

*Защита информации: организация,
постановки задач и методы*

А.В. Галатенко, В.А. Носов, А.Е. Панкратьев

Московский государственный университет имени М.В.Ломоносова
Москва, Россия

Москва, 15 апреля 2020г.

Организационные варианты

Заниматься исследованиями в области защиты информации на кафедре MaTIC можно:

- выбрав соответствующую специализацию (группу защиты информации);
 - плюсы: продуманный набор спец. курсов
 - минусы: дополнительная нагрузка (в виде продуманного набора спец. курсов)
- выбрав математический поток кафедры MaTIC;
- выбрав экономический поток кафедры MaTIC.

Возможные научные руководители



Валентин Александрович Носов,
vnosov40@mail.ru

Тематика исследований:

- математические модели криптографических стандартов и их свойства;
- комбинаторные и криптографические объекты, их свойства и построение;
- шифрующие автоматы в булевой параметризации;
- совершенные шифры и латинские квадраты.

Возможные научные руководители

Антон Евгеньевич Панкратьев,
aankrat@intsys.msu.ru



Тематика исследований:

- квазигруппы и латинские квадраты;
- гиперболические группы;
- перспективные криптоалгоритмы;
- компьютерная алгебра.

Возможные научные руководители

Алексей Владимирович Галатенко,
agalat@intsys.msu.ru



Тематика исследований:

- математическое моделирование защищенных систем;
- выявление вторжений;
- аппаратная реализация криптопримитивов;
- криптографические приложения квазигрупп.





Примеры постановок задач

- разработка новых криптографических примитивов (шифров, хэш-функций) на основе перспективных алгебраических и комбинаторных структур; анализ стойкости и возможности эффективной реализации;
- исследование и эффективная реализация новых криптографических стандартов (национальных, отраслевых, корпоративных...);
- исследование свойств перспективных алгебраических и комбинаторных структур (квазигрупп, параметрических систем подстановок) с точки зрения потенциальных криптографических приложений;
- разработка “кремниевого компилятора” для криптоалгоритмов;
- реализация различных компонент систем активного аудита (предупреждения вторжений, обнаружения вторжений).

Используемый арсенал

- алгебра и алгебраические структуры;
- комбинаторика и мощностные оценки;
- компьютерное моделирование и генерация богатых гипотез;
- конечнозначные логики и методы проверки полноты;
- математическая статистика и проверка гипотез;
- распознавание образов, разладка и выявление нетипичности;
- синтез схем из функциональных элементов;
- теория автоматов и регулярные языки;
- теория вероятностей и MCMC;
- теория сложности, полиномиальность и NP-полнота.

Литература

-  В. А. Носов. *Построение классов латинских квадратов в булевой базе данных*. Интеллектуальные системы, 4(3–4):307–320, 1999.
-  V. A. Nosov. *Constructing families of latin squares over boolean domains*. Boolean Functions in Cryptology and Information Security, 200–207, 2008.
-  V. A. Nosov, A. E. Pankratiev. *On functional specification of latin squares*. Journal of Mathematical Sciences, 169(4):533–540, 2010.
-  А. В. Галатенко, А. Е. Панкратьев. *О сложности проверки полиномиальной полноты конечных квазигрупп*. Дискретная математика, 30(4):3–11, 2018.