СЕКЦИЯ 4. «ТЕОР.ПРОГРАММИРОВАНИЕ И ЗАЩИТА ИНФОРМАЦИИ»

Кириллова Ю.П. (4 к., 1 гр.) Криптоанализ одного обобщения криптосистемы Меркля-Хеллмана.

Научный руководитель – доц. **Деундяк В.М.**

(*Кафедра алгебры и дискретной математики*)

Исследуется стойкость модификации В.О.Осипяна классической рюкзачной криптоситемы Меркля-Хеллмана. На основе криптоалгоритма Шамира для классической системы Меркля-Хеллмана построен криптоалгоритм для этой модификации.

Бибов А.Ю. (маг., 1г.) О распространении декодеров Сидельникова на класс кодов БЧХ

Научный руководитель — доц. **Деундяк В.М.**

(*Кафедра алгебры и дискретной математики)*

Рассмотренно распространение декодеров Сидельникова для кодов Рида-Соломона на семейство кодов Боуза-Чоудхури-Хоквингема. Представленны соответствующие алгоритмы декодирования и их программная реализация, основанная на разработанной автором библитеке GFL, которая предназначенна для вычислений в конечных полях.

Евпак С.А. (маг., 1 г.) Возможность применения обобщенных кодов Рида-Маллера в модели широковещательного шифрования

Научный руководитель – асс. **Мкртичян В.В.**

(*Кафедра алгебры и дискретной математики*)

Рассмотрены обобщенные коды Рида-Маллера. Исследована теоретическая возможность их применения в модели широковещательного шифрования.

Толмачев О.В., Фаткуллин Р.И. (маг., 1 г.) Исследование кодеков семейств циклических кодов, "близких" к кодам БЧХ.

Научный руководитель – доц. **Кряквин В.Д.**

(Кафедра алгебры и дискретной математики)

Исследуются циклические коды, отличие в построении которых от кодов Боуза-Чоудхури-Хоквингема состоит в том, что вместо 2t корней порождающего многочлена кода Боуза-Чоудхури-Хоквингема берется 2t корней с пропуском одной степени между последним и предпоследним корнем или с пропуском одной степени между третьим и вторым с конца корнем. Модификацией алгоритма Питерсона-Горенстейна-Цирлера строится декодер анализируемых кодов. В заключении приводятся результаты некоторых из проведенных авторами численных экспериментов и расчетов.

Жданова М.А. (маг., 1г.) Обобщенная марковская математическая модель источника ошибок в q-ичном цифровом канале n физических состояний.

Научный руководитель — доц. **Деундяк В.М.**

(*Кафедра алгебры и дискретной математики)*

Рассмотрена марковская математическая модель источника ошибок в q-ичном цифровом канале n физических состояний, сочетающая в себе преимущества двух подходов к моделированию источников ошибок - моделирования на основе цепей Маркова и q-ичной QPn-модели. Представлена комьютерная модель, построенная на основе рассматриваемой модели, а также ее программная реализация.

Рева М.С. (3 к., 1 гр.) Разработка программного средства криптоанализа шифра замены.

Научный руководитель — доц. **Деундяк В.М.**

(*Кафедра алгебры и дискретной математики)*

Представленное программное средство криптоанализа шифра замены позволяет производить атаку на ключ методом частотного анализа. Может использоваться с целью обучения в курсе «криптографии».

Горячий М.С. (4к., 1 гр.) Системный стеганографический анализ радиосигналов.

Научный руководитель — асс. **Маевский А.Э.**

(*Кафедра алгебры и дискретной математики)*

Рассматривается задача стеганографического анализа (обнаружение и классификация) радиосигналов, принимаемых на фоне шумов высокой интенсивности. На основе анализа существующих методик разработан и программно реализован комплексный подход к обработке радиосигналов, проведен ряд вычислительных экспериментов. Разработаны рекомендации по использованию в ряде практических задач.

Летуновский О.И. **Модификация криптосистемы RSA**

Научный руководитель – проф. **Пилиди В.С.**

(Кафедра информатики и вычислительного эксперимента)

Разработана модификация и выполнена программная реализация обобщения криптосистемы RSA на случай полиномиального кольца.