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, 26 марта 2021г.

Несколько советов

- Постарайтесь выбрать научного руководителя по душе:
  - сходите на спец. семинар;
  - поговорите с учениками;
  - поговорите с предполагаемым руководителем о возможных постановках задач, требованиях, перспективах...
- Постарайтесь выбрать задачу, которой было бы интересно заниматься:
  - конечно, суетиться не стоит...
  - но и откладывать на год тоже плохая идея;
  - попросите предоставить статьи и/или ссылки, чтобы хотя бы по диагонали посмотреть на предполагаемую предметную область;
  - работа над задачей должна приносить удовольствие и удовлетворение.

Возможные научные руководители

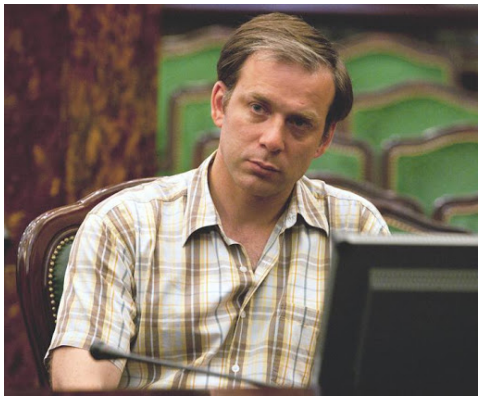
Валентин Александрович Носов,
vnosov40@mail.ru

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,
apankrat@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.


A. V. Galatenko, V. A. Nosov, A. E. Pankratiev. *Latin Squares over Quasigroups.* Lobachevskii Journal of Mathematics, 41(2):194–203, 2020.


A. V. Galatenko, A. E. Pankratiev, V. M. Staroverov. *Efficient verification of polynomial completeness of quasigroups.* Lobachevskii Journal of Mathematics, 41(8):1444–1453, 2020.

Некоторые публикации учеников


А. В. Годнева. *Умножение с параметром и его применение в криптографии.* Интеллектуальные системы. Теория и приложения. 18(1):61–74, 2014.


Д. Е. Александров. *Об оценках мощности некоторых классов регулярных языков.* Дискретная математика, 27(2):3–21, 2015.


А. В. Поляков. *Метод идентификации личности по отпечаткам пальцев на основе сферического локально-чувствительного хэширования.* Программная инженерия, 5:207–214, 2017.


С. О. Супрунюк, Е. А. Курганов. *О глубине аппаратной реализации потокового шифра ZUC.* Программная инженерия, 9(5):221–227, 2018.


И. Б. Казаков. *Критерий надежности канала с запрещениями.* Интеллектуальные системы. Теория и приложения. 23(2):33–56, 2019.


К. Д. Царегородцев. *О взаимно однозначном соответствии между правильными семействами булевых функций и рёберными ориентациями булевых кубов.* Прикладная дисктерная математика, 48:16–21, 2020.


D. E. Alexandrov, S. A. Nersisyan. *Identification of contact angle and heterogenity detection in tactile images.* International Journal of Biology and Biomedical Engineering, 12:186–191, 2018.


S. A. Nersisyan *et al.*. *A Post-Processing Algorithm for miRNA Microarray Data.* International Journal of Molecular Sciences, 21(4), 2020.