


Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

**АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Безопасность открытых информационных систем»**

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина имеет целью:

обучить студентов принципам обеспечения информационной безопасности, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем;

содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Названная дисциплина является базовой для изучения других дисциплин специальности "Информационная безопасность автоматизированных систем", а также будет использована при выполнении курсовых и дипломных работ.

Задачи освоения дисциплины:

дать основы:

методологии создания систем защиты информации;

методов, средств и приемов ведения информационных войн;

обеспечения информационной безопасности компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Основы информационной безопасности» относится к числу дисциплин базового блока и занимает важное место в рамках образовательной программы подготовки по специальности – 10.05.03 "Информационная безопасность автоматизированных систем".

Дисциплина читается в 5-ом семестре студентам 3-го курса очной формы обучения и базируется на знаниях и умениях, приобретённых в результате освоения дисциплин: «Информатика»; «Гуманитарные аспекты информационной безопасности», «Теория информации», «Организационное и правовое обеспечение информационной безопасности».


Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Компьютерные сети»; «Модели безопасности компьютерных систем»; «Защита в операционных системах»; «Основы построения защищённых компьютерных сетей»; «Защита программ и данных»; «Техническая защита информации»; «Криптографические методы защиты информации»; «Криптографические протоколы».

**3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ДИСЦИПЛИНЕ
(МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ
ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

- способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

- способность применять нормативные правовые акты в профессиональной деятельности (ОПК-6);

- способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

- способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-26).

В результате изучения дисциплины студент должен:

• **знать:**

сущность и понятие информации, информационной безопасности и характеристику ее составляющих;

место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;

основные нормативные правовые акты в области информационной безопасности; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;

источники и классификацию угроз информационной безопасности;

• **уметь:**

классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;

применять методы научных исследований в профессиональной деятельности;

• **владеть:**

профессиональной терминологией в области информационной безопасности;

основными методами научных исследований в профессиональной деятельности;

навыками применения типовых технических средств защиты информации;

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зачетных единицы (108 часов).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии: лекционные занятия, интерактивный опрос в ходе лекций, эвристическая беседа, диалог, ознакомительные беседы с представителями потенциальных работодателей.

При организации самостоятельной работы занятий используются образовательные технологии развивающего, проблемного и проектного обучения.

6. КОНТРОЛЬ УСПЕВАЕМОСТИ

Программой дисциплины предусмотрены следующие виды текущего контроля: письменные и устные опросы на лекциях, написание рефератов.

Промежуточная аттестация проводится в форме зачёта.