Аннотация рабочей программы дисциплины/практики
Б1.О.21 Защита информации
Специальность/направление подготовки: 09.03.01 Информатика и вычислительная техника
Специализация/профиль: Проектирование АСОИУ на транспорте

1. Цели освоения дисциплины(модуля)/практики
Сформировать систему компетенций для усвоения теоретических, практических, современных представлений о основных принципах, методах и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах

2. Компетенции, формируемые в результате освоения дисциплины (модуля)\ практики	
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	
Индикатор	ОПК-3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Индикатор	ОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Индикатор	ОПК-3.3. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

3. В результате освоения дисциплины (модуля)/практики обучающийся должен

3.1	**Знать:**
3.1.1	правовые основы защиты компьютерной информации, модели и методы криптографической защиты и криптоанализа;
3.2	**Уметь:**
3.2.1	Применять криптографические методы на программном уровне: создание и отладка модулей шифрования/дешифрования, подготовка к передаче и обработка приема специально структурированных данных;
3.3	**Владеть:**
3.3.1	базовыми знаниями и приемами вычислений модулярной арифметики, теории чисел для расширенного решения задач криптографической защиты информации.

4. Структура и содержание дисциплины (модуля)/практики
Наименование разделов
Раздел 1. Введение в криптографическую защиту информации
Основные понятия криптографической защиты информации /Лек/
Система шифрования RSA /Лек/
Основы теории чисел. Теоремы Ферма, Эйлера и Гаусса в теории чисел /Лек/
Модулярная арифметика и классы вычетов /Лек/
Проблемы теории чисел /Лек/
Раздел 2. Фундаментальные алгоритмы
Особенности алгоритмов в теории чисел /Лек/
Алгоритм деления /Лек/
Теорема деления /Лек/
Алгоритм Эвклида /Лек/
Расширенный алгоритм Эвклида /Лек/
Программа алгоритма Эвклида /Лаб/
Раздел 3. Факторизация чисел
Теорема о разложении. Существование разложения /Лек/
Алгоритм Ферма разложения на множители /Лек/
Фундаментальное свойство простых чисел /Лек/
Единственность разложения /Лек/

Числа Кармайкла и тест Миллера /Лек/
Метод квадратичного решета /Ср/
Метод Поларда /Ср/
Тест Соловэа-Штрассена /Ср/
Факторизация чисел /Лаб/
Тесты на простоту /Лаб/
Раздел 4. Простые числа
Полиномиальная формула /Лек/
Экспоненциальные формулы: числа Мерсенна, числа Ферма /Лек/
Решето Эратосфена /Лек/
Генерация ключей. Шифрование RSA и подготовка данных к приему и передаче /Лаб/
Раздел 5. Арифметика остатков
Отношение эквивалентности /Лек/
Сравнения /Лек/
Арифметика остатков /Лек/
Критерий делимости /Лек/
Степени /Лек/
Диофантовы уравнения /Лек/
Деление по модулю /Лек/
Теорема Ферма /Лек/
Вычисление корней. Квадратные корни /Лек/
Дискретное логарифмирование /Ср/
Раздел 6. Системы сравнений
Линейные уравнения /Лек/
Китайский алгоритм остатков: взаимно простые модули /Лек/
Свойства степени. Алгоритм степени /Лек/
Раздел 7. Группы
Арифметические группы /Лек/
Подгруппы /Лек/
Циклические подгруппы /Лек/
Поиск подгрупп. Теорема Лагранжа /Лек/
Раздел 8. Контроль знаний
Подгоотовка к лабораторным /Ср/
Подготовка к лекциям /Ср/
Подготовка к зачету /Ср/
Интерактивная беседа /К/

Трудоёмкость: 3 ЗЕ.