**Разложение группы на смежные классы по подгруппе**

Данная операция лежит в основе как защиты информации от непреднамеренного доступа к ней, так и для защиты информации от ошибок или помех.

Подгруппа — это есть подмножество группы на котором задана операция группы: таблица Кэлли в группе должна совпадать с таблицей Кэлли в подгруппе.

Количество подгрупп определяется по теореме Ла Гранджа как: «Деление без остатка порядка группы на порядок подгруппы».

Для разложения группы на классы удобно представить эту операцию в виде таблицы. Первая строка — это все элементы подгруппы, вторая строка: надо взять элемент группы, который не принадлежит первой строке или подгруппе. Третья строка: берём элемент группы, который не принадлежит ни одной из строк и так далее.

Первый столбец этой таблицы называется столбцом, образующим смежные классы

Замечания:

* Для исправления ошибок в качестве столбца образующих смежные классы (столбца лидеров смежных классов) используется самый крайний левый столбец.