**СПИСОК ТЕМ КУРСУ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

1. Угрозы информационной безопасности. Атаки на информацию. Целостность. Конфиденциальность. Аутентификация.

2. Базовые криптографические операции: замена, перестановка, гаммирование. Симметричное и несимметричное шифрование. Криптосистема. Криптостойкость. Рассеивание и запутывание.

3. Атаки криптоаналитика: на основе открытых текстов, на основе выбранных открытых текстов, на основе закрытых текстов. Частотный анализ.

4. Докомпьютерные шифры. Афинный шифр. Шифр Хилла. Шифр Вижинера. Стеганография.

5. Делитель нуля, обратимость по mod n. Обращение по mod n. Соотношение Безу. Расширенный алгоритм Евклида.

6. Абсолютно-стойкий шифр, невозможность его применения на практике. Потоковые шифры.

7. Симметричные компьютерные шифры. Сеть Фейстеля. Подстановочно-перестановочная сеть. DES, AES, ГОСТ.

8. Несимметричное шифрование RSA. Криптостойкость RSA.

9. Хэш-функция. Парадокс дней рождения. Цифровая подпись. Цифровая подпись с дополнением. Цифровая подпись с восстановлением хэш-кода.

10. Неэффективность атак полного перебора при достаточной длине ключа. Закон Амдала.