

**Аннотация рабочей программы дисциплины «Информационная безопасность»  
для направления подготовки 09.03.02 Информационные системы и технологии  
Направленность (профиль) образовательной программы - Безопасность  
информационных систем**

**1. Цели и задачи освоения дисциплины**

**Цель дисциплины:** заложить терминологический фундамент, рассмотреть основные общеметодологические принципы теории информационной безопасности; изучить методы и средства обеспечения информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации и противодействия этим нарушениям.

**Задачами дисциплины** являются формирование знаний у студентов о современном состоянии проблемы обеспечения информационной безопасности при использовании компьютерных технологий, существующих угрозах, видах обеспечения информационной безопасности, методах и средствах защиты информации и основах построения комплексных систем защиты.

**2. Компетенции обучающегося, формируемые в результате освоения дисциплины**

Вместе с другими дисциплинами ОП дисциплина «Информационная безопасность» обеспечивает формирование следующих компетенций бакалавров:

способностью использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования (ОПК-2);

пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны (ОПК-4);

способностью проводить сбор, анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования (ПК-22);

способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ДПК-3).

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

**Знать:** принципы ИБ; основные угрозы информационной безопасности; сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны; методы и критерии оценки эффективности мероприятий по защите информации.

**Уметь:** различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия; использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования; проводить сбор, анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования; планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия; рассчитывать эффективность мероприятий по защите информации

**Владеть:** современной терминологией и методологией в области информационной безопасности.

**3. Содержание дисциплины**

Свойства информации как объекта защиты. Актуальность проблемы обеспечения безопасности информации. Угрозы информационной безопасности. Виды противников и

каналы утечки информации. Вредоносное ПО. Компьютерные вирусы и средства защиты от них. Управление рисками. Программно-технические методы защиты. Информационные войны и информационное оружие.