

**Аннотация рабочей программы дисциплины
направление подготовки 09.03.03 «Прикладная информатика»
направленность «Прикладная информатика в экономике»**

Дисциплина: Б1.В.11 Информационная безопасность и защита информации

Цели освоения дисциплины:

Целью освоения дисциплины «Информационная безопасность и защита информации» является формирование знаний и умений, связанных с организацией информационной безопасности и защиты информации, планированием, подготовкой и реализацией процесса информационной безопасности, освоение различных технологий обеспечения информационной безопасности и защиты информации.

Формируемые компетенции:

ОК-4: способностью использовать основы правовых знаний в различных сферах деятельности;

ОПК-4: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ПК-11: способностью эксплуатировать и сопровождать информационные системы и сервисы.

Планируемые результаты обучения:

Знать: современную научную парадигму информационной безопасности; организационно-правовые основы защиты информационных ресурсов предприятия; теоретические и практические знания по правовым основам защиты информации при работе на вычислительной технике и в каналах связи; модели, стратегии, систем и технологических основ комплексного обеспечения информационной безопасности, вопросы правового и организационного обеспечения информационной безопасности; о концепции информационной безопасности; содержание основных понятий обеспечения информационной безопасности; источники угроз безопасности информации; методы оценки уязвимости информации; методы создания, организации и обеспечения функционирования систем комплексной защиты информации; методы пресечения разглашения конфиденциальной информации; виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений.

Уметь: решать вопросы в сфере обеспечения информационной безопасности; применить практические навыки и способности по осуществлению мероприятий по обеспечению информационной безопасности компьютерных сетей; использовать методы и средства защиты данных; выполнять анализ способов нарушений информационной безопасности; отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; применять действующую законодательную

базу в области информационной безопасности; разрабатывать проекты положений, инструкций и других организационно- распорядительных документов, регламентирующих работу по защите информации.

Владеть: криптографическими, программно-аппаратными и техническими методами и средствами защиты информации; методами криптографической защиты; основными технологиями построения защищенных ЭИС; основными понятиями безопасности информации; средствами обеспечения информационной безопасностью.

Содержание дисциплины:

Раздел 1. Обеспечение информационной безопасности: содержание и структура понятия.

Раздел 2. Стандарты и спецификации в области информационной безопасности.

Раздел 3. Комплексная система защиты информации.

Раздел 4. Процедурный уровень информационной безопасности.

Раздел 5. Административный уровень информационной безопасности.

Виды учебной работы: лекции, лабораторные работы.

Используемые образовательные технологии: Проведение лабораторных занятий построено на групповой совместной деятельности бакалавров, в том числе с использованием криптографических, программно-аппаратными и технических методов и средствами защиты информации. Во время занятий используются беседа, мозговой штурм, круглый стол.

Формы текущего контроля успеваемости: курсовые работы, аудиторные самостоятельные работы, устный опрос, тестирование.

Формы промежуточной аттестации: экзамен (6).

Трудоемкость дисциплины: 4 ЗЕ.

