktorli autentifikatsiya
 - D) Tayposkvotting
39. Rahbar nomidan pul o‘tkazish yoki hujjat yuborishni talab qiluvchi hujum qaysi?
- A) DDoS
 - B) Biznes pochta buzish (BEC)
 - C) SQL injection
 - D) Kriptomayning

40. Quyidagilardan qaysi biri fishingning ishonchli belgisi emas?

- A) SMS-kod so‘ralishi
- B) Shoshilinch harakat talab qilinishi
- C) Xatda imlo xatolari yo‘qligi
- D) Jo‘natuvchi domeni tashkilotga mos kelmasligi

M5. Identifikatsiya, autentifikatsiya va avtorizatsiya

41. Foydalanuvchi login kiritishi qaysi bosqich?

- A) Audit
- B) Identifikatsiya
- C) Avtorizatsiya
- D) Autentifikatsiya

42. Foydalanuvchiga tizimda huquqlar berilishi qaysi bosqich?

- A) Shifrlash
- B) Identifikatsiya
- C) Autentifikatsiya
- D) Avtorizatsiya

43. Quyidagilardan qaysi biri egalik omiliga kiradi?

- A) Barmoq izi
- B) Parol
- C) Maxfiy savol javobi
- D) Autentifikator ilovasi o‘rnatilgan smartfon

44. Parol va maxfiy savol birgalikda nima uchun 2FA hisoblanmaydi?

- A) Parol egalik omili
- B) Ikkalasi ham bilish omili
- C) Maxfiy savol egalik omili
- D) Ikkalasi ham biometrik omil

45. Bir saytdan sizib chiqqan login-parollarni boshqa saytlarda sinash hujumi qaysi?

- A) Credential stuffing
- B) Spoofing
- C) XSS
- D) Shoulder surfing

46. Parol entropiyasi formulasi qaysi (L – uzunlik, N – alifbo hajmi)?

- A) $H = L \cdot \log_2 N$
- B) $H = N \cdot \log_2 L$
- C) $H = L + N$
- D) $H = N^L / 2$

47. NIST ning zamonaviy tavsiyalariga ko‘ra parollarni qachon almashtirish kerak?
- A) Hech qachon, hatto buzilganda ham
 - B) Har kuni
 - C) Buzilganlik belgisi bo‘lganda
 - D) Har 30 kunda majburiy
48. Fishingga eng chidamli 2FA usuli qaysi?
- A) Maxfiy savol
 - B) SMS-kod
 - C) Passkey yoki apparat kalit (FIDO2)
 - D) Elektron pochtaga yuborilgan kod
49. Huquqlar rollarga beriladigan kirishni boshqarish modeli qaysi?
- A) TOTP
 - B) DAC
 - C) RBAC
 - D) MAC
50. Kompyuter sinfida o‘quvchilarning standart hisobda ishlashi qaysi tamoyilga mos?
- A) Kerkgoffs tamoyili
 - B) Kam huquqlar tamoyili
 - C) Standart bo‘yicha ruxsat berish
 - D) Ko‘chki effekti

M6. Kriptografiya asoslari

51. Shifr xavfsizligi faqat kalitning maxfiyligiga asoslanishi kerakligi qaysi tamoyil?
- A) Mayer tamoyili
 - B) Kam huquqlar tamoyili
 - C) Kerkgoffs tamoyili
 - D) PDCA tamoyili
52. Sezar shifrida $k = 3$ bo‘lsa, **A** harfi nimaga almashadi?
- A) D
 - B) C
 - C) B
 - D) Z
53. Lotin alifbosidagi Sezar shifrida nechta ma’noli kalit bor?
- A) 25
 - B) Cheksiz ko‘p
 - C) 3

- D) 26
54. Bir alifboli o‘rniga qo‘yish shifrlarini kalitsiz ochish usuli qaysi?
- A) Ko‘chki effekti
 - B) Tuzlash
 - C) Chastota tahlili
 - D) Segmentlash
55. AES qaysi turdagi algoritmi?
- A) Klassik o‘rniga qo‘yish shifri
 - B) Simmetrik blokli shifr
 - C) Asimmetrik shifr
 - D) Xesh-funksiya
56. RSA qaysi matematik masalaning murakkabligiga asoslangan?
- A) Katta sonlarni tub ko‘paytuvchilarga ajratish
 - B) Matritsalarini ko‘paytirish
 - C) Sonlarni saralash
 - D) Kvadrat tenglamani yechish
57. Asimmetrik shifrlashda xabarni kimning qaysi kaliti bilan shifrlash kerak?
- A) Qabul qiluvchining ochiq kaliti
 - B) Umumiy maxfiy kalit
 - C) Qabul qiluvchining yopiq kaliti
 - D) Jo‘natuvchining yopiq kaliti
58. SHA-256 xesh qiymati necha bit uzunlikka ega?
- A) 128
 - B) Ma’lumot uzunligiga teng
 - C) 256
 - D) 64
59. Xeshlash va shifrlashning asosiy farqi nimada?
- A) Farqi yo‘q
 - B) Xeshlash kalit bilan ochiladi
 - C) Shifrlash har doim bir xil uzunlikdagi natija beradi
 - D) Xeshdan dastlabki ma’lumotni tiklab bo‘lmaydi
60. ERI yaratishda hujjat xeshi qaysi kalit bilan imzolanadi?
- A) Qabul qiluvchining ochiq kaliti
 - B) Sertifikatlash markazining ochiq kaliti
 - C) Imzolovchining ochiq kaliti
 - D) Imzolovchining yopiq kaliti

M7. Tarmoq xavfsizligi

- 61.** Trafikni qoidalar asosida filtrlaydigan vosita qaysi?
- A) Xesh-funksiya
 - B) Tarmoqlararo ekran
 - C) Keylogger
 - D) Parol menejeri
- 62.** Hujumchi ikki tomon orasiga kirib trafikni o'qiydigan yoki o'zgartiradigan hujum qaysi?
- A) DDoS
 - B) "O'rtadagi odam" (MitM)
 - C) Baiting
 - D) Brute force
- 63.** Botnet yordamida xizmatni ishdan chiqarish hujumi qaysi?
- A) Sniffing
 - B) DDoS
 - C) Phishing
 - D) XSS
- 64.** Internetdan ochiq serverlar joylashtiriladigan ajratilgan segment qanday ataladi?
- A) SIEM
 - B) LAN
 - C) VLAN-1
 - D) DMZ
- 65.** Ochiq tarmoq orqali shifrlangan tunnel hosil qiluvchi texnologiya qaysi?
- A) DHCP
 - B) IDS
 - C) DNS
 - D) VPN
- 66.** Hujumni aniqlab, uni avtomatik to'sib qo'yuvchi tizim qaysi?
- A) DNS
 - B) IPS
 - C) FTP
 - D) IDS
- 67.** Ulanish holatini eslab qoluvchi tarmoqlararo ekran qanday ataladi?
- A) Kommutator
 - B) Paketli filtr
 - C) Proksi-server
 - D) Holatni kuzatuvchi (stateful) ekran

68. Tarmoqni mantiqiy qismlarga ajratish uchun qaysi texnologiya ishlatiladi?
- A) AES
 - B) SHA-256
 - C) TOTP
 - D) VLAN
69. Wi-Fi uchun hozirgi kunda tavsiya etiladigan xavfsizlik rejimi qaysi?
- A) WPA (TKIP)
 - B) WEP
 - C) WPA3
 - D) Ochiq tarmoq
70. Ekran qoidalari ro'yxati oxiridagi "hammasini taqiqlash" qoidasi qaysi tamoyilni ifodalaydi?
- A) Gibridd shifrlash
 - B) Standart bo'yicha rad etish
 - C) Ko'chki effekti
 - D) Kam huquqlar

M8. Veb-xavfsizlik. OWASP Top-10

71. OWASP Top 10:2025 ro'yxatida birinchi o'rinda qaysi toifa turadi?
- A) Kirishni boshqarishning buzilishi (Broken Access Control)
 - B) Kriptografik nosozliklar
 - C) Xavfsiz bo'lmagan loyihalash
 - D) Injeksiya (Injection)
72. OWASP Top 10:2025 da yangi kiritilgan toifa qaysi?
- A) Istisno holatlarni noto'g'ri qayta ishlash
 - B) Injeksiya
 - C) Kriptografik nosozliklar
 - D) Kirishni boshqarishning buzilishi
73. SQL injection dan himoyaning asosiy usuli qaysi?
- A) Parametrlangan so'rovlar
 - B) Sahifa rangini o'zgartirish
 - C) Parolni uzaytirish
 - D) Saytga HTTPS o'rnatish
74. OWASP Top 10:2025 da XSS qaysi toifaga kiritilgan?
- A) A09 – Jurnallar va ogohlantirish
 - B) A01 – Kirishni boshqarishning buzilishi
 - C) A05 – Injeksiya

- D) A04 – Kriptografik nosozliklar
75. XSS dan himoya uchun JavaScript da **innerHTML** o‘rniga nima ishlatish tavsiya etiladi?
- A) **eval**
 - B) **textContent**
 - C) **outerHTML**
 - D) **document.write**
76. Sahifada bajariladigan skriptlar manbalarini cheklovchi HTTP sarlavhasi qaysi?
- A) User-Agent
 - B) Content-Length
 - C) Content Security Policy (CSP)
 - D) Accept-Language
77. URL dagi **id** ni o‘zgartirib boshqa o‘quvchi bahosini ko‘rish qaysi toifaga misol?
- A) Kriptografik nosozliklar
 - B) Yetkazib berish zanjiridagi nosozliklar
 - C) Kirishni boshqarishning buzilishi
 - D) Jurnallardagi nosozliklar
78. Zaif yoki zararlangan kutubxonalardan foydalanish OWASP Top 10:2025 ning qaysi toifasiga kiradi?
- A) A07 – Autentifikatsiyadagi nosozliklar
 - B) A03 – Dasturiy ta’minot yetkazib berish zanjiridagi nosozliklar
 - C) A10 – Istisno holatlar
 - D) A06 – Xavfsiz bo‘lmagan loyihalash
79. Sessiya cookie sini JavaScript orqali o‘qilishidan himoya qiluvchi atribut qaysi?
- A) HttpOnly
 - B) Domain
 - C) Expires
 - D) Path
80. OWASP Juice Shop nima?
- A) Onlayn do‘konlar uchun antivirus
 - B) Rasmiy xavfsiz to‘lov tizimi
 - C) Brauzer kengaytmasi
 - D) O‘qitish uchun ataylab zaif qilib yaratilgan o‘quv veb-ilovasi

M9. Axborot tizimlari xavfsizligini boshqarish

81. AXBT qaysi takomillashtirish sikliga asoslanadi?
- A) OSI

- B) SWOT
- C) PDCA
- D) ADDIE

82. Himoya choralari ko‘rilgandan keyin qolgan xavf qanday ataladi?

- A) Nol xavf
- B) Boshlang‘ich xavf
- C) Qoldiq xavf
- D) Tashqi xavf

83. Sug‘urta qilish xavfni boshqarishning qaysi strategiyasi?

- A) Xavfni kamaytirish
- B) Xavfni rad etish
- C) Xavfni qabul qilish
- D) Xavfni o‘tkazish

84. 3-2-1 qoidasida “1” nimani bildiradi?

- A) Kamida bitta nusxa boshqa joyda saqlanadi
- B) Bitta tashuvchi yetarli
- C) Faqat bitta fayl nusxalanadi
- D) Kuniga bir marta nusxa olinadi

85. Oxirgi to‘liq nusxadan keyin o‘zgargan fayllar nusxasi qanday ataladi?

- A) Differensial nusxa
- B) To‘liq nusxa
- C) Ortib boruvchi nusxa
- D) Ko‘zgu nusxa

86. Tizimni qancha vaqt ichida tiklash kerakligini bildiruvchi ko‘rsatkich qaysi?

- A) RPO
- B) ALE
- C) RTO
- D) SLE

87. Bitta hodisadan zarar 4 mln so‘m, hodisa yiliga 2 marta bo‘lsa, ALE nechaga teng?

- A) 2 mln so‘m
- B) 8 mln so‘m
- C) 4 mln so‘m
- D) 6 mln so‘m

88. Insidentga javob berishda zararlangan kompyuterni tarmoqdan uzish qaysi bosqich?

- A) Cheklash

- B) Xulosa
- C) Tiklash
- D) Tayyorgarlik

89. Zaxira nusxaning ishonchliligini qanday tekshirish mumkin?

- A) Nusxa hajmiga qarab
- B) Tekshirish shart emas
- C) Nusxa fayllari nomiga qarab
- D) Muntazam tiklash sinovlari orqali

90. Xavf matritsasida ehtimollik 3 va ta'sir 3 bo'lsa, xavf darajasi qanday?

- A) Nol
- B) Yuqori (9)
- C) O'rta (6)
- D) Past (3)

M10. Ta'lim muassasasida axborot xavfsizligi

91. O'quvchilar ro'yxatini "havolasi bor har kim" rejimida ulashish qanday xavf tug'diradi?

- A) Faqat fayl hajmi kattalashishi
- B) Hech qanday xavf yo'q
- C) Shaxsga doir ma'lumotlar sizib chiqishi
- D) Faqat kompyuter sekinlashishi

92. Maktab tadbirlari suratlarini ijtimoiy tarmoqda e'lon qilishdan oldin nima qilish kerak?

- A) Hech narsa qilish shart emas
- B) Suratlar sifatini pasaytirish
- C) Ota-onalar roziligini olish
- D) Faqat o'qituvchilar roziligini olish

93. Internetda shaxs faoliyatidan qoladigan ma'lumotlar majmui qanday ataladi?

- A) Raqamli imzo
- B) Raqamli sertifikat
- C) Raqamli iz
- D) Raqamli kalit

94. O'quvchi kiberbullingga duch kelsa, birinchi navbatda nima qilish tavsiya etiladi?

- A) Dalillarni saqlab, ishonchli kattalarga xabar berish
- B) Hech kimga aytmaslik
- C) Javoban haqorat yozish

- D) Telefonni sindirish
- 95.** Raqamli xavfsizlikni o'qitishda qaysi yondashuv samaraliroq?
- A) Amaliy ko'nikma va aniq harakatlarni o'rgatish
 - B) Faqat qo'rqitish
 - C) Faqat ma'ruza o'qish
 - D) Internetdan foydalanishni butunlay taqiqlash
- 96.** "Xavfsiz Internet kuni" har yili qaysi oyda o'tkaziladi?
- A) Fevral
 - B) Sentabr
 - C) Iyun
 - D) Dekabr
- 97.** Kiberxavfsizlik madaniyatini shakllantirishda rahbariyatning roli qanday?
- A) Xatoga yo'l qo'yganlarni ommaviy jazolash
 - B) Hech qanday rol o'ynamaydi
 - C) Shaxsiy namuna ko'rsatish va qoidalarini qo'llab-quvvatlash
 - D) Faqat AT mas'uliga topshirib qo'yish
- 98.** 1–4-sinf o'quvchilari uchun raqamli xavfsizlikning asosiy mavzusi qaysi?
- A) Shaxsiy ma'lumotni notanishlarga bermaslik va kattalarga aytish
 - B) IDS sozlash
 - C) RSA algoritmi
 - D) OWASP Top 10
- 99.** Xodim ishdan ketganda uning akkauntlari bilan nima qilinadi?
- A) Parolini ochiq e'lon qilinadi
 - B) O'chiriladi yoki bloklanadi
 - C) O'zgarishsiz qoldiriladi
 - D) Boshqa xodimga parol bilan beriladi
- 100.** Xatoga yo'l qo'ygan xodimning tez xabar berishini rag'batlantiruvchi muhit qanday ataladi?
- A) Yopiqlik madaniyati
 - B) Jazolash madaniyati
 - C) Raqamli tafovut
 - D) Ayblamaslik madaniyati

Javoblar kaliti

Jadvalda har bir qator bitta mavzuning 10 ta savoliga mos keladi; ustun raqami – savolning mavzu ichidagi tartib raqami.

Savollar	1	2	3	4	5	6	7	8	9	10
M1 (1–10)	C	D	B	A	C	D	D	B	C	D
M2 (11–20)	D	A	A	D	B	A	D	C	D	B
M3 (21–30)	B	A	A	B	C	D	D	A	B	D
M4 (31–40)	D	B	C	B	C	D	A	B	B	C
M5 (41–50)	B	D	D	B	A	A	C	C	C	B
M6 (51–60)	C	A	A	C	B	A	A	C	D	D
M7 (61–70)	B	B	B	D	D	B	D	D	C	B
M8 (71–80)	A	A	A	C	B	C	C	B	A	D
M9 (81–90)	C	C	D	A	A	C	B	A	D	B
M10 (91–100)	C	C	C	A	A	A	C	A	B	D

XI. YAKUNIY NAZORAT (YOZMA ISH) MATERIALLARI VA BAHOLASH MEZONLARI

Yakuniy nazorat yozma ish shaklida o'tkaziladi. Har bir variant 3 ta topshiriqdan iborat: 1–2-savollar – nazariy (ta'rif, tamoyil, taqqoslash, misollar bilan yoritish), 3-topshiriq – amaliy (shifrlash yoki xesh masalasi, tahdid modeli, fishing xati tahlili, xavfsizlik siyosati bandi, insidentga javob rejasi yoki dars fragmenti). Yozma ish uchun 80 daqiqa vaqt beriladi. Yozma ishda qo'shimcha adabiyot, telefon va Internetdan foydalanish taqiqlanadi; amaliy topshiriqlar uchun oddiy kalkulyatordan foydalanishga ruxsat etiladi.

1. Yakuniy nazorat uchun nazariy savollar

1. Axborot, axborot resursi va axborot xavfsizligi tushunchalari. Axborot xavfsizligi va kiberxavfsizlik.
2. Axborot xavfsizligining CIA uchligi: konfidensiallik, yaxlitlik, foydalanuvchanlik.
3. Autentiklik, inkor etib bo'lmazlik va hisobdorlik xususiyatlari.
4. Aktiv, tahdid, zaiflik, hujum va xavf tushunchalari, ularning o'zaro bog'liqligi.
5. Himoya choralarining turlari. Ko'p qatlamli himoya tamoyili.
6. O'zbekistonda axborot xavfsizligi sohasidagi me'yoriy-huquqiy baza.
7. "Kiberxavfsizlik to'g'risida"gi Qonunning asosiy tushunchalari va qoidalari.
8. "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun: subyekt, mulkdor, operator, ishlov berish qoidalari.
9. Axborot texnologiyalari sohasidagi huquqbuzarliklar uchun javobgarlik.
10. Xalqaro standartlar (ISO/IEC 27001, NIST CSF) va axborot xavfsizligi siyosati.
11. Axborotga tahdidlarning tasnifi. Passiv va faol hujumlar.
12. Zararli dasturlarning tasnifi. Viruslar va chuvalchanglar.
13. Trojanlar, josus dasturlar, rootkitlar va botnetlar.
14. To'lov talab qiluvchi dasturlar. WannaCry hodisasi va undan saboqlar.
15. Zararli dasturlarning tarqalish yo'llari va antiviruslarning aniqlash usullari.
16. Ijtimoiy muhandislik tushunchasi va uning psixologik asoslari.
17. Ijtimoiy muhandislik hujumlarining turlari: pretexting, baiting, vishing, smishing, kvishing.
18. Fishing va uning turlari. Nishonli fishing va BEC.
19. Fishing xatlari va soxta saytlarni aniqlash belgilari. URL tahlili.

20. Ijtimoiy muhandislikdan himoyalash choralari.
21. Identifikatsiya, autentifikatsiya, avtorizatsiya va audit.
22. Autentifikatsiya omillari. Ikki faktorli va ko'p faktorli autentifikatsiya.
23. Parollarga hujum turlari. Parol kuchliligi va entropiya.
24. Zamonaviy parol siyosati (NIST tavsiyalari). Parol menejerlari.
25. Kirishni boshqarish modellari (DAC, MAC, RBAC) va kam huquqlar tamoyili.
26. Kriptografiyaning asosiy tushunchalari. Kerckhoffs tamoyili.
27. Klassik shifrlar: Sesar va Vajner shifrlari, ularning kriptotahlili.
28. Simmetrik shifrlash. AES algoritmi va kalit tarqatish muammosi.
29. Asimmetrik shifrlash. RSA algoritmi. Gibril shifrlash.
30. Xesh-funksiyalar, ularning xossalari va qo'llanilishi.
31. Elektron raqamli imzo, sertifikatlar va ochiq kalitlar infratuzilmasi. E-IMZO.
32. Tarmoq xavfsizligiga tahdidlar: sniffing, MitM, spoofing, DoS/DDoS.
33. Tarmoqlararo ekranlar: turlari, qoidalari, DMZ.
34. VPN texnologiyasi va uning cheklovlari.
35. IDS va IPS tizimlari. Tarmoqni segmentlash va Wi-Fi xavfsizligi.
36. Veb-ilova arxitekturasini va HTTPS. OWASP loyihasi.
37. OWASP Top 10:2025 ro'yxati va asosiy toifalar.
38. SQL injection zaifligi va undan himoyalash.
39. Saytlararo skripting (XSS): turlari va himoya choralari.
40. Xavfsiz veb-dasturlash tamoyillari.
41. Axborot xavfsizligini boshqarish tizimi va PDCA sikli.
42. Xavflarni baholash: sifatli va miqdoriy usullar, xavf matritsasi.
43. Xavfni boshqarish strategiyalari va qoldiq xavf.
44. Zaxira nusxalash turlari, 3-2-1 qoidasi, RPO va RTO.
45. Insidentlarga javob berish bosqichlari.
46. Ta'lim muassasasining axborot aktivlari va ularga xos xavflar.
47. Ta'lim muassasasida o'quvchilar va xodimlarning shaxsga doir ma'lumotlarini himoya qilish.
48. O'quvchilarning raqamli xavfsizligiga tahdidlar: firibgarlik, raqamli iz, kiberbulling.
49. Raqamli xavfsizlikni o'qitishning mazmuni va metodikasi.
50. Kiberxavfsizlik madaniyati va uni maktabda shakllantirish yo'llari.

2. Yakuniy nazorat uchun amaliy topshiriqlar

1. Berilgan maktab axborot tizimi uchun 5 ta aktiv, ularga tahdid va zaifliklarni aniqlang va xavf matritsasini tuzing.
2. O'quvchilar ma'lumotlari sizib chiqqan holat uchun qaysi CIA xususiyatlari buzilganini aniqlang va 5 ta chorani taklif qiling.
3. Maktab xavfsizlik siyosatining "Kirishni boshqarish va parollar" bo'limini (6–8 qoida) yozing.
4. Elektron jurnal tizimi uchun RBAC modeli asosida rollar va huquqlar jadvalini tuzing.
5. Quyidagi parollar entropiyasini hisoblang va kuchliligini baholang: **dars2026, Dars#2026, olma-daryo-qalam-tog** (so'zlar 7776 so'zli lug'atdan).
6. Berilgan fishing xati (o'qituvchi beradi) belgilarini aniqlang, asosiy domenni yozing va to'g'ri harakat algoritmini tuzing.
7. O'qituvchilar uchun "Fishingni aniqlash" eslatmasining 8 bandini yozing.
8. **INFORMATIKA** so'zini Sezar shifri bilan $k = 7$ da shifrlang va natijani tekshirish usulini ko'rsating.
9. **DARS** so'zini **KOD** kaliti bilan Vijnier usulida shifrlang (hisoblash jadvali bilan).
10. RSA o'quv misoli: $p = 3$, $q = 11$, $e = 7$ bo'lsa, n , $\varphi(n)$ va d ni toping; $M = 4$ ni shifrlang.
11. Ikki tomonning xabar almashinuvi uchun gibrid shifrlash sxemasini chizing va har bir qadamni tushuntiring.
12. ERI yaratish va tekshirish sxemasini chizing; qaysi bosqichda qaysi kalit ishlatilishini ko'rsating.
13. Yuklab olingan fayl yaxlitligini tekshirish tartibini (buyruqlar bilan) yozing va xeshlar mos kelmasa nima qilish kerakligini tushuntiring.
14. Python'da faylning SHA-256 xeshini hisoblovchi funksiya yozing.
15. Maktab tarmog'i uchun tarmoqlararo ekranning 6 ta qoidasini (manba, manzil, port, harakat) tuzing.
16. Maktab tarmog'ini segmentlash sxemasini (kamida 4 segment) chizing va segmentlar orasidagi ruxsatlarni ko'rsating.
17. SQL injection zaifligi bo'lgan so'rovni xavfsiz parametrlangan so'rovga aylantiring va farqini tushuntiring.
18. Maktab elektron tizimidagi 3 ta mumkin bo'lgan zaiflikni OWASP Top 10:2025 toifalariga moslashtiring va himoya choralarini yozing.
19. Maktab ma'muriyati hujjatlari uchun 3-2-1 qoidasiga asoslangan zaxira strategiyasini (RPO, RTO, jadval) tuzing.

20. To'lov talab qiluvchi dastur bilan zararlangan kompyuter uchun insidentga javob rejasini bosqichma-bosqich yozing.
21. ALE ni hisoblang: bitta hodisadan zarar 6 mln so'm, hodisa 4 yilda bir marta; himoya chorasi yiliga 1 mln so'm tursa, u asoslanganmi?
22. Kompyuter sinfi uchun 10 bandli xavfsizlik nazorat varag'ini tuzing.
23. 7-sinf o'quvchilari uchun "Kuchli parol va 2FA" mavzusida 15 daqiqalik dars fragmenti rejasini tuzing.
24. Ota-onalar uchun "Farzandingiz Internetda" eslatmasining 8 bandini yozing.
25. Kiberbulling holatida o'qituvchining harakatlar algoritmini (blok-sxema shaklida) tuzing.

3. Yozma ish variantlari

Variantlar shunday tuzilganki, birinchi nazariy savol 1–25-savollardan (asosiy tushunchalar, huquqiy asoslar, tahdidlar, ijtimoiy muhandislik, autentifikatsiya), ikkinchisi 26–50-savollardan (kriptografiya, tarmoq va veb-xavfsizlik, xavfsizlikni boshqarish, ta'lim muassasasida xavfsizlik) olinadi. Raqamlar yuqoridagi ro'yxatlardagi tartib raqamlariga mos keladi.

Variant	1-nazariy savol	2-nazariy savol	Amaliy topshiriq
1	24. Zamonaviy parol siyosati (NIST tavsiyalari). Parol menejerlari.	37. OWASP Top 10:2025 ro'yxati va asosiy toifalar.	10-amaliy topshiriq
2	7. "Kiberxavfsizlik to'g'risida"gi Qonunning asosiy tushunchalari va qoidalari.	26. Kriptografiyaning asosiy tushunchalari. Kerkgooffs tamoyili.	14-amaliy topshiriq
3	8. "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun: subyekt, mulkdor, operator, ishlov berish qoidalari.	28. Simmetrik shifrlash. AES algoritmi va kalit tarqatish muammosi.	4-amaliy topshiriq
4	18. Fishing va uning turlari. Nishonli fishing va BEC.	47. Ta'lim muassasasida o'quvchilar va xodimlarning shaxsga doir ma'lumotlarini himoya qilish.	5-amaliy topshiriq
5	23. Parollarga hujum turlari. Parol kuchliligi va entropiya.	27. Klassik shifrlar: Sezar va Vijiner shifrlari, ularning kriptotahlili.	19-amaliy topshiriq
6	12. Zararli dasturlarning tasnifi. Viruslar va chuvalchanglar.	48. O'quvchilarning raqamli xavfsizligiga tahdidlar: firibgarlik, raqamli iz, kiberbulling.	15-amaliy topshiriq

Variant	1-nazariy savol	2-nazariy savol	Amaliy topshiriq
7	9. Axborot texnologiyalari sohasidagi huquqbuzarliklar uchun javobgarlik.	45. Insidentlarga javob berish bosqichlari.	3-amaliy topshiriq
8	6. O'zbekistonda axborot xavfsizligi sohasidagi me'yoriy-huquqiy baza.	36. Veb-ilova arxitekturasini va HTTPS. OWASP loyihasi.	2-amaliy topshiriq
9	11. Axborotga tahdidlarning tasnifi. Passiv va faol hujumlar.	29. Asimmetrik shifrlash. RSA algoritmi. Gibril shifrlash.	23-amaliy topshiriq
10	16. Ijtimoiy muhandislik tushunchasi va uning psixologik asoslari.	50. Kiberxavfsizlik madaniyati va uni maktabda shakllantirish yo'llari.	20-amaliy topshiriq
11	10. Xalqaro standartlar (ISO/IEC 27001, NIST CSF) va axborot xavfsizligi siyosati.	31. Elektron raqamli imzo, sertifikatlar va ochiq kalitlar infratuzilmasi. E-IMZO.	18-amaliy topshiriq
12	20. Ijtimoiy muhandislikdan himoyalash choralarini.	46. Ta'lim muassasasining axborot aktivlari va ularga xos xavflar.	25-amaliy topshiriq
13	13. Troyanlar, josus dasturlar, rootkitlar va botnetlar.	35. IDS va IPS tizimlari. Tarmoqni segmentlash va Wi-Fi xavfsizligi.	13-amaliy topshiriq
14	21. Identifikatsiya, autentifikatsiya, avtorizatsiya va audit.	41. Axborot xavfsizligini boshqarish tizimi va PDCA sikli.	12-amaliy topshiriq
15	15. Zararli dasturlarning tarqalish yo'llari va antiviruslarning aniqlash usullari.	32. Tarmoq xavfsizligiga tahdidlar: sniffing, MitM, spoofing, DoS/DDoS.	8-amaliy topshiriq
16	3. Autentiklik, inkor etib bo'lmazlik va hisobdorlik xususiyatlari.	38. SQL injection zaifligi va undan himoyalash.	7-amaliy topshiriq
17	2. Axborot xavfsizligining CIA uchligi: konfidensiallik, yaxlitlik, foydalanuvchanlik.	30. Xesh-funksiyalar, ularning xossalari va qo'llanilishi.	9-amaliy topshiriq
18	14. To'lov talab qiluvchi dasturlar. WannaCry hodisasi va undan saboqlar.	44. Zaxira nusxalash turlari, 3-2-1 qoidasi, RPO va RTO.	11-amaliy topshiriq
19	25. Kirishni boshqarish modellari (DAC, MAC, RBAC) va kam huquqlar tamoyili.	40. Xavfsiz veb-dasturlash tamoyillari.	6-amaliy topshiriq
20	5. Himoya choralarining turlari. Ko'p qatlamli himoya tamoyili.	33. Tarmoqlararo ekranlar: turlari, qoidalari, DMZ.	22-amaliy topshiriq

Variant	1-nazariy savol	2-nazariy savol	Amaliy topshiriq
21	1. Axborot, axborot resursi va axborot xavfsizligi tushunchalari. Axborot xavfsizligi va kiberxavfsizlik.	49. Raqamli xavfsizlikni o'qitishning mazmuni va metodikasi.	16-amaliy topshiriq
22	22. Autentifikatsiya omillari. Ikki faktorli va ko'p faktorli autentifikatsiya.	34. VPN texnologiyasi va uning cheklovlari.	24-amaliy topshiriq
23	4. Aktiv, tahdid, zaiflik, hujum va xavf tushunchalari, ularning o'zaro bog'liqligi.	39. Saytlararo skripting (XSS): turlari va himoya choralari.	1-amaliy topshiriq
24	19. Fishing xatlari va soxta saytlarni aniqlash belgilari. URL tahlili.	43. Xavfni boshqarish strategiyalari va qoldiq xavf.	17-amaliy topshiriq
25	17. Ijtimoiy muhandislik hujumlarining turlari: pretexting, baiting, vishing, smishing, kvishing.	42. Xavflarni baholash: sifatli va miqdoriy usullar, xavf matritsasi.	21-amaliy topshiriq
26	21. Identifikatsiya, autentifikatsiya, avtorizatsiya va audit.	47. Ta'lim muassasasida o'quvchilar va xodimlarning shaxsga doir ma'lumotlarini himoya qilish.	2-amaliy topshiriq
27	12. Zararli dasturlarning tasnifi. Viruslar va chuvalchanglar.	36. Veb-ilova arxitekturasini va HTTPS. OWASP loyihasi.	3-amaliy topshiriq
28	9. Axborot texnologiyalari sohasidagi huquqbuzarliklar uchun javobgarlik.	49. Raqamli xavfsizlikni o'qitishning mazmuni va metodikasi.	15-amaliy topshiriq
29	13. Troyanlar, josus dasturlar, rootkitlar va botnetlar.	30. Xesh-funksiyalar, ularning xossalari va qo'llanilishi.	1-amaliy topshiriq
30	4. Aktiv, tahdid, zaiflik, hujum va xavf tushunchalari, ularning o'zaro bog'liqligi.	32. Tarmoq xavfsizligiga tahdidlar: sniffing, MitM, spoofing, DoS/DDoS.	10-amaliy topshiriq

4. Yozma ish variantining namunaviy ko'rinishi

NAMANGAN DAVLAT PEDAGOGIKA INSTITUTI

“Axborot xavfsizligi” fanidan yakuniy nazorat yozma ishi

1-VARIANT

Tinglovchi F.I.Sh.: _____ Guruh: _____

Sana: _____

1. Zamonaviy parol siyosati (NIST tavsiyalari). Parol menejerlari.
2. OWASP Top 10:2025 ro'yxati va asosiy toifalar.

3. RSA o'quv misoli: $p = 3$, $q = 11$, $e = 7$ bo'lsa, n , $\varphi(n)$ va d ni toping; $M = 4$ ni shifrlang.

Vaqt: 80 daqiqa. Har bir topshiriq 5 baholik shkalada baholanadi; yozma ish bahosi uchta topshiriq baholarining o'rtacha arifmetigi sifatida, butun songa yaxlitlangan holda qo'yiladi.

5. Yozma ish topshiriqlarini baholash mezonlari

Baho	Nazariy savol	Amaliy topshiriq
5	Savol to'liq, ilmiy aniq va mantiqiy yoritilgan; tushunchalar to'g'ri ta'riflangan; ta'lim muassasasi amaliyotidan o'rinli misollar; mustaqil xulosa bor	Topshiriq to'liq va to'g'ri bajarilgan; hisob-kitoblar xatosiz; yechim xavfsizlik nuqtayi nazaridan asoslangan
4	Savol asosan to'g'ri yoritilgan, 1–2 ta kichik noaniqlik; misollar yetarli emas	Topshiriq bajarilgan, 1–2 ta kichik kamchilik bor
3	Savol qisman yoritilgan, ayrim ta'riflar noaniq; misollar yo'q	Topshiriq qisman bajarilgan, jiddiy kamchiliklar bor
2	Javob berilmagan yoki mazmunga mos emas, ko'chirish holati aniqlangan	Topshiriq bajarilmagan yoki yechim mutlaqo noto'g'ri

6. Fan bo'yicha tinglovchi bilimni baholash mezonlari (o'quv dasturiga muvofiq)

a) “5” (a'lo) baho olish uchun tinglovchining bilim darajasi quyidagilarga javob berishi lozim:

- fanning mohiyati va mazmunini to'liq yorita olsa;
- fandagi mavzularni bayon qilishda ilmiylik va mantiqiylik saqlanib, ilmiy xatolik va chalkashliklarga yo'l qo'ymasa;
- fan bo'yicha mavzu materiallarining nazariy yoki amaliy ahamiyati haqida aniq tasavvurga ega bo'lsa;
- fan doirasida mustaqil erkin fikrlash qobiliyatini namoyon eta olsa;
- berilgan savollarga aniq va lo'nda javob bera olsa;
- konspektga puxta tayyorlangan bo'lsa;
- mustaqil topshiriqlarni to'liq va aniq bajargan bo'lsa;
- barcha amaliy ko'nikma va malakalarni o'zlashtirgan bo'lsa;
- nazariy bilimlarni turli vaziyatda qo'llay olsa;
- tizimli yondashish, uzviylikka amal qilsa.

b) “4” (yaxshi) baho olish uchun tinglovchining bilim darajasi quyidagilarga javob berishi lozim:

- fanning mohiyati va mazmunini tushungan, fandagi mavzularni bayon qilishda ilmiy va mantiqiy chalkashliklarga yo'l qo'ymasa;

- fanning mazmuni va amaliy ahamiyatini tushungan bo‘lsa;
- fan bo‘yicha berilgan vazifa va topshiriqlarni o‘quv dasturi doirasida bajarsa;
- fan bo‘yicha berilgan savollarga to‘g‘ri javob bera olsa;
- fan bo‘yicha konspektini puxta shakllantirgan bo‘lsa;
- fan bo‘yicha mustaqil topshiriqlarni to‘liq bajargan bo‘lsa;
- barcha amaliy ko‘nikma va malakalarni o‘zlashtirishga harakat qilgan bo‘lsa.

d) “3” (qoniqarli) baho olish uchun tinglovchining bilim darajasi quyidagilarga javob berishi lozim:

- fan haqida umumiy tushunchaga ega bo‘lsa;
- fandagi mavzularni tor doirada yoritib, bayon qilishda ayrim chalkashliklarga yo‘l qo‘yilsa;
- fan bo‘yicha mustaqil topshiriqlarni qisman bajargan bo‘lsa;
- bayon qilish ravon bo‘lmasa;
- fan bo‘yicha savollarga mujmal va chalkash javoblar olinsa;
- fan bo‘yicha matn puxta shakllantirilmagan bo‘lsa.

e) quyidagi hollarda tinglovchining bilim darajasi qoniqarsiz “2” baho bilan baholanishi mumkin:

- fan bo‘yicha mashg‘ulotlarga tayyorgarlik ko‘rilmagan bo‘lsa;
- fan bo‘yicha mashg‘ulotlarga doir hech qanday tasavvurga ega bo‘lmasa;
- fan bo‘yicha mustaqil topshiriqlarni to‘liq bajarmagan bo‘lsa;
- fan bo‘yicha matnlarni boshqalardan ko‘chirib olganligi sezilib tursa (plagiat aniqlansa);
- fan bo‘yicha matnda jiddiy xato va chalkashliklarga yo‘l qo‘yilgan bo‘lsa;
- fanga doir berilgan savollarga javob olinmasa;
- fanni bilmasa.

XII. ADABIYOTLAR RO‘YXATI

Asosiy adabiyotlar

1. Stallings W., Brown L. Computer Security: Principles and Practice. 4th Ed. – Pearson, 2018.
2. Stallings W. Cryptography and Network Security: Principles and Practice. 8th Ed. – Pearson, 2020.
3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd Ed. – Wiley, 2020.
4. Whitman M.E., Mattord H.J. Principles of Information Security. 6th Ed. – Cengage, 2017.

Me‘yoriy-huquqiy hujjatlar

5. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. O‘RQ-764-son, 2022-yil 15-aprel.
6. O‘zbekiston Respublikasining “Shaxsga doir ma‘lumotlar to‘g‘risida”gi Qonuni. O‘RQ-547-son, 2019-yil 2-iyul.

Qo‘shimcha adabiyotlar

7. Mitnick K.D., Simon W.L. The Art of Deception: Controlling the Human Element of Security. – Wiley, 2002.

Axborot manbalari

8. <https://owasp.org/www-project-top-ten/> – OWASP Top 10: veb-lovalarning asosiy zaifliklari.
9. <https://www.cisa.gov/topics/cybersecurity-best-practices> – CISA: kiberxavfsizlik bo‘yicha amaliy tavsiyalar.
10. <https://csrc.nist.gov> – NIST Computer Security Resource Center.
11. <https://lex.uz> – O‘zbekiston Respublikasi Qonunchilik ma‘lumotlari milliy bazasi.

Xalqaro universitetlarning tegishli o‘quv manbalari

12. <https://cs50.harvard.edu/cybersecurity/> – Harvard University. CS50’s Introduction to Cybersecurity.
13. <https://ocw.mit.edu/courses/6-858-computer-systems-security-fall-2014/> – MIT. 6.858 Computer Systems Security.

Amaliy va laboratoriya mashg‘ulotlarida foydalaniladigan qo‘shimcha elektron resurslar

- O‘zbekiston Respublikasining “Elektron raqamli imzo to‘g‘risida”gi Qonuni. O‘RQ-793-son, 2022-yil 12-oktabr (lex.uz).

- O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonuni. 560-II-son, 2003-yil 11-dekabr (lex.uz).
- <https://owasp.org/www-project-juice-shop/> – OWASP Juice Shop o‘quv ilovasi va “Pwning OWASP Juice Shop” qo‘llanmasi.
- <https://pages.nist.gov/800-63-4/> – NIST SP 800-63B: raqamli identifikatsiya va parollar bo‘yicha tavsiyalar.
- <https://www.nist.gov/cyberframework> – NIST Cybersecurity Framework 2.0.
- <https://cryptography.io> – Python **cryptography** kutubxonasi hujjatlari.
- <https://veracrypt.io>, <https://keepassxc.org>, <https://bitwarden.com> – shifrlash va parol menejeri vositalari.
- <https://www.wireshark.org> – Wireshark tarmoq analizatori va o‘quv qo‘llanmalari.
- <https://www.eicar.org> – EICAR antivirus sinov fayli.
- <https://e-imzo.uz> – E-IMZO elektron raqamli imzo tizimi.
- <https://uzcert.uz> – Kiberxavfsizlik markazi (UZCERT): ogohlantirishlar va tavsiyalar.
- <https://www.saferinternetday.org> – Xavfsiz Internet kuni: o‘quvchilar va ota-onalar uchun materiallar.