

# АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

## ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

(название дисциплины)

10.03.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

(код направления (специальности) подготовки)

7

(семестр)

### 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- Целями освоения дисциплины «Политики информационной безопасности в корпоративных информационных системах» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность»; формирование у студентов обобщенного представления по следующим вопросам: -назначение политик информационной безопасности на предприятии; -требования к политике информационной безопасности; -стандарты информационной безопасности; - содержание политик информационной безопасности. Базисы. Руководства. Процедуры; - аудит проведения информационной безопасности на предприятии; административные политики (Governing Policy) информационной безопасности на предприятии; технические политики (Technical Policy) информационной безопасности на предприятии; политики информационной безопасности на предприятии конечного пользователя (End User Policy)

### 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

- Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.12). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.
- Дисциплина изучается на четвертом курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Методология информационной безопасности», «Структуры данных» и «Основы информационной безопасности» «Информационные технологии», «Безопасность операционных систем» по направлению 10.03.01 «Информационная безопасность», квалификации - бакалавр. Кроме того, для грамотного использования полученных знаний в профессиональной деятельности, требуется изучение курсов «Математика»; «Информатика». Курс тесно взаимосвязан с другими дисциплинами. Он является полезным для изучения таких дисциплин как «Корпоративные информационные системы», «Программно-аппаратные средства защиты информации», «Техническая защита информации», «Система защиты информации на предприятии».

### 3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

- ПК-3 – способностью администрировать подсистемы информационной безопасности объекта защиты;
- ПК-4 – способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.

### 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

- Определение политики информационной безопасности. Назначение политик информационной безопасности предприятия
- Принципы политики ИБ. Требования к политике информационной безопасности.
- Стандарты информационной безопасности
- Этапы выработки политик информационной безопасности
- Содержание политик информационной безопасности. Базисы. Руководства. Процедуры
- Реализация политик информационной безопасности на предприятии. Аудит проведения

