СЕКЦИЯ 4. «ТЕОР. ПРОГРАММИРОВАНИЕ И ЗАЩИТА ИНФОРМАЦИИ»

Михайлова Е.А. (4 к., 1 гр.) Применение структурированных матриц для борьбы с помехами в канале со стираниями.
Научный руководитель — доц. **Деундяк В.М.**
(Кафедра алгебры и дискретной математики)
Для канала со стираниями строятся кодеки, основанные на применении матриц Коши и матриц Вандермонда. Рассматриваются быстрые обращения матриц Коши. Обсуждается задача об обратимости квадратных подматриц матрицы Вандермонда.

Гриценко В. В. (4 к., 1 гр.) Алгоритм построения всех обратимых циркулянтов над поляии Галуа и его применение в задачах защиты информации.
Научный руководитель — к.т.н. **Косолапов Ю. В.**
(Кафедра алгебры и дискретной математики)
Обратимые циркулянтные матрицы (циркулянты) можно использовать в качестве случайных кодеков при защите информации в канале перехвата второго типа. В работе проведен анализ циркулянтов над конечными полями на обратимость и описывается алгоритм построения множества всех обратимых циркулянтов заданного порядка над фиксированным конечным полем.

Сопин В.В. (3 к., 1 гр.) Решение полиномиальных уравнений над полями Галуа и их применение в задачах защиты информации.
Научные руководители — доц. **Деундяк В.М.,** асп.**Чекунов Е.С.**
(Кафедра алгебры и дискретной математики)
Проведено эксперементальное исследования различных методов решения полиномиальных уравнений над конечными полями. Особое внимание уделено полученному недавно алгоритму Федоренко над полями характеристики 2. Введено обобщение схемы Горнера для полей характеристики больше 2.

Пушкарь В.Ю. (5 к., 1 гр.) Примеры криптографических протоколов на группах кос и их анализ.
Научный руководитель — доц. **Деундяк В.М.**
(Кафедра алгебры и дискретной математики)
Рассматриваются две интерпретации протокола выработки общего секретного ключа Диффи-Хэллмана: Ко-Ли и Аншель-Аншель-Голдфилд. Приводится компьютерная модель данного протокола интерпретации Ко-Ли. Обсуждаются известные методы взлома и криптографическая стойкость двух интерпретаций.

Жданова М.А. (маг., 2 г.) О применении теории скрытых марковских моделей к моделированию источников ошибок.
Научный руководитель — доц. **Деундяк В.М.**
(Кафедра алгебры и дискретной математики)
Рассматривается модель источника ошибок в q-ичном цифровом канале передачи данных, построенная на основе скрытой марковской модели. Предлагается модификация алгоритма прямого хода для представленной модели.

Герасимова А.Ю. (4 к.) Дискретное преобразование всплесков, реализация и применение
Научный руководитель – доц. **Кряквин В.Д.**
(Кафедра алгебры и дискретной математики)
С помощью реализованного одно и двумерного преобразования всплесков И. Добеши численно анализируются его возможности по сжатию и обработке информации.

Бессуднова Н. В. Исследование структуры двоичных кодов Рида-Маллера.
Научный руководитель - к.т.н. **Мкртичян В. В.**
(Кафедра алгебры и дискретной математики)
В докладе рассматривается структура порождающих матриц для двоичных кодов Рида-Малера с параметрами m и r. Доказываются утверждения о весе кодовых слов.

Таран А.А. (4к.) Выявление аномалий в сети с использованием алгоритма Фишера
Научный руководитель – доц. **Нестеренко В.А.**
(*Кафедра информатики и вычислительного эксперимента*)
Используется алгоритм Фишера как метод нахождения характеристики состояния системы позволяющей эффективно разделять нормальные и аномальные состояния.

Бредихин Д.П. (5к.) Сокрытие информации о процессах в ОС Windows
Научный руководитель – доц. **Нестеренко В.А.**
(*Кафедра информатики и вычислительного эксперимента*)
Рассматривается метод, демонстрирующий комплексный подход к скрытию процессов. В предлагаемом подходе используются следующие методики: исключение записи о целевом процессе из списка PsActiveProcesses, исключение таблицы дескрипторов целевого процесса из списка таблиц дескрипторов, исключение записи о целевом процессе и его потоках из таблицы дескрипторов процессов и потоков PspCidTable, исключение записей о целевом процессе и его потоках из таблицы дескрипторов процесса csrss.exe.

Гармашова Ю. (4 к., 1 гр.) Реализация алгоритмов эллиптической криптографии
Научный руководитель — доц. **Савельев В.А.**
(Кафедра информатики и вычислительного эксперимента)
Представлена реализация алгоритма Эль-Гамаля на основе эллиптической арифметики, встроенная в пакет openSSL.

Попова И.Д. (4 к., 11 гр.) Модификация и программная реализация одного стеганографического алгоритма
Научный руководитель – проф. **Пилиди В.С.**
(*Кафедра информатики и вычислительного эксперимента*)
Написана программа, реализующая стеганографический алгоритм, основанный на алгоритме фрактального сжатия изображений и использовании кода Рида – Маллера.

Буртыка Ф.Б. (маг., 1 г.), Трепачева А.В. (маг., 1 г.) Полностью гомоморфная криптосистема скрывающая схему вычислений
Научный руководитель – проф. **Пилиди В.С.**
(*Кафедра информатики и вычислительного эксперимента*)
Предложен метод построения полностью гомоморфных криптосистем, реализующий возможность скрытия схем вычислений над открытыми текстами. Приведен пример построения такой криптосистемы на основе криптосистем Пэйе и RSA.

Евпак С.А. (маг., 2 г.) Модель защиты данных от НСД, основанная на помехоустойчивых кодах Рида-Маллера и списочном декодировании.

Научный руководитель — асс. **Мкртичян В.В.**

(*Кафедра алгебры и дискретной математики)*

Исследуется проблема защиты легально тиражируемых данных от несанкционированного доступа. Для q-ичных кодов Рида – Маллера получены достаточные условия возможности их применения в схемах специального широковещательного шифрования (ССШШ). Доказано, что классические бинарные коды Рида-Маллера в ССШШ применять нельзя. Показана возможность обнаруживать не только одного, но и нескольких злоумышленников. Построена математическая модель эффективной ССШШ на основе q-ичных кодов Рида-Маллера.