**СРСП 1.** Шифр с использованием кодового слова.

**Форма и содержание отчета**

Отчет должен содержать:

1. Титульный лист установленного образца.
2. Описание комплексного поиск возможных методов доступа.
3. Сравнительный анализ рассмотренных терминалов защищенной информационной системы.
4. Перечень использованных информационных источников.

Отчет выполняется на листах формата А4 рукописным или печатным способом. При рукописном оформлении отчета текст следует излагать четким почерком чернилами черного цвета.

Шифр **Цезаря** — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации- шифр простой замены.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки. Естественным развитием шифра Цезаря стал шифр Виженера. С точки зрения современного криптоанализа, шифр Цезаря не имеет приемлемой стойкости.



Рисунок 1 Шифр Цезаря

#### Математическая модель

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:





где x — символ открытого текста
y — символ шифрованного текста
n — мощность алфавита (кол-во символов)
k — ключ.
Можно заметить, что суперпозиция двух шифрований на ключах k1 и k2 — есть просто шифрование на ключе k1+k2. Более общее, множество шифрующих преобразований шифра Цезаря образует группу Z.

Алфавит:



Ответ: «Пхнфчузхещнд»

**Пример вскрытия шифра Цезаря**

 Пусть дана следующая криптограмма:

**Цярснсмщи ямякзж онкдждм мд снкыйн гкю онгрсямнбнцмщф**

**йпзоснвпялл мн б гптвзф рктцяюф нм ркнемдд**

Для расшифровки подсчитаем, сколько раз встречается в ней каждая буква. Результаты сведем в таблицу:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Буква | н | м | я | к | д | с | р | г | о | п | з | ф | ц | б | в | ж | й | л | т | щ | ю | е | и | ы |
| Число вхождений | 11 | 9 | 6 | 6 | 5 | 5 | 4 | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 1 |

Наиболее часто встречающийся символ "и" скорее всего, означает букву "о". Сделав такое предположение, рассмотрим следующий по частоте символ "м". В криптограмме имеется двухбуквенное сочетание "мн", и так как "н" - это "о", то символ "м" соответствует согласной.

Среди согласных в русском языке выделяются по частоте буквы "т" и "н", и потому "м" скорее всего, означает одну из этих букв, Разберем случай, когда "м" означает "н", предоставляя читателю самостоятельно убедиться, что другая возможность не приводит к осмысленной расшифровке криптограммы.

Если "м" - это "н", то в сочетании "мд", встречающемся в криптограмме, "д" означает скорее всего гласную. Из наиболее вероятных для "д" вариантов "а", "е", "и" выбираем "е", потому что лишь в этом случае имеющееся в криптограмме слово "ркнемдд" допускает осмысленную расшифровку. Итак, три знака разгаданы: "н" - это "о", "м" - "н", "д" - "е". Обращаемся к сочетанию "ямякзж". В нем "я" может означать лишь гласную "а" или "и". Любые другие возможности заведомо не допускают разумного прочтения слова "ямякзж". Испытаем букву "а". Подставляя вместо "я" букву "а", вместо "м" *—* "н"*,* вместо других знаков - точки, получим недописанное слово "ана...". В словаре имеется всего лишь несколько слов из 6 букв с таким началом: "анализ", "аналог", "ананас", "анатом". Из них годится лишь первое. Если вместо "я" подставить букву "и", то получится шестибуквенное сочетание с началом "ини", но в словаре нет ни одного такого слова. Расшифрованы еще четыре буквы: "я", "к", "з", "ж". Они означают соответственно "а", "л", "и", "э".

В слове "онкждм" известны все символы, кроме первого. Заменяя их буквами, получаем: ".олезен", Ясно, что неизвестная буква - это "п". Значит, "о" расшифровывается как "п".

Не разгаданы еще два сравнительно часто встречающиеся знака "о" и "р". Рассмотрим сочетание "ркнемдд", означающее ".ло.нее". Имеется немного вариантов его прочтения, один из них - "сложнее", и, следовательно, скорее всего "р" - это "с", "е"- это "ж".

Из нерасшифрованных еще знаков чаще всего встречается "с". В соответствии с таблицей  среди оставшихся согласных наибольшую частоту имеет "т", Естественно, поэтому предположить, что "с" означает "т".

Попытаемся восстановить зашифрованный текст, подставляя вместо разгаданных знаков соответствующие им буквы:

**.астотн.. анализ полезен не то..ко .л. по.стано.о.н.. ..ипто..а..**

**но . ….и. сл..а.. он сложнее**

 Ясны (по контексту), по крайней мере: ".астотн.." означает "частотный", "тол..о" – "только", ".л." – "для". С учетом новой информации текст примет следующую форму:

 **Частотный анализ полезен не только для подстано.очны. к.ипто..а..**

**но . д...и. сл.чая. он сложнее**

 Окончательная расшифровка не представляет труда. Текст таков:

 **Частотный анализ полезен не только для подстановочных крипто­грамм, но в других случаях он сложнее**