**O’ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA**

**KOMMUNIKATSIYALARNI RIVOJLANTIRISH VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT**

**TEXNOLOGIYALARI UNIVERSITETI**

**AMALIY ISH**

**Fakultet :** AKTSIM

**Fan:** Kiberxavfsizlik

**Guruh:** CSFOO1-1



**Bajardi:** Mengliboyev Kamoliddin

**Tekshirdi:** Xolimtayeva Iqbola

**1-amaliy ish**

**Kiberxavfsizlikda risklarni baholashni o‘rganish**

**Ishdan maqsad:** Kiberxavfsizlikda sodir bo‘lishi mumkin bo‘lgan risklarini

galstuk-babochka usuli haqida nazariy va amaliy ko‘nikmalarga ega bo‘lish.

**Nazariy qism**

Tahdid – tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan

hodisa. Yoki, tahdid - axborot xavfsizligini buzuvchi potensial yoki real mavjud

xavfni tug‘diruvchi sharoit va omillar majmui. Tahdid tashkilotning aktivlariga

qaratilgan bo‘ladi. Masalan, aktiv sifatida korxonaga tegishli biror bir saqlanuvchi

hujjat bo‘lsa, u holda ushbu hujjat saqlanadigan xonaga nisbatan tahdid amalgaoshirilish mumkin.

**Risk** – potensial foyda yoki zarar bo‘lib, umumiy holda har qanday vaziyatgabiror bir hodisani yuzaga kelish ehtimoli qo‘shilganida risk paydo bo‘ladi. ISO “risk – bu noaniqlikning maqsadlarga ta’siri” sifatida ta’rif bergan.

Masalan, universitetga o‘qishga kirish jarayonini ko‘raylik. Umumiy holda bu jarayonni o‘zi risk hisoblanmaydi. Faqatgina abituriyent hujjatlarini va kirish imtihonlarini topshirganida, u o‘qishga kirishi yoki kira olmasligi mumkin. Bu o‘z

navbatida qabul qilinish yoki qabul qilinmaslik riskini yuzaga kelishiga sabab bo‘ladi.

Kiberxavfsizlikda yoki axborot xavfsizligida risklarga salbiy ko‘rinishda

qaraladi.

*Hujumchi kabi fikrlash* - bo‘lishi mumkin bo‘lgan xavfni oldini olish

maqsadida qonuniy foydalanuvchining hujumchi kabi fikrlash jarayoni.

*Tizimli fikrlash* - kafolatlangan amallarni ta’minlash uchun ijtimoiy va

texnik cheklovlarning o‘zaro ta’sirini hisobga oladigan fikrlash jarayoni.

**“Galstuk-babochka” tahlil usuli.**

Ushbu usul o‘rganilayotgan salbiy hodisaning sababdan oqibatga qadar rivojlanishini grafik

tavsiflash va tahlil qilishdir. Ushbu usulning asosiy yo‘nalishi tekshirilayotgan hodisaga

qarshi choralar va uni keltirib chiqaradigan sabablarga 4 qaratilgan. Us hbu usulni amalga

oshirish quyidagi bosqichlarni ajratishi mumkin:

1. Grafik markazida tahlil qilish uchun hodisani aniqlash.

2. Tekshirilayotgan hodisaga olib kelishi mumkin bo‘lgan sabablar

ro‘yxatini tuzish.

3. Tekshirilayotgan voqea oldidan vaziyatning rivojlanish mexanizmini

tahlil qilish

4. Hodisaning rivojlanishiga olib keladigan omillar va uning oqibatlari

tavsiflanishi mumkin.

5. Hodisadan oldin deb ataladigan sabablarning rivojlanishiga to‘sqinlik

qiladigan to‘siqlarni namoyish qilish profilaktika choralari. Eskalatsiya omillari

uchun to‘siqlarni ham ko‘rsatishingiz mumkin.

6. Tekshirilayotgan voqea sabab bo‘lishi mumkin bo‘lgan oqibatlar

ro‘yxatini tuzish.

7. O‘rganilayotgan voqeaning oqibatlarini rivojlanishiga to‘sqinlik qiladigan

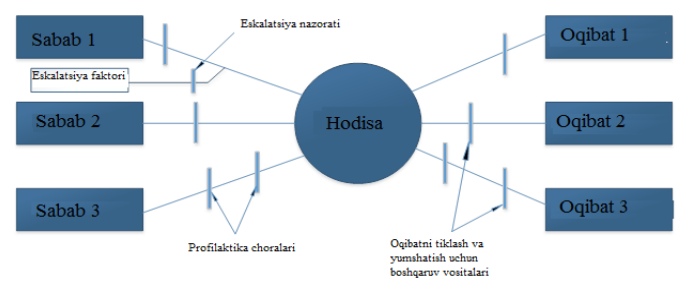
to‘siqlarni namoyish qilish.

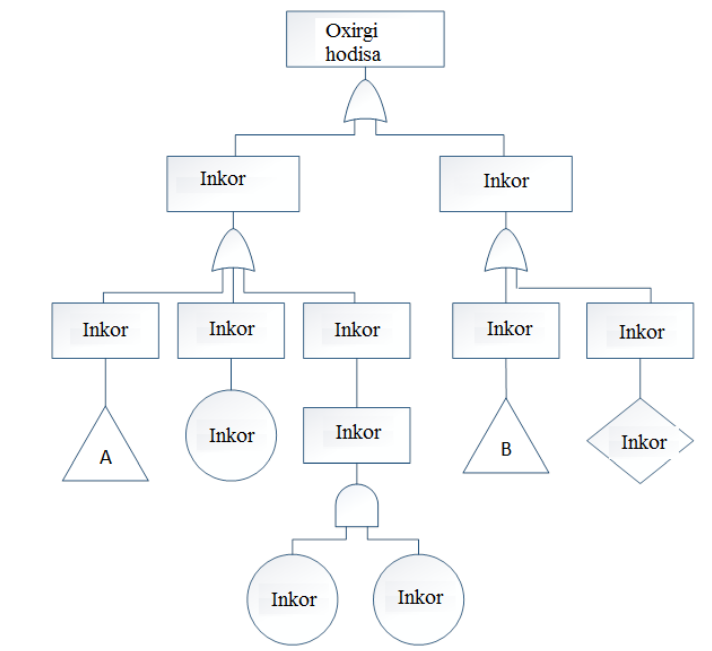
«Galstuk-babochka» tahlilini o‘tkazish orqali biz xavfli hodisalar va ularning oqibatlarini

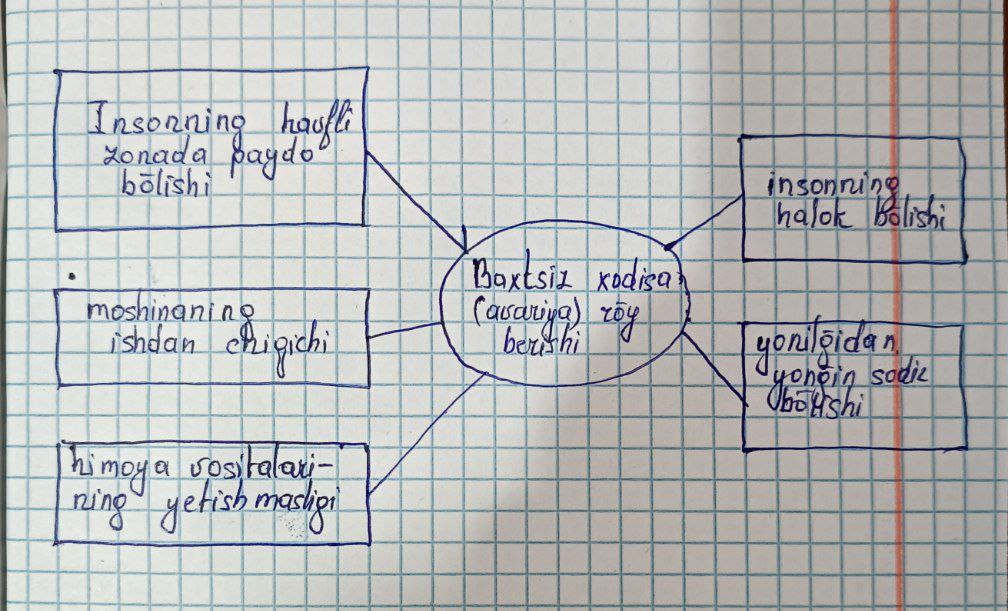
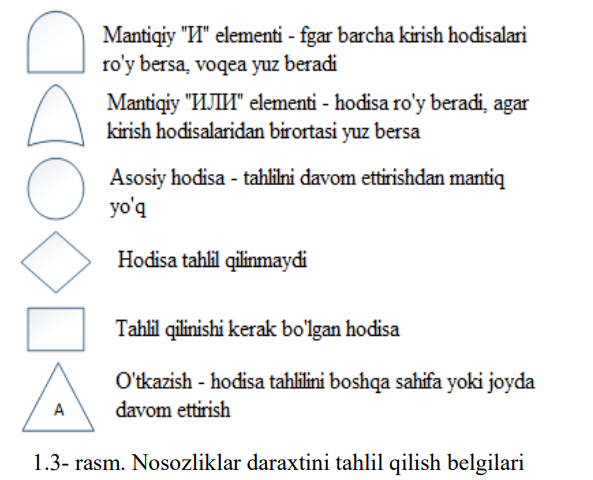
oldini olish, yumshatish yoki kutilayotgan hodisalarni kuchaytirish, tezlashtirishga

yo‘naltirilgan xavfli voqealar va to‘siqlarning asosiy yo‘llarini aniq ko‘rsatadigan oddiy

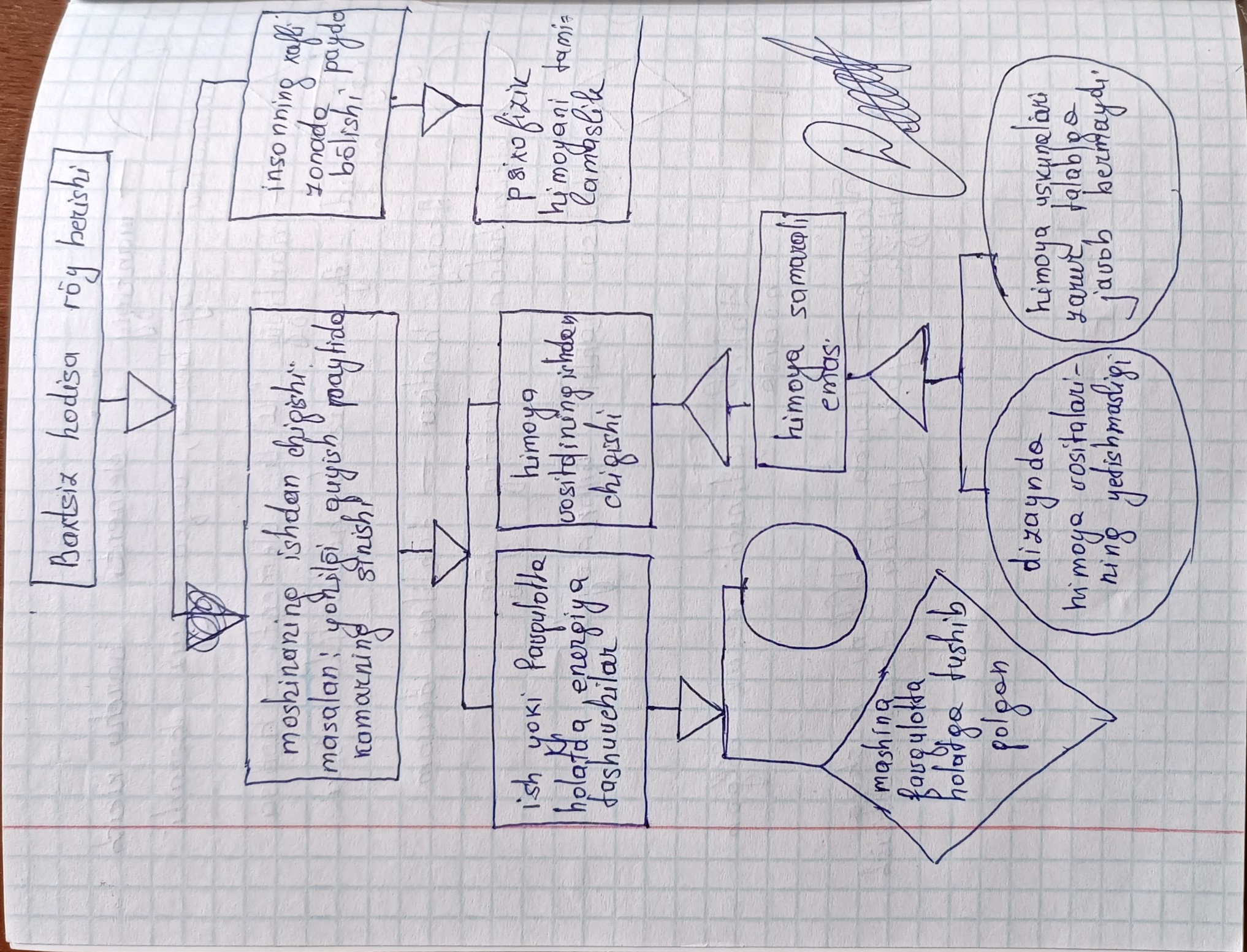
diagramma kiritamiz (tekshirilayotgan voqea ijobiy bo‘lgan taqdirda).



**Nosozliklarni tahlil qilish.**



**Amaliy qism**

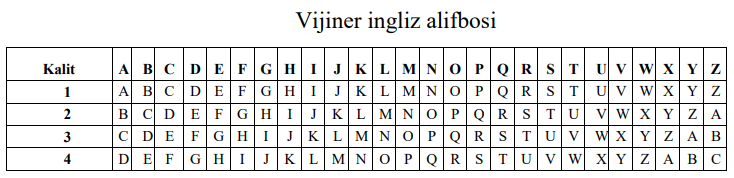


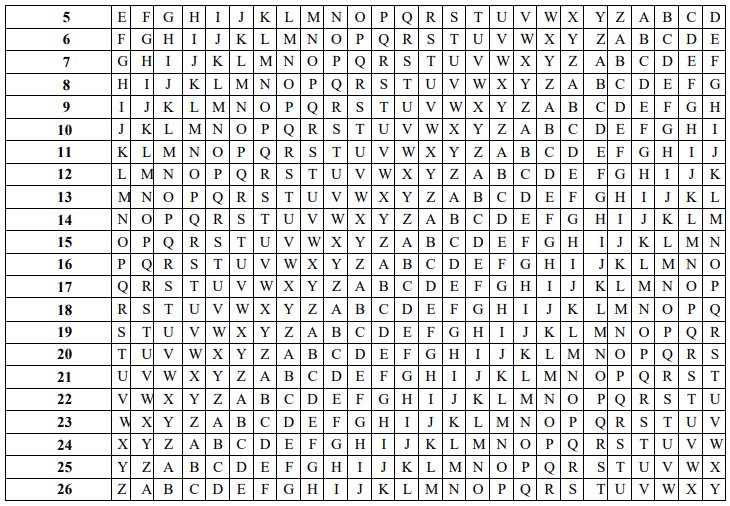
**2-amaliy ish**

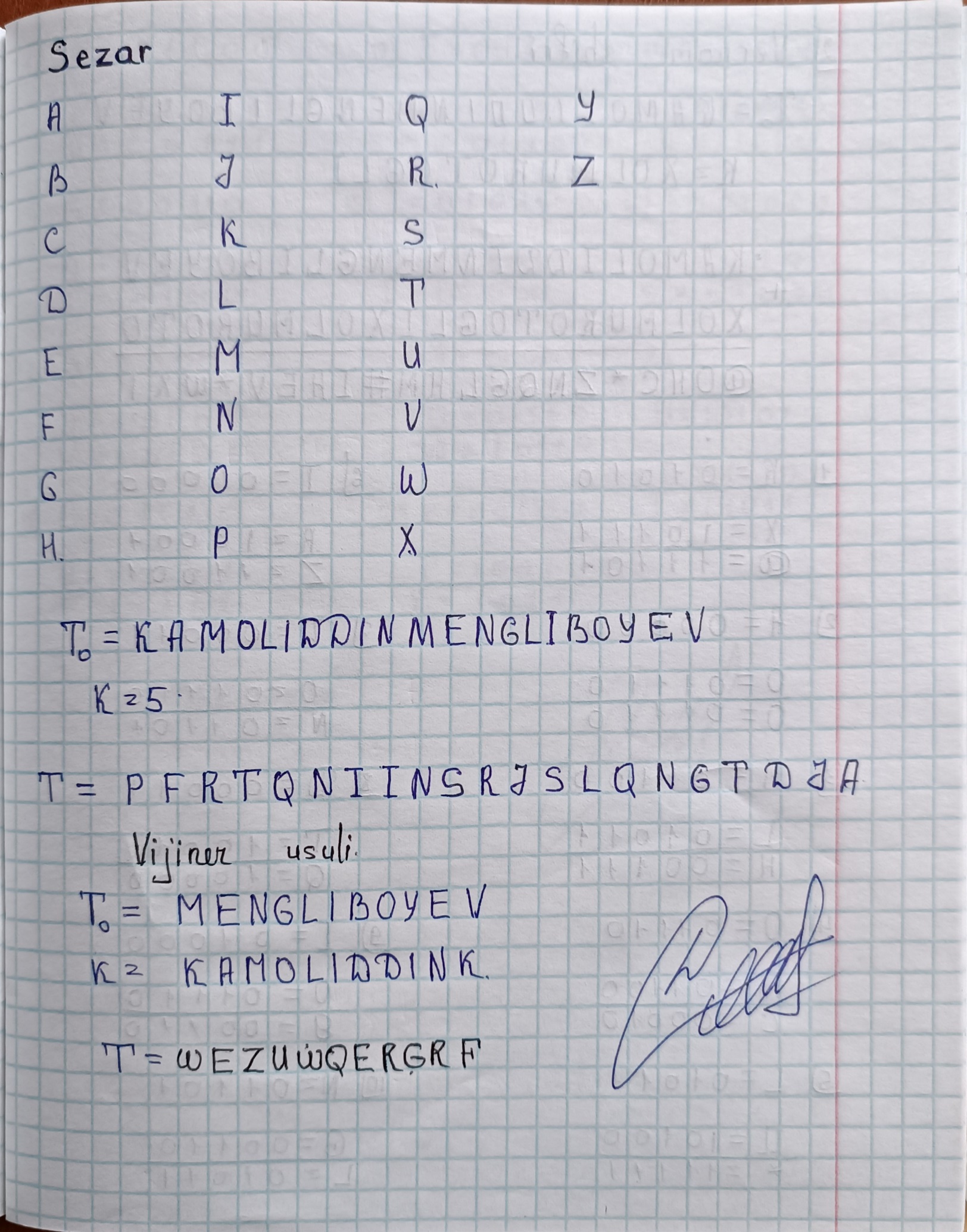
**Klassik shifrlash algoritmlarini ishlash tartibini o‘rganish**

**Ishdan maqsad:** Klassik shifrlash algoritmlarini ishlashi haqida nazariy va

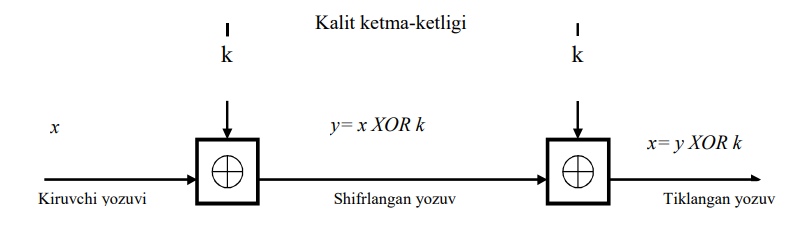
amaliy bilim ko‘nikmalarni shakllantirish.

 **Amaliy qism**





**Vernam shifri.**



Kiruvchi matnni shifrlashda x-kiruvchi matn ikkilik ko‘rinishiga o‘tkaziladi

va ikkilik modul ostida ikkilik ketma-ketlikdagi k-kalit bilan shifrlash amalga

oshiriladi. Bu shifrlangan yozuv quyidagi tenglik orqali amalga oshiriladi.

y = x ⊕k

Deshifrlash uchun shifrmatn va kalit xor amalida qo‘shiladi.

