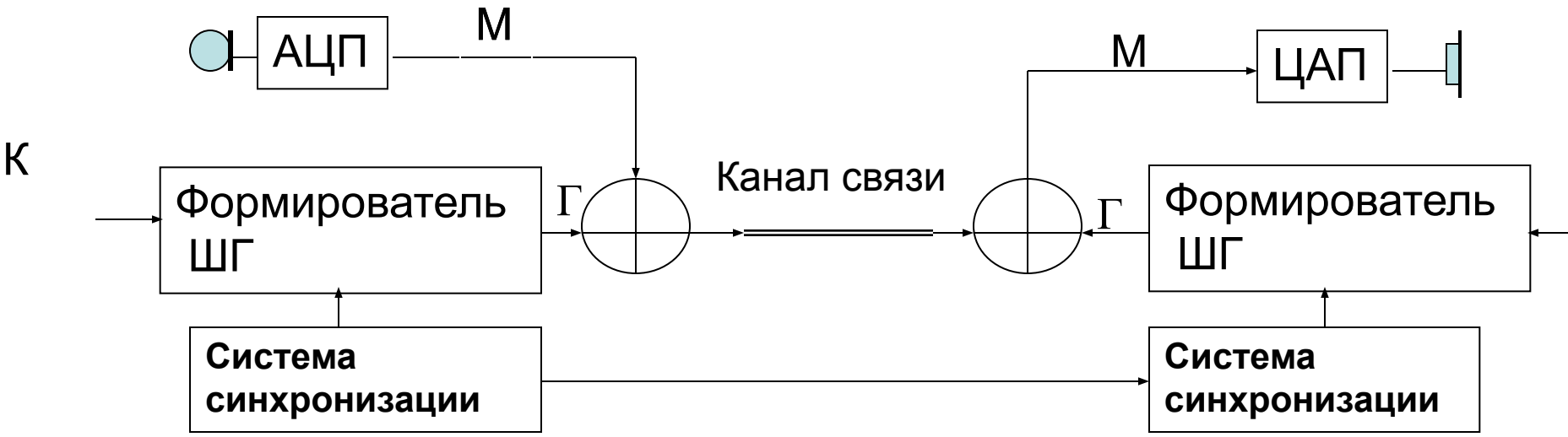
Лекция
Шифрование в цифровой и аналоговой телефонии

- Лектор: профессор Яковлев В.А.

1. Принципы построения цифровых систем шифрования



$E=M \oplus Г$ $Г=f(S,K)$

$M=E \oplus Г$

Аналого-цифровые преобразователи:
ИКМ - 64 кбит/с
ДМ - 16-32 кбит/с
Вокодер - 1,2 - 13 кбит/с

Структурная схема формирователя шифрующей гаммы по алгоритму А5

$h_1(x) = x^{19} + x^5 + x^2 + x + 1,$

$h_2(x) = x^{22} + x + 1,$

$h_3(x) = x^{23} + x^{15} + x^2 + x + 1.$

Структурная схема формирователя шифрующей гаммы по алгоритму A5/2

$$M(x_1\ x_2\ x_3) = x_1\ x_2 \oplus x_1\ x_3 \oplus x_2\ x_3$$

A5/3

Средства шифрования в мобильной связи

Название	Фото	Сеть\информ	Производитель/поставщик
Талисман-GSM		GSM 900\1800(РЕЧЬ)	**«СОВТЕХКОМ»**
Ancort		GSM 900\1800(РЕЧЬ)	**«АНКОРТ»(Разрешение ФСБ РФ)**
SMP-«Атлас»		GSM 900\1800 «Мегафон»(РЕЧЬ)	**НТЦ «АТЛАС**

GSMK CryptoPhone 220	GSM 900\1800(РЕЧЬ)	**CRYTO AG**
TopSec GSM	GSM 900\1800(РЕЧЬ)	**ROHDE&SCHWARZ**
GSMK CryptoPhone G10i	GSM 900\1800(РЕЧЬ)	**CRYTO AG**
GSMK CryptoPhone PSTN/1	PSTN\GSM(РЕЧЬ)	**CRYTO AG**

Специальный сотовый телефон стандарта GSM-900/1800 обеспечивает:

- - в открытом режиме выполнение всех штатных функций стандарта GSM (речь, данные, факс, SMS);
- - в защищенном режиме гарантированную криптографическую защиту речевой информации и аутентификацию абонентов.
- **Тактико-технические характеристики:**
- - абонентский принцип шифрования; аутентификационные данные - криптономер;
- носитель ключевой информации - российская интеллектуальная карта РИК;
- невозможность использования телефона другим лицом в случае его утраты;
- - время синхронизации менее 5 сек.;
- продолжительность работы телефона в активном режиме
- - не менее 3-х часов в защищенном режиме;
- - не менее 3,5 часов в открытом режиме;
- Габаритные размеры: 140х48х25 мм. Вес: 180 г.

Разработчики и производители аппаратуры засекреченной связи

ФГУП НИИ Автоматика
ФГУП Пензенский научно-исследовательский электротехнический институт
ФГУП Калугаприбор
НТЦ «Атлас»

Средства шифрования телефонной связи

Талисман -К	**PSTN(РЕЧЬ, ФАКС, ПК)**	**«СОВТЕХКОМ»(Сертификат ФСТЭК РФ)**
Фрактал А/В	PSTN\ISDN(РЕЧЬ)	**«НОВО»**
Voice coder 2400	PSTN(РЕЧЬ)	«СИГНАЛ-КОМ»(Сертификат Гостехкомиссии при Президенте РФ №50 от 12.09.1996г)
Е-20М	PSTN(РЕЧЬ)	**Пензенский Научно-исследовательский Электротехнический Институт** (Сертификат ФСБ РФ)

«Монолит»	**PSTN(РЕЧЬ,ФАКС)**	**Пензенский Научно-исследовательский Электротехнический Институт**
Талисман-401	**PSTN(РЕЧЬ)**	**«КАЛУГАПРИБОР» (Сертификат ФСБ РФ)**
«Гамма-М»	**PSTN(РЕЧЬ, ПК)**	**НИИ «АВТОМАТИКА» (Сертификат ФСБ РФ)**
«Гамма-СТ-М»	**Станция генерации ключей**	**НИИ «АВТОМАТИКА» (Сертификат ФСБ РФ)**

Схема применения аппаратуры шифрования телефонной связи

АППАРАТУРА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ РЕЧЕВОЙ И ДОКУМЕНТАЛЬНОЙ ИНФОРМАЦИИ (Е-20)

- 1 Установление открытых соединений по сети ТфОП
- 2 Переход в режим шифрования (закрытый режим) нажатием одной кнопки
- 3 Индикация текущего времени, номера вызываемого абонента, открытого или закрытого режимов работы, продолжительности телефонного разговора и установленных режимов работы на табло
- 4 Память на 16 номеров
- **5** Гнездо для ключевого носителя информации

Е-20

Состав:

- > Шифратор
- > РПУ
- > Устройство передачи (приема) документальной информации от ПЭВМ
- > Модем, обеспечивающий работу по коммутируемой сети общего пользования на скоростях 2,4; 4,8; 9,6 кбит/с
- **Обеспечивает:**
- > Режим телефонного аппарата общего пользования
- > Режим громкоговорящего ответа
- > Режим криптографической защиты речи
- > Режим передачи и криптографической защиты данных с встроенным устройством имитозащиты и повышением достоверности информации

Технические характеристики Е-20

- виды передаваемой информации речь, данные
- тип стыка с ООД RS-232C (асинхронный)
- слоговая разборчивость в закрытом режиме 90%
- мощность множества ключей 10^{77}
- длина ключа (бит) 256
- ключевой носитель К1634ДК4
- электропитание 220В 50 Гц;
- потребляемая мощность (не более) 25 В*А
- диапазон рабочих температур от 5°С до 40°С
  габаритные размеры:
- прибора 290*130*280 мм
- блока питания 238*100*110 мм
- масса прибора 5,5 кг
- блока питания 2,9кг

Гамма

Технические параметры

- В режиме шифрования речи используется
- метод линейного предсказания с высоким качеством речевого синтеза.
- Скорость передачи: 2400, 4800, 9600 бит/с
- Длина ключа: 256 бит
- Мощность множества ключей: более 10^{77}
- Электропитание: Сеть переменного тока 220 В, 50 Гц;.
- Потребляемая мощность: 20 ВА.
- Габаритные размеры: 345x270x103 мм
- Масса: 8 кг

Аппарат шифрования речевой, факсимильной и документальной информации Гамма*

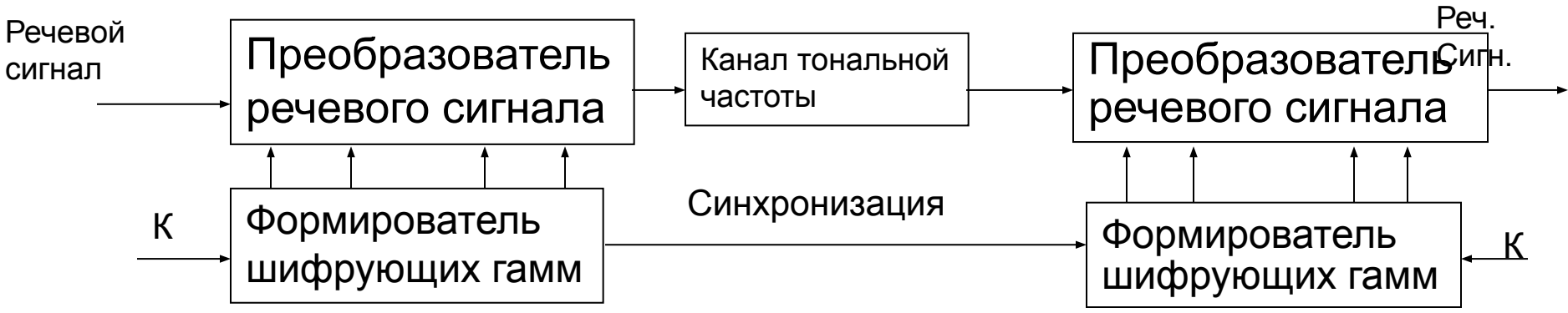
- Аппарат Гамма" предназначен для шифрования речевой, факсимильной и документальной информации с гарантированной стойкостью в дуплексном режиме.
- Аппарат имеет три дуплексных режима связи: режим открытой связи (работает как стандартный телефонный аппарат); режим шифрования речи; режим шифрования данных (факсимильные аппараты и ПЭВМ подключаются по стандартному интерфейсу V.24/V.28(RS-232-C). Аппарат обеспечивает работу через телефонную коммутируемую сеть общего пользования по 2-х проводной линии в соответствии с рекомендациями МККТТ V.22bis и V.32. Скорость передачи данных 2400, 4800 или 9600 бит в секунду выбирается автоматически или вручную.

АППАРАТЫ ШИФРОВАНИЯ ПОТОКОВ ЦИФРОВОЙ ИНФОРМАЦИИ "Е14", "Е14А"

Изделия Е14, Е14А предназначены для криптографической защиты высокоскоростных потоков конфиденциальной информации, передаваемых в дуплексных кабельных, оптоволоконных, радиорелейных и спутниковых каналах цифровых систем уплотнения типа ИКМ.

Параметры информационного потока на входе и выходе аппарата:
Вид информации – цифровая информация, передаваемая со скоростью: Е14 - 2,048 Мбит/с
Е14А - 8,448 Мбит/с
Интерфейс - ITU-T G.703
Ключевая система - композиция долговременного ключа и ключа по алгоритму открытого распределения
Срок действия долговременного ключа – 3 месяца
Длина ключа 256 бит
Мощность множества ключей - 1077
Ввод ключевой информации через малогабаритное переносное устройство считывания УС-К-1
Электронный носитель ключа - типа DATA KEY (1634ДК3).

2. Принципы построения аналоговых систем шифрования



Способы преобразования речи:

-инверсия спектра;

- перестановки частотных полос;

- временные преобразования сигнала

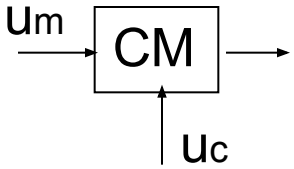
Частотные преобразования сигнала

A

-

Спектр речевого сигнала

Инверсия спектра



cosAcos B=1/2(cos(A+B)+cos(A-B))

Перестановки частотных полос

1 2 3 4 5

Число вариантов перестановок: 5!

Число вариантов инверсии: 2^5

Общее число вариантов преобразования: 3840

2 4 1и 5и 3

Временные преобразования сигнала

Длина сегмента: 20-60 мс
Число сегментов 8-16
Допустимая задержка: 250-500мс

Характеристики аналоговых маскираторов (скремблеров) речи отечественного производства

Маскиратор	СТА-100	Базальт	Туман	Орех-А	MAS-1	Конфи-002	SCR-M1.2	UGRA
Производитель	Маском	Прогресс	Сигнал	Анкад	Сигнал-Рокс	Конфидент	Маском	ПНИЭИ
Технические характеристики:								
способ крипто-прербразования	ВП+КИС	ВП	НКИС	ВП+ КИС+ПМВ	НКИС	ВП	ВП	ЧВП
задержка	320	>300		320		500	450	900
диапазон частот	0.3-3.4 кГц							
число комбинаций пробразований	10^{16}	10^{16}	1	10^{36}	1	$2 \bullet 10^{15}$	$2 \bullet 10^{25}$	нд
длина сегмента (мс)				32		32	32	
вес (кг)	3	3	0,8	0,09	0,28	0,22	1	1
канал связи	городск. и междугор. АТС					радиоканал		

ВП -временные перестановки, ЧВР - частотно-временные перестановки, КИС - коммутируемая инверсия, НКИС - некоммутируемая инверсия, ПМВ - преобразование масштаба времени.