## 1.12.16 Тема 1. Основные понятия, определения и проблемы в области информационной безопасности и защиты информации. Цели и задачи информационной безопасности.

## Место информационной безопасности в национальной безопасности РФ

Понятие информации. Фазы обращения информации в информационных системах. Место информационной безопасности в национальной безопасности РФ. Цели и задачи обеспечения информационной безопасности. Составляющие информационной безопасности. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности. Виды и источники угроз информационной безопасности РФ.

## Практическая работа

## РАЗРАБОТКА СЦЕНАРИЕВ ДЕЙСТВИЙ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ

## БЕЗОПАСНОСТИ

*Цель работы*: изучение возможностей моделирования на основе сетей Петри для построения сценариев действий нарушителя на объекте информатизации.

**Литература**

1. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. - Обеспечение информационной безопасности бизнеса. – М.: Изд.центр “Альпина Паблишерз”, 2011.
2. Башлы П.Н., Бабаш А.В., Баранова Е.К. Информационная безопасность: учебно-практическое пособие. – М.: Изд.центр ЕАОИ, 2010. – 216 с.
3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: РИОР\_ИНФРА-М, 2016. – 322 с.
4. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум. – М.: РИОР\_ИНФРА-М, 2015. – 196 с.
5. Руководящие документы ФСТЭК РФ: <http://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii>

## 15.12.16 Тема 2. Общие понятия криптографической защиты информации.

## Классические криптосистемы

Криптографическая система. Место криптографической защиты информации в обеспечении информационной безопасности. Краткие сведения из истории криптографии.

Классификация классических криптоалгоритмов, примеры реализации моноалфавиных, многоалфавитных подстановок и шифров перестановок. Требования к системам шифрования и примеры их реализации в классических криптографических алгоритмах.

## Практическая работа

## ИСПОЛЬЗОВАНИЕ КЛАССИЧЕСКИХ КРИПТОАЛГОРИТМОВ ПОДСТАНОВКИ И ПЕРЕСТАНОВКИ ДЛЯ ЗАЩИТЫ ТЕКСТОВОЙ ИНФОРМАЦИИ

*Цель работы:* Изучение классических криптографических алгоритмов моноалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты текстовой информации. Использование гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров.

Литература

1. Бабаш А.В., Баранова Е.К. Криптографические методы защиты информации. Учебник – М.: КНОРУС, 2016.- 192 с.
2. Бабаш А.В., Баранова Е.К. Криптографические методы защиты информации. Лабораторный практикум (+CD): учебное пособие. – М., КНОРУС, 2015.- 196 с.
3. Смарт Н. Криптография. – М.: Техносфера, 2006. – 528 с.