Примерный перечень тем курсовых работ
по дисциплине “Криптографические методы защиты информации”
профессор каф. ИБиТУ Рацеев С.М.

1. Реализация схемы разделения секрета Фельдмана-Шамира.
2. Реализация схемы разделения секрета Асмута-Блума с использованием GPU.
3. Схемы разделения секрета для произвольных структур доступа.
4. Модели и алгоритмы визуальной криптографии.
5. Использование криптографической программной библиотеки Crypto++.
6. Использование криптографической программной библиотеки BouncyCastle в Java и C# программах.
7. Использование криптографического пакета OpenSSL.
8. Клиент-серверная реализация модифицированного протокола аутентификации Шнорра.
9. Программная реализация криптографического протокола с нулевым разглашением на основе задачи о нахождении гамильтонова цикла в графе с использованием технологии CUDA.
10. Программная реализация протокола аутентификации на основе графических паролей.
11. Протоколы аутентификации, основанные на нескольких вычислительно сложных задачах.
12. Программная реализация шифра AES с использованием аппаратного ускорения и GPU.
13. Высокоскоростная программная реализация шифра “Кузнечик” из ГОСТ Р 34.12-2015.
14. Программная реализация гибридного шифра DHAES.
15. Программная реализация некоторых “облегченных” блочных шифров и проверка их на экстремальность.
16. Симметричные схемы аутентификации сообщений, основанные на блочных шифрах.
17. Построение совершенных имитостойких шифров на основе латинских прямоугольников.
18. Получение критериев совершенных шифров при различных начальных условиях.
19. Построение и реализация совершенных и (k|y)-совершенных шифров.
20. Реализация схем разделения секрета на группы участников.
21. Почти пороговые схемы разделения секрета.

Примерный перечень тем курсовых работ
по дисциплине “Методы алгебраической геометрии в криптографии”
профессор каф. ИБиТУРацеев С.М.

1. Программная реализация гомоморфного шифра Джентри.
2. Программная реализация гомоморфного шифра на основе матричных полиномов.
3. Построение и реализация оптимальных кодов аутентификации.
4. Постквантовые электронные подписи, основанные на хеш-функциях.
5. Построение хеш-функций на основе нейронных сетей.
6. Построение и реализация схемы Шамира на основе конечных полей.
7. Построение и реализация совершенных шифров на основе ортогональных таблиц, стойких к имитации и подмене.
8. Программная реализация рюкзачной криптосистемы Шора-Ривеста на основе конечных полей.
9. Программная реализация схемы Блома предварительного распределения ключей на основе конечных полей.
10. Программная реализация гибридного шифра DHAES на эллиптических кривых.
11. Реализация протокола аутентификации Шнорра на эллиптических кривых.
12. Реализация протокола аутентификации Окамото на эллиптических кривых.
13. Реализация семейства протоколов MTI на эллиптических кривых.
14. Криптосистемы, основанные на группах кос.
15. Криптосистемы, основанные на решетках.

Перечень направлений дипломных работ
профессор каф. ИБиТУ Рацеев С.М.

1. Модели и методы распознавания открытых текстов.
2. Криптоанализ шифров с помощью генетических алгоритмов.
3. Совершенные имитостойкиешифры.
4. Шифры, близкие к экстремальным.

5. Итеративные блочные шифры.
6. Шифры, не распространяющие искажений.
7. Контроль целостности данных с помощью хеш-функций.
8. Оптимальные коды аутентификации.
9. Совершенные схемы разделения секрета.
10. Криптосистемына эллиптических кривых.
11. Постквантовые криптосистемы.
12. Криптосистемы на основе нейронных сетей.
13. Генераторы псевдослучайных и случайных последовательностей.
14. Шифрование изображений и видео.

Примерный перечень тем для НИР
профессор каф. ИБиТУ Рацеев С.М.

1. Построение совершенных шифров замены с неограниченным ключом по заданному набору параметров.
2. Применение генетических алгоритмов в задачах криптоанализа.
3. Применение математических моделей открытых текстов в задачах исправления искаженных криптограмм.
4. Программная реализация и сравнительный анализ российских стандартов электронной подписи ГОСТ Р 34.10-X.
5. Разработка программных средств визуального разделения секрета.
6. Построение и реализация совершенных шифров, стойких к имитации и подмене.
7. Построение и реализация высокоскоростных алгоритмов шифрования изображений и видео.
8. Разработка программных средств высокопроизводительных схем разделения секрета.
9. Построение и реализация совершенных и (k|y)-совершенных шифров.
10. Построение и реализация совершенных имитостойких шифров на основе комбинаторных объектов.
11. Построение и реализация оптимальных кодов аутентификации с неограниченным ключом на основе ортогональных таблиц.
12. Высокоскоростная реализация хэш-функции ГОСТ Р 34.11-2012 и исследование ее на сбалансированность.
13. Программная реализация и исследование некоторых симметричных шифров на экстремальность.
14. Построение и реализация высокоскоростных алгоритмов шифрования изображений и видео с использованием постквантовой криптографии.