

## **Темы к семинару 8 декабря. ТАиШ. Часть 2. Теория шифров.**

Семинар будет проходить по расписанию, в понедельник, 8 декабря с 08.00 до 11.25.

Необходимо подготовить сообщение на 5 -6 минут с презентацией (не использовать экзотические цвета), можно подглядывать в печатные материалы, но не читать, свой метод шифрования надо хорошо понимать. Рядом с темой указана фамилия докладчика.

Готовясь докладу знать ответы на вопросы:

- как зашифровать текст
- как расшифровать
- преимущества
- недостатки
- подготовить пример зашифрование/дешифрование

Бойченко Александр	Квадрат Полибия
Боридько Андрей	Шифр Гронсвельда
Видишев Артём	Шифр Фальконера
Волкова Арина	Шифр Плейфера (Уитстона)
Гладкова Анна	Шифр Бэкона
Гончаров Роман	Уточнить у преподавателя тему
Горбачева Алена	Шифр Наполеона
Египкин Владимир	Шифровальное устройство Уодсворта
Зубков Дмитрий	Дисковый шифратор Джейфферсона
Иваниченко Владимир	Уточнить у преподавателя тему
Ивахненко Владимир	Таблица Порта
Каплунов Тимур	Шифр Ардженти
Карабанов Владимир	Таблица Тритемия
Киреев Никита	Решетка Кардано
Колмыков Никита	Шифр Вернама
Копанева Екатерина	Шифр Ришелье (прямоугольник)
Короткиян Артём	Концепция избыточной информации в работах Шеннона
Кучеров Константин	Шифр Аве Мария

Лаврикова Елена	Шифрующий диск Хеберна (1922 г)
Лавриненко Николай	Шифр Альберти
Локтев Дмитрий	Шифр Кеплера
Матвеев Матвей	Шифр на основе шифровального диска
Николаенко Артём	Табличка Энея
Пак Юлия Артуровна	Шифромашин «Энигма»
Палагута Юлия	Таблица Виженера
Прокуряков Дмитрий	Метод гаммирования
Сивцов Андрей	Шифр Чейза
Сидорук Дарья	Магические квадраты
Синельников Никита	Шифрование методом публичного ключа
Ткачёв Дмитрий	Частотный анализ Аль-Кинди
Федоренко Никита	«Великое дело» чернильниц и симпатических чернил
Хорошилов Никита	Шифр Альберти
Шевелев Александр	Шифр Атбаш
Шмарова Анна	Шифр Галилея
Шпакова Вероника	«Скитала» — первый аппаратный шифр