

**Аннотация рабочей программы дисциплины «Основы управления информационной безопасностью» для направления подготовки 10.03.01 Информационная безопасность.  
Направленность (профиль) образовательной программы - Безопасность автоматизированных систем (по отраслям или в сфере профессиональной деятельности)**

**1. Цели и задачи освоения дисциплины**

**Цель изучения дисциплины:**

Овладение основными принципами управления уровнем информационной безопасности защищаемых ресурсов организации, сформировать систему знаний о принципах, методах, подходах и инструментах эффективного управления информационной безопасностью в современной организации

**Задачи изучения дисциплины:**

Привитие обучаемым основ культуры обеспечения информационной безопасности; формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем; получение студентами знаний о структуре и принципах построения политики информационной безопасности организации.

**2. Компетенции обучающегося, формируемые в результате освоения дисциплины и индикаторы их достижения**

2.1. Универсальные компетенции и индикаторы их достижения

Категория (группа) универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
Командная работа и лидерство	УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	ИД-1УК-3-знает различные приемы и способы социализации личности и социального взаимодействия ИД-2УК-3-умеет строить отношения с окружающими людьми, с коллегами ИД-3УК-3- имеет практический опыт участия в командной работе, в социальных проектах, распределения ролей в условиях командного взаимодействия

2.2. Общепрофессиональные компетенции и индикаторы их достижения

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ИД-1ОПК-5 знает: основы законодательства Российской Федерации, систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации, правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую

	<p>характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации, правовые основы организации делопроизводства, виды и состав документации современной организации;</p> <p>ИД-2 ОПК-5 умеет: формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, определять виды документов, необходимых для оформления управленческих действий в профессиональной деятельности, грамотно составлять и оформлять служебные документы.</p> <p>ИД-3 ОПК-5 владеет: действиями (навыками) по применению нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации в сфере профессиональной деятельности</p>
<p>ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;</p>	<p>ИД-1ОПК-10- знать: цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью, принципы формирования политики информационной безопасности объекта информатизации, принципы организации информационных систем в соответствии с требованиями по защите информации, особенности комплексного подхода к обеспечению информационной безопасности организации</p> <p>ИД-2ОПК-10- уметь: разрабатывать модели угроз и модели нарушителя объекта информатизации, оценивать информационные риски объекта информатизации, определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации</p> <p>ИД-3ОПК-10- иметь навыки: участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;</p>

### 3. Содержание дисциплины

Анализ объекта защиты. Модель угроз и модель нарушителя. Основы управления рисками ИБ. Система управления информационной безопасностью. Политика информационной безопасности.