

- Практическое занятие № 1. Применение алгоритма Евклида для нахождения НОД.
- Практическое занятие № 2. Решение линейных диофантовых уравнений.
- Практическое занятие № 3. Решение задач с применением теории чисел.
- Практическое занятие № 4. Применение классических шифров замены.
- Практическое занятие № 5. Применение классических шифров перестановки.

## ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1. ПРИМЕНЕНИЕ АЛГОРИТМА ЕВКЛИДА ДЛЯ НАХОЖДЕНИЯ НОД

**Цель:** изучить применение алгоритма Евклида и бинарного алгоритма для нахождения НОД.

### *Задание:*

1. С помощью алгоритма Евклида найти НОД чисел:
  1. НОД (130 , 15)
  2. НОД (374 , 32)
  3. НОД (5741 , 76)
  4. НОД (846 , 42 )
  5. НОД (5783 , 3420 )
2. С помощью расширенного Алгоритма Евклида найти НОД (a, b) и значения s и t:
  1. a = 57    b = 14
  2. a = 328    b = 36
  3. a = 1179    b = 27
  4. a = 502    b = 52
  5. a = 791    b = 13
3. С помощью бинарного алгоритма найти НОД двух данных чисел, записанных в двоичной системе счисления:
  1. a = 11000001000    b = 11110000100
  2. a = 1000001111    b = 1101100011
  3. a = 1011100101    b = 1000110001
  4. a = 1001011101    b = 1000110001
  5. a = 1000011100    b = 111010001

**Содержание отчета:** Отчет должен содержать пошаговое решение заданий.

### *Контрольные вопросы:*

1. Что понимается под наибольший общий делитель двух целых чисел?
2. Какой алгоритм можно использовать для нахождения наибольший общий делитель?

## ПРАКТИЧЕСКАЯ ЗАНЯТИЕ № 2. РЕШЕНИЕ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ

**Цель:** изучить решение линейных диофантовых уравнений, решение задач с элементами теории чисел.

### *Теоретические вопросы*

1. Понятие неопределенного уравнения.
2. Понятие диофантового уравнения.
3. Понятие линейного диофантового уравнения.

### *Задание:*

1. Найдите частное и общие решения следующих линейных диофантовых уравнений:
  1.  $25x + 10y = 15$
  2.  $19x + 13y = 20$
  3.  $14x + 21y = 77$
  4.  $40x + 16y = 88$
2. Определите, сколько из следующих целых чисел пройдут испытание Ферма на простоту чисел: 100, 110, 130, 150, 200, 250, 271, 341, 561. Используйте основание 2.
3. Найдите результаты следующих операций:
  1.  $22 \bmod 7$
  2.  $140 \bmod 10$
  3.  $-78 \bmod 13$
  4.  $0 \bmod 15$

**Содержание отчета:** Отчет должен содержать пошаговое решение заданий.

### *Контрольные вопросы:*

1. Что такое линейное диофантовое уравнение двух переменных? Сколько решений может иметь такое уравнение? Как может быть найдено решение(я)?
2. Объясните разницу между простым числом и составным целым числом.

## ПРАКТИЧЕСКАЯ ЗАНЯТИЕ № 3. РЕШЕНИЕ ЗАДАЧ С ПРИМЕНЕНИЕМ ТЕОРИИ ЧИСЕЛ

**Цель:** решение задач с элементами теории чисел.

### *Теоретические вопросы*

1. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.
2. Отношения сравнимости. Свойства сравнений. Модулярная арифметика.
3. Сравнения первой степени. Линейные диофантовые уравнения. Расширенный алгоритм Евклида.
4. Арифметические операции над большими числами.

### *Задания:*

1. Найти НОД (1176, 315).
2. Решить систему сравнений

$$a) \begin{cases} x \equiv 2 \pmod{5}, \\ x \equiv 8 \pmod{11}; \end{cases} \quad b) \begin{cases} 4x \equiv 3 \pmod{15}, \\ 3x \equiv 1 \pmod{10}. \end{cases}$$

$$c) \begin{cases} x \equiv 2 \pmod{5}, \\ x \equiv 8 \pmod{11}. \end{cases} \quad d) \begin{cases} 3x + 4y \equiv 29 \pmod{143}, \\ 2x - 9y \equiv -847 \pmod{143}. \end{cases}$$

3. Найти остаток от деления:

$$a) 2^{1050} \text{ на } 17; \quad b) 5^{1995} \text{ на } 9; \quad c) 7^{1018} \text{ на } 19.$$

**Содержание отчета:** Отчет должен содержать пошаговое решение заданий.

### *Контрольные вопросы:*

1. Какие числа называются взаимно простыми?
2. Как выполняются арифметические операции над большими числами?

## ПРАКТИЧЕСКАЯ ЗАНЯТИЕ № 4. ПРИМЕНЕНИЕ КЛАССИЧЕСКИХ ШИФРОВЗАМЕНЫ.

**Цель:** приобрести практический навык в исследовании простейших методов криптографической защиты информации.

### Вопросы для повторения:

1. В чем заключается система шифрования Цезаря?
2. Как используется схема Вижинера?
3. В чем отличие шифра Гронсфельда от шифра Цезаря?
4. Как производится расшифровка текста?

### Методические указания.

#### Шифры простой замены

**Система шифрования Цезаря** - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на  $K$  букв.

Известная фраза Юлия Цезаря

VENI VI D I VICI, где

A	B	C	D	E	F	G	H	I	G	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

пришел, увидел, победил,

зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF при смещении на 4 символа влево.

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером  $5 \times 5$ , заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в зашифрованное сообщение букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

M		↑ T		L		E		X
A		K		F		Q		Y
N		B		R		O		W
C		J		H		D		P
U		I		S		G		V

**Схема шифрования Вижинера.** Таблица Вижинера представляет собой квадратную матрицу с  $n^2$  элементами, где  $n$  — число символов используемого алфавита. На рисунке показана верхняя часть таблицы Вижинера для кириллицы. Каждая строка получена циклическим сдвигом алфавита на символ. Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица шифрования.

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а
в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б
г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в
д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г
е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д

И т.д. до 33-ей строки..

**Таблица Вижинера**

Осуществляется это следующим образом. Из полной таблицы выбирается первая строка и те строки, первые буквы которых соответствуют буквам ключа. Первой

размещается первая строка, а под нею — строки, соответствующие буквам ключа в порядке следования этих букв в ключе шифрования (например ключ «книга»).

Процесс шифрования осуществляется следующим образом:

1. под каждой буквой шифруемого текста записываются буквы ключа. Ключ при этом повторяется необходимое число раз.

2. каждая буква шифруемого текста заменяется по подматрице буквами находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящимися под ними букв ключа.

3. полученный текст может разбиваться на группы по несколько знаков.

Пусть, например, требуется зашифровать сообщение: *максимально допустимой ценой является пятьсот руб. за штуку*. В соответствии с первым правилом записываем под буквами шифруемого текста буквы ключа. Получаем:

максимально допустимой ценой является пятьсот руб. за штуку  
 книгакнигак нигакнигак нигак нигакниг акнигак ниг ак нигак

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й
н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з
г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в
а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я

Дальше осуществляется непосредственное шифрование в соответствии со вторым правилом, а именно: берем первую букву шифруемого текста (М) и соответствующую ей букву ключа (К); по букве шифруемого текста (М) входим в рабочую матрицу шифрования и выбираем под ней букву, расположенную в строке, соответствующей букве ключа (К), — в нашем примере такой буквой является Ч; выбранную таким образом букву помещаем в зашифрованный текст. Эта процедура циклически повторяется до зашифрования всего текста.

Эксперименты показали, что при использовании такого метода статистические характеристики исходного текста практически не проявляются в зашифрованном сообщении. Нетрудно видеть, что замена по таблице Вижинера эквивалентна простой замене с циклическим изменением алфавита, т.е. здесь мы имеем полиалфавитную подстановку, причем число используемых алфавитов определяется числом букв в слове ключа. Поэтому стойкость такой замены определяется произведением стойкости прямой замены на число используемых алфавитов, т.е. число букв в ключе.

Расшифровка текста производится в следующей последовательности:

1. над буквами зашифрованного текста последовательно надписываются буквы ключа, причем ключ повторяется необходимое число раз.

2. в строке подматрицы Вижинера, соответствующей букве ключа отыскивается буква, соответствующая знаку зашифрованного текста. Находящаяся под ней буква первой строки подматрицы и будет буквой исходного текста.

3. полученный текст группируется в слова по смыслу.

Нетрудно видеть, что процедуры как прямого, так и обратного преобразования являются строго формальными, что позволяет реализовать их алгоритмически. Более того, обе процедуры легко реализуются по одному и тому же алгоритму.

Одним из недостатков шифрования по таблице Вижинера является то, что при небольшой длине ключа надежность шифрования остается невысокой, а формирование длинных ключей сопряжено с трудностями.

Нецелесообразно выбирать ключи с повторяющимися буквами, так как при этом стойкость шифра не возрастает. В то же время ключ должен легко запоминаться, чтобы его можно было не записывать. Последовательность же букв не имеющих смысла, запомнить трудно.

С целью повышения стойкости шифрования можно использовать усовершенствованные варианты таблицы Вижинера. Приведем только некоторые из них:

- во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке.
- В качестве ключа используется случайность последовательных чисел. Из таблицы Вижинера выбираются десять произвольных строк, которые кодируются натуральными числами от 0 до 10. Эти строки используются в соответствии с чередованием цифр в выбранном ключе.

Известны также и многие другие модификации метода.

### Шифры сложной замены

**Шифр Гронсфельда** состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Зашифрованное сообщение получают примерно также, как в шифре Цезаря, но используют не одно жестко заданное смещение, а фрагменты ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда сообщение

С	О	В	Е	Р	Ш	Е	Н	Н	О	С	Е	К	Р	Е	Т	Н	О
<b>3</b>	<b>1</b>	<b>4</b>	<b>3</b>	<b>1</b>	<b>4</b>	<b>3</b>	<b>1</b>	<b>4</b>	<b>3</b>	<b>1</b>	<b>4</b>	<b>3</b>	<b>1</b>	<b>4</b>	<b>3</b>	<b>1</b>	<b>4</b>
Ф	П	Ё	З	С	Ь	З	О	С	С	Т	И	Н	С	И	Х	О	Т

**В шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_					
А	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_					
Б	_	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_				
В	Я	_	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_			
Г	Ю	Я	_	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_		
Д	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	
Е	Ь	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_
...	...																																						
Я	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	А	Б	...				
_	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	А	Б	...			

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Зашифрованное сообщение получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

П Р И Е З Ж А Ю \_ Ш Е С Т О Г О  
 А Г А В А А Г А В А А Г А В А А  
 П Н И Г З Ж Ю Ю Ю Ш Е О Т М Г О

Такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

## **Практическая часть.**

### **Задание**

**1.** Придумайте 5 фраз, каждая минимум из 5 слов, и зашифруйте их разными методами (то есть, фразы и методы шифрования не должны повторяться).



## ПРАКТИЧЕСКАЯ ЗАНЯТИЕ № 5. ПРИМЕНЕНИЕ КЛАССИЧЕСКИХ ШИФРОВ ПЕРЕСТАНОВКИ

**Цель:** приобрести практический навык в исследовании простейших методов криптографической защиты информации.

### Вопросы для повторения:

1. Объясните сущность алгоритма перестановки
2. Как производится расшифровка текста?

### Методические указания.

Алгоритм перестановки заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые разновидности этого метода, которые могут быть использованы в автоматизированных системах.

Самая простая перестановка — написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв. Например, из фразы

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ.

получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЬ ТСУП

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, следует его дополнить незначащей буквой (например, О) до числа, кратного пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО.

Тогда шифрограмма, несмотря на столь незначительные изменения, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЪТСУП

Кажется, ничего сложного, но при расшифровке проявляются серьезные неудобства.

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам:

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает метод одиночной перестановки по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово «ЛУНАТИК», получим следующую таблицу:

Л	У	Н	А	Т	И	К		А	И	К	Л	Н	Т	У
4	7	5	1	6	2	3		1	2	3	4	5	6	7
Н	О	Н	С	Б	Н	Я		С	Н	Я	Н	Н	Б	О
Е	Е	О	Я	О	Е	Т		Я	Е	Т	Е	О	О	Е
Я	С	В	Е	Л	П	Н		Е	П	Н	Я	В	Л	С
С	Т	И	Щ	Е	О	Ы		Щ	О	Ы	С	И	Е	Т
Н	А	Т	Е	Е	Н	М		Е	Н	М	Н	Т	Е	А
До перестановки								После перестановки						

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка:

СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются алгоритмы двойных перестановок. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке перестановки проводятся в обратном порядке. Например, сообщение “Приезжаю\_шестого” можно зашифровать следующим образом:

2	4	1	3		1	2	3	4		1	2	3	4	
4	П	Р	И	Е	4	И	П	Е	Р	1	А	З	Ю	Ж
1	3	Ж	А	Ю	1	А	З	Ю	Ж	2	Е	_	С	Ш
2	_	Ш	Е	С	2	Е	_	С	Ш	3	Г	Т	О	О
3	Т	О	Г	О	3	Г	Т	О	О	4	И	П	Е	Р

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка АЗЮЖЕ\_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной

таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 x 3 их 36, для 4 x 4 их 576, а для 5\*5 их 14400.

## Практическая часть.

### Задание

1. Придумайте 4 фразы, каждая минимум из 4 слов, и зашифруйте их разными методами (то есть, фразы и методы шифрования не должны повторяться).
2. Используя таблицу кодировки ASCII, запишите получившиеся результаты в двоичном коде.

**Таблица соответствия кодов ASCII и значений**

Шестнадцатеричная система счисления	ASCII символ	Шестнадцатеричная система счисления	ASCII символ	Шестнадцатеричная система счисления	ASCII символ	Шестнадцатеричная система счисления	ASCII символ	Шестнадцатеричная система счисления	ASCII символ
20	пробел	40	@	60	`	C0	A	E0	a
21	!	41	A	61	a	C1	Б	E1	б
22	"	42	B	62	b	C2	В	E2	в
23	#	43	C	63	c	C3	Г	E3	г
24	\$	44	D	64	d	C4	Д	E4	д
25	%	45	E	65	e	C5	Е	E5	е
26	&	46	F	66	f	C6	Ж	E6	ж
27	'	47	G	67	g	C7	З	E7	з
28	(	48	H	68	h	C8	И	E8	и
29	)	49	I	69	i	C9	Й	E9	й
2A	*	4A	J	6A	j	CA	К	EA	к
2B	+	4B	K	6B	k	CB	Л	EB	л
2C	,	4C	L	6C	l	CC	М	EC	м
2D	-	4D	M	6D	m	CD	Н	ED	н
2E	.	4E	N	6E	n	CE	О	EE	о
2F	/	4F	O	6F	o	CF	П	EF	п
30	0	50	P	70	p	D0	Р	F0	р
31	1	51	Q	71	q	D1	С	F1	с
32	2	52	R	72	r	D2	Т	F2	т
33	3	53	S	73	s	D3	У	F3	у
34	4	54	T	74	t	D4	Ф	F4	ф
35	5	55	U	75	u	D5	Х	F5	х
36	6	56	V	76	v	D6	Ц	F6	ц
37	7	57	W	77	w	D7	Ч	F7	ч
38	8	58	X	78	x	D8	Ш	F8	ш
39	9	59	Y	79	y	D9	Щ	F9	щ
3A	:	5A	Z	7A	z	DA	Ъ	FA	ъ
3B	;	5B	[	7B	{	DB	Ы	FB	ы
3C	<	5C	\	7C		DC	Ь	FC	ь
3D	=	5D	]	7D	}	DD	Э	FD	э
3E	>	5E	^	7E	~	DE	Ю	FE	ю
3F	?	5F	_	7F	•	DF	Я	FF	я