Сорокина С.В., (2 год обучения)

**Тема доклада: Двойственность матроидов и совершенные идеальные схемы разделения секрета**

Научный руководитель: д. ф.-м. н., профессор кафедры «Высшая и прикладная математика» Титов С.С.

В работе рассматривается один из методов защиты информации – разграничение доступа к конфиденциальной информации посредством схем разделения секрета, в которых любая разрешённая группа пользователей может однозначно восстановить секрет (т.е. секретную информацию, например, пин-код или пароль) по известным его частям, а ни одна из неразрешённых групп пользователей не сможет получить никакой информации о секрете (совершенность схемы).

Тема исследования направлена на решение математических проблем в области **совершенных идеальных** схем разделения секрета, в которых размер частей секрета равен размеру самого секрета, и связана с изучением таких комбинаторных объектов как матроиды.

Для решения проблемы построения схемы разделения секрета по её матроиду в работе сформулирована гипотеза, что код идеальной схемы разделения секрета определяется через список циклов матроида, двойственного к данному. Эта гипотеза проверена на классе матроидов, представимых как векторные над конечными полями, через двойственность порождающей и проверочной матрицы кода.

Для решения проблемы описания многомерных векторных схем разделения секрета производятся исследования на матроидах, не представимых как векторные ни над какими полями. В результате исследований будет определена категория матроидов, для которых выдвинутая гипотеза справедлива, и разработана методика построения кода идеальной совершенной схемы по её структуре доступа.

Для решения проблемы существования нелинейных схем разделения секрета предлагается применить теорию двойственности к новым недавно открытым классам матроидов