***Задание №1***

1. Зашифровать сообщение одним из следующих методов:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Последняя цифра студенческого билета | | | | | | | | | | |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
| Сообщение | 1 | 2 | 3 | 4 | 5 | 5 | 4 | 3 | 2 | 1 |
| Метод | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 5 | 4 | 3 |
| Предпоследняя цифра студенческого билета | | | | | | | | | | |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
| Ключевое слово/ магический квадрат/ размер блока | - | Следующий | - | 4х4 | Самоучитель | - | Волшебный | Конвертация | 4х4 | - |

*Варианты сообщений*

1. Под информационной безопасностью следует понимать защиту интересов субъектов информационных отношений

2. Под доступом к информации понимается ознакомление модификация и уничтожение информации

3. Правила разграничения доступа служат для регламентации права доступа субъекта доступа к объекту доступа

4. Доступность — это возможность за приемлемое время получить требуемую информационную услугу

5. Конфиденциальность данных это статус предоставляемый данным и определяющий требуемую степень их защиты

*Варианты методов*

а) Метод простой перестановки

б) Метод одиночной перестановки по ключу

в) Метод двойной перестановки сообщения

г) Шифрование магическими квадратами

д) Биграммный шифр Плейфера