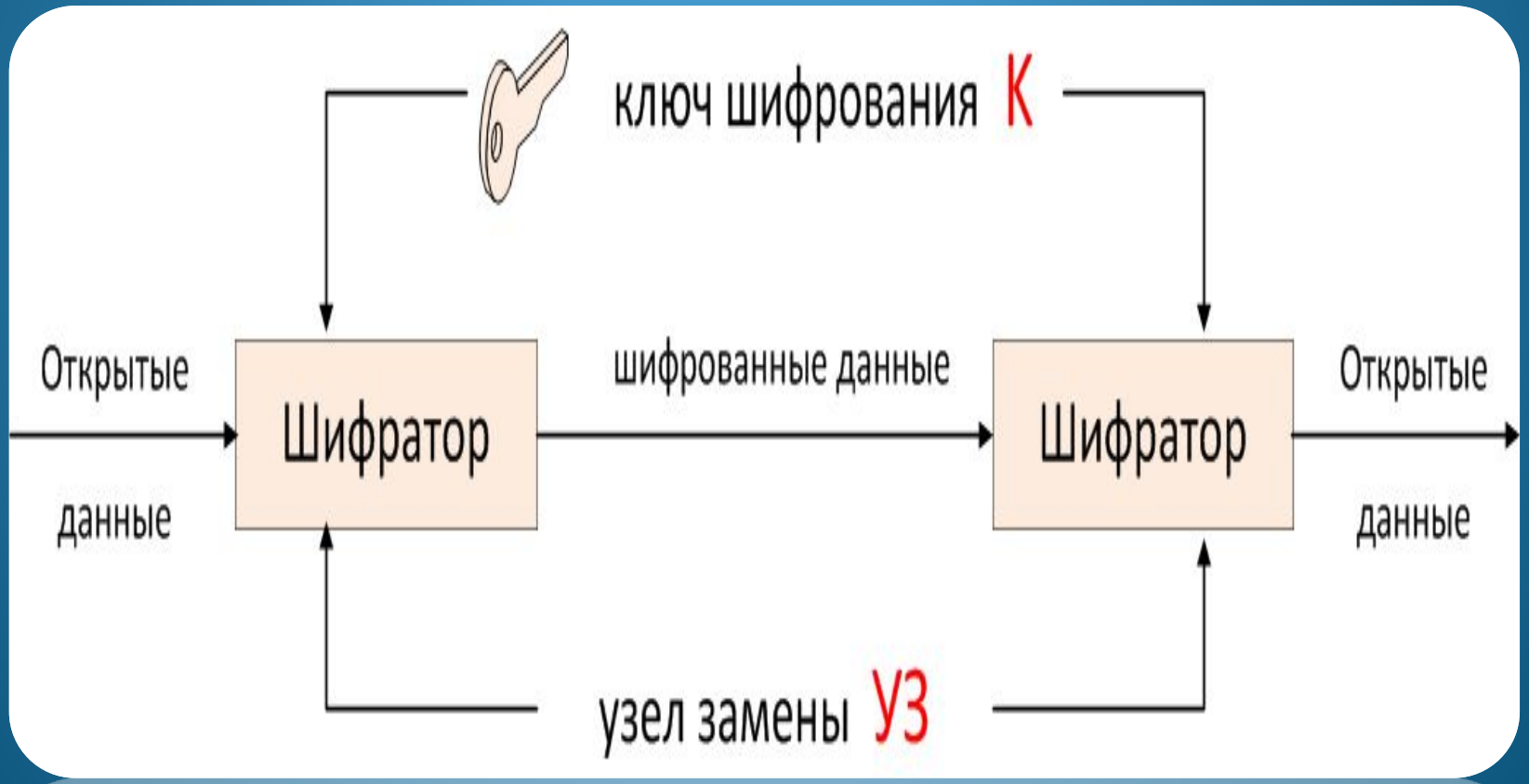
Шифр ГОСТ 28147-89.



Шифр және шифрлау

Шифр – франц. «chiffre» - цифр, араб. «sifr» - нөл. Шифр – таратылатын ақпараттың құпия болуын қамтамасыз ету үшін кілті бар мәтінді түрлендіру жүйесі.

Қайда қолданылады?

Дипломатиялық қарым-қатынаста

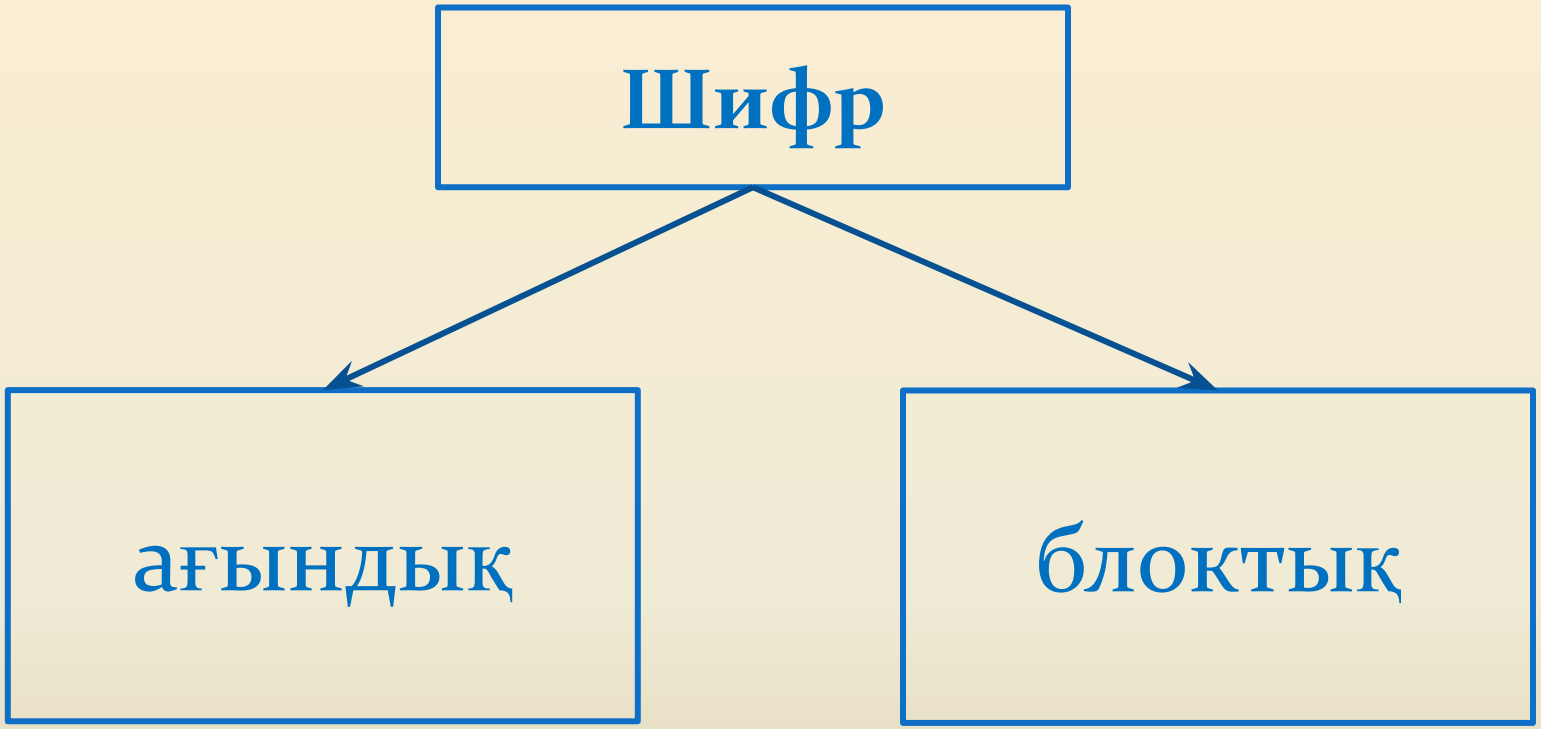
Әскери салада

Интернет-қызмет көрсетулерде

Шифр және шифрлау

Шифрлау **(ciphering, encryption) – белгілі бір адамнан басқалар оқи алмайтындай етіліп ақпаратты математикалық, алгоритмдік (криптографиялық) түрлендіру әдісі. Қабылдаушы жақ бұл ақпаратты дұрыс оқу үшін оны кері шифрлауы (decryption) керек. Шифрлау – бөлшекті (әрбір кезекті бөлшек тәуелсіз шифрланады) және ағынды (әрбір таңба бір-бірінен тәуелсіз шифрланады) түрде жүргізілуі мүмкін.**

Шифр және шифрлау



Характеристики составных алгоритмов шифрования

Название алгоритма	Размер ключа, бит	Размер блока, бит	Размер вектора инициализации, бит	Количество циклов шифрования
Lucipher	128	128		
DES	56	64	64	16
FEAL-1	64	64	4	
B-Crypt	56	64	64	
IDEA	128	64		
ГОСТ 28147-89	256	64	64	32

- **ГОСТ 28147-89 - отечественный стандарт на шифрование данных . Стандарт включает три алгоритма зашифровывания (расшифровывания) данных: режим простой замены, режим гаммирования, режим гаммирования с обратной связью - и режим выработки имитовставки.**

- **С помощью имитовставки можно зафиксировать случайную или умышленную модификацию зашифрованной информации. Вырабатывать имитовставку можно или перед зашифровыванием (после расшифровывания) всего сообщения, или одновременно с зашифровыванием (расшифровыванием) по блокам. При этом блок информации шифруется первыми шестнадцатью циклами в режиме простой замены, затем складывается по модулю 2 со вторым блоком, результат суммирования вновь шифруется первыми шестнадцатью циклами и т. д.**

- **Алгоритмы шифрования ГОСТ 28147-89 обладают достоинствами других алгоритмов для симметричных систем и превосходят их своими возможностями. Так, ГОСТ 28147-89 (256-битовый ключ, 32 цикла шифрования) по сравнению с такими алгоритмами, как DES (56-битовый ключ, 16 циклов шифрования) и FEAL-1 (64-битовый ключ, 4 цикла шифрования) обладает более высокой криптостойкостью за счет более длинного ключа и большего числа циклов шифрования.**

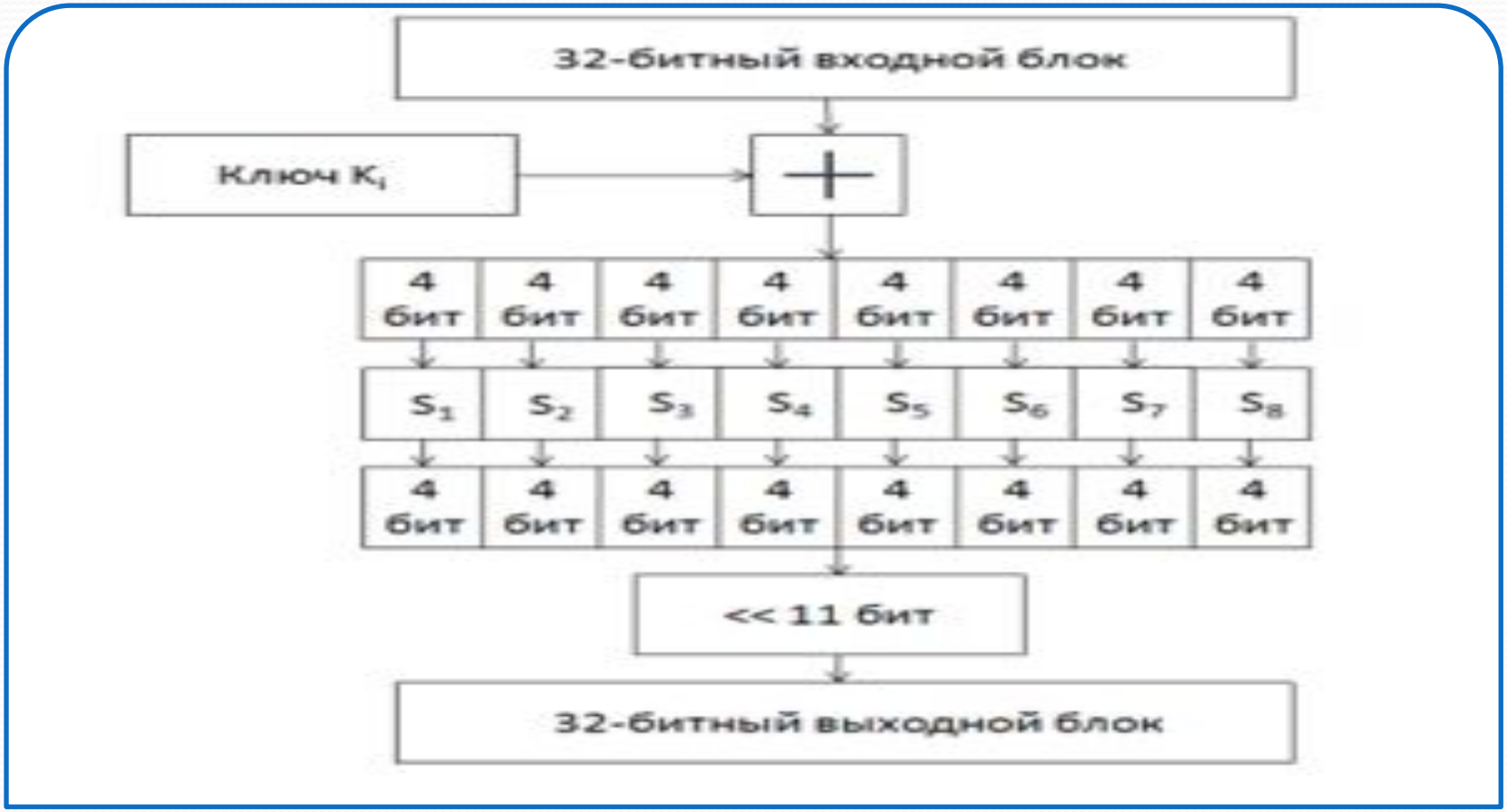
- **Достоинствами ГОСТ 28147-89 являются также наличие защиты от навязывания ложных данных (выработка имитовставки) и одинаковый цикл шифрования во всех четырех алгоритмах ГОСТа.**

ГОСТ 28147-89

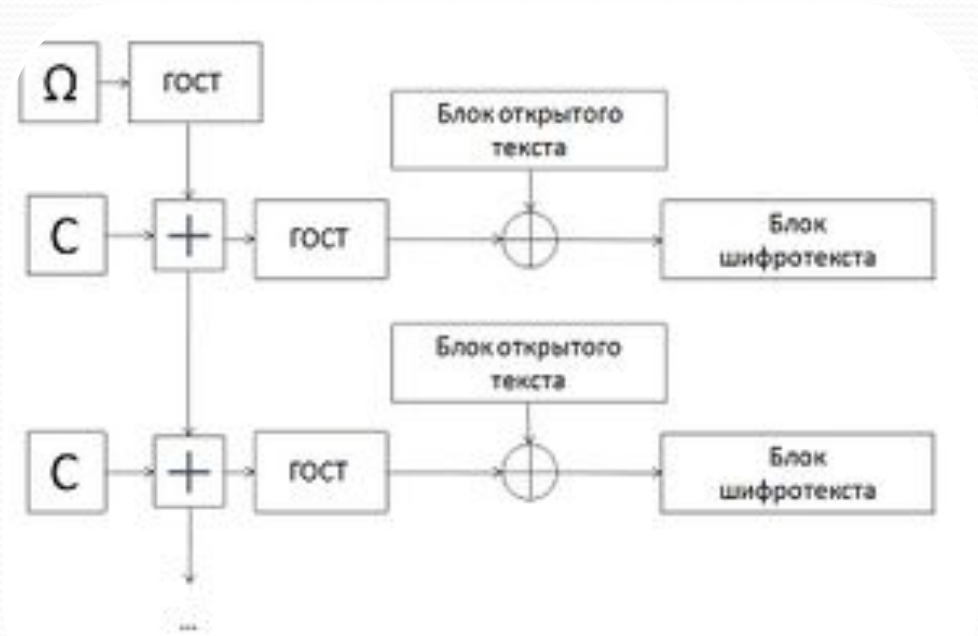
- 1989 жылы қабылданды.
- Толық атауы – «Ақпаратты өңдеу жүйелері. Криптографиялық қорғау. Криптографиялық түрлендіру алгоритмі».
- 256 битті кілті, 32 түрлендіру циклі (раунды), 64 битті блогы бар блоктық шифр.
- Алгоритмінің негізі – Фейстель желісі.

4 жұмыс режимі бар:

- Қарапайым орын басу
- Кері байланыспен тағамдау
- Тағамдау
- Мәнтовстаяка оңдеу режимі

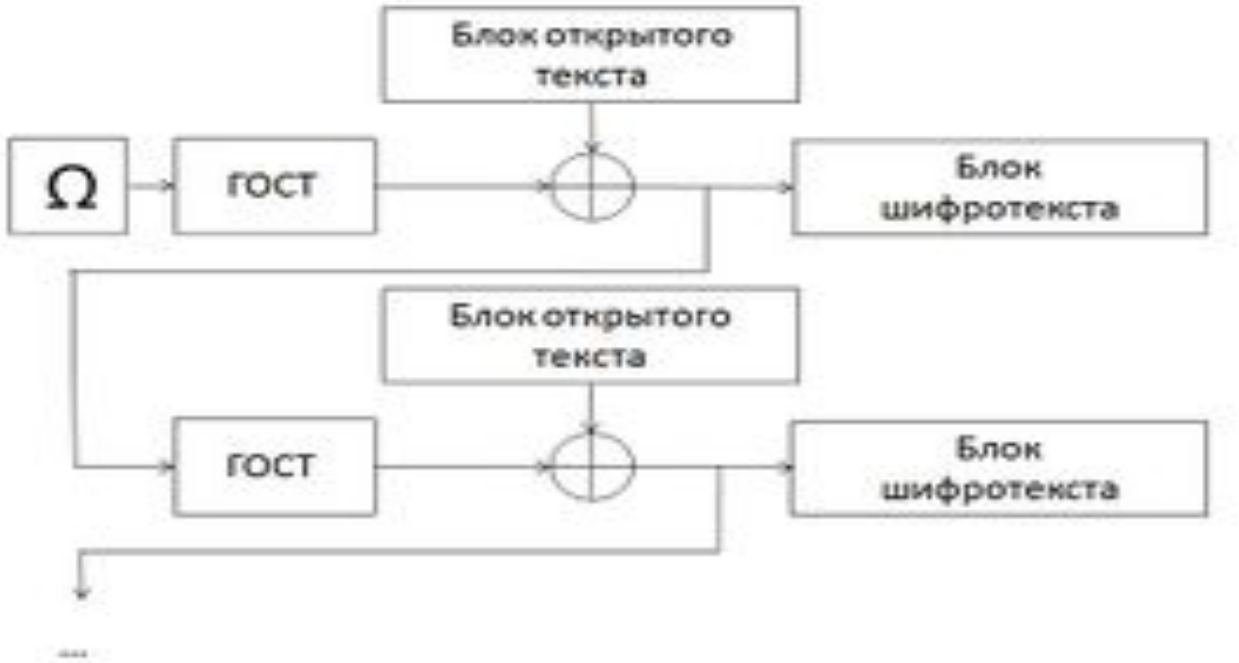


Қарапайым орын басу

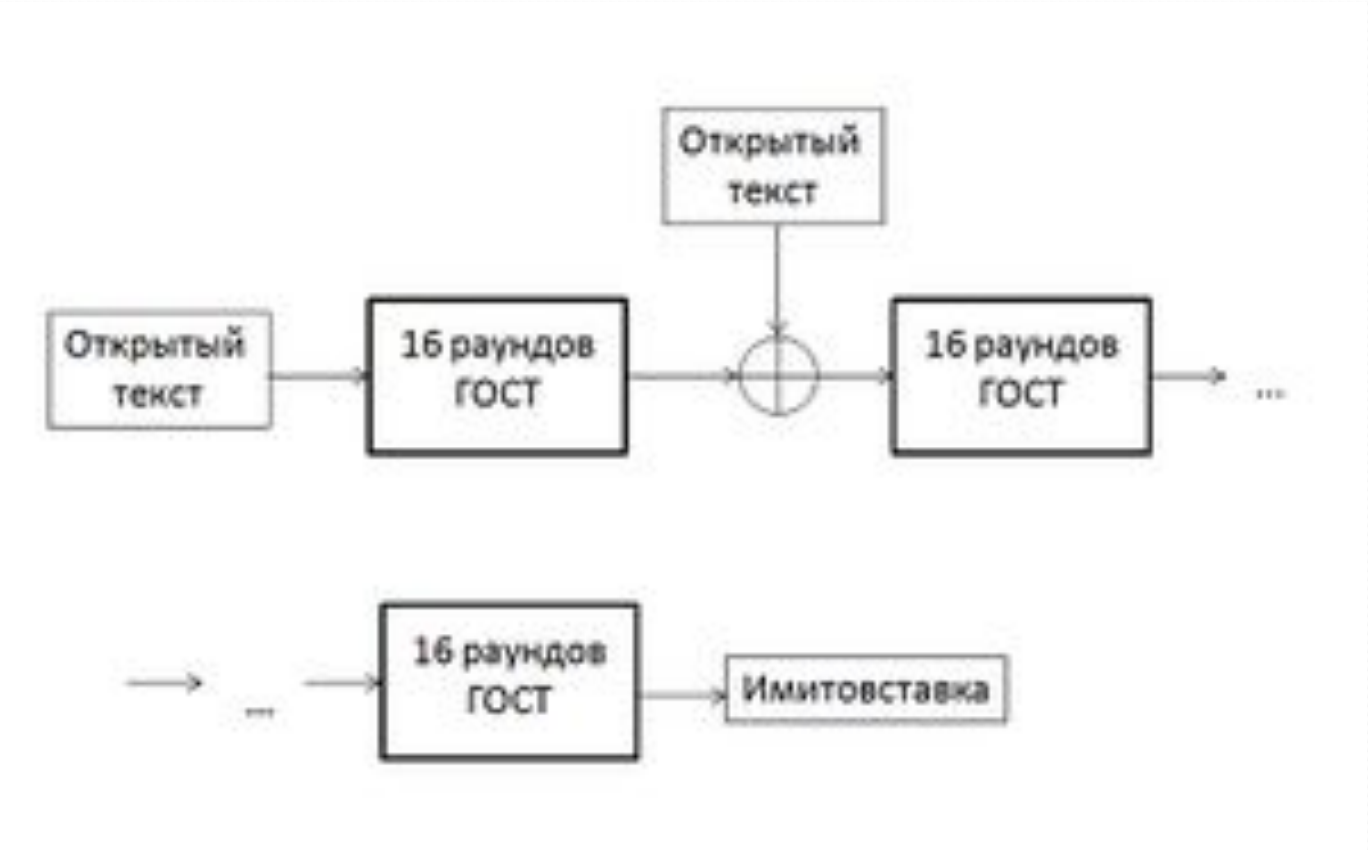

Ω
ГОСТ
Блок открытого текста
C
ГОСТ
Блок шифротекста
Блок открытого текста
C
ГОСТ
Блок шифротекста

Гаммалау

Кері байланысты гаммалау



Имитовставка өңдеу режимі



НАЗАРЛАРЫҢЫЗҒА РАХМЕТ!