Математические основы защиты информации (МОЗИ).

Конечно, науки с таким названием не существует. С проблемой, вызвавшей появление в учебных планах некоторых ВУЗов этой странной аббревиатуры (МОЗИ) я столкнулся еще в середине 80-х, когда ко мне пришли знакомые радиотехники с просьбой о помощи. Они принесли статью из какого-то своего специализированного журнала, где на первых станицах говорилось, какую схему требуется сконструировать, в конце эта схема была нарисована, а между этим был десяток страниц абсолютно непонятной им математики --- и это при том, что математическая подготовка радиотехников была одной из самых высоких среди инженерных специальностей. Причем надо сказать, что эта математика не были ни особенно трудной, ни сверхсовременной. Беда была в том, что это была совсем другая математика, та, которую «технари» традиционно относили к «этой вашей абстрактной башне из слоновой кости», искусству ради искусства, которое «никогда никому ни для чего толкового не пригодится». Пригодившиеся разделы вполне традиционной арифметики и алгебры и составляют теперь основу так экзотически называемого курса. Замечательно, что востребованным оказался один из красивейших сюжетов современной (по меркам трехтысячелетней истории) математики --- речь идет о конечных полях, появившихся в начале 19 века в работах Галуа. Элементарному введению в эту тематику и будет посвящен наш курс. Будет рассказано также, как это все используется в радиолокации и системах опознавания «свой-чужой», но здесь мы ограничимся только принципиальными схемами применения: реальные системы и их технические реализации «в железе» и представляют собой уже отдельную область. Никаких предварительных знаний, выходящих за рамки школьной математики, от слушателей не требуется; очень приветствуются навыки устного счета и любовь к целым числам.