

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

**АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
по специальности 10.05.01 «Компьютерная безопасность», специализация
«Математические методы защиты информации»**

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 «Компьютерная безопасность», 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» изучается в 5 семестре и относится к числу базовой части дисциплин блока Б1, предназначенного для студентов, обучающихся по специальности 10.05.01 – «Компьютерная безопасность».

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов: «Информатика»; «Гуманитарные аспекты информационной безопасности», «Теория информации», «Организационное и правовое обеспечение информационной безопасности».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

знание базовых понятий в области информатики и теории информации;

способность использовать нормативные правовые документы;

способность анализировать социально-значимые проблемы и процессы;


способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Компьютерные сети»; «Модели безопасности компьютерных систем»; «Защита в операционных системах»; «Основы построения защищенных 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 понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

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

- способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения (ОПК-7);

- способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-13);

- способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-15);

- разрабатывать проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем (ПК-16).

В результате изучения дисциплины студент должен:

• **знать:**

роль и место информационной безопасности в системе национальной безопасности страны;

содержание информационной войны, методы и средства её ведения;

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

методы и технологии управления в сфере профессиональной деятельности;

основные средства и методы обеспечения информационной безопасности;

основные средства и методы обеспечения информационной безопасности;

• **уметь:**

пользоваться современной научно-технической информацией по исследуемым проблемам и задачам

анализировать и оценивать угрозы информационной безопасности объекта;

принимать управленческие решения и оценивать их эффективность;

анализировать и оценивать угрозы информационной безопасности компьютерных систем;

применять действующую законодательную базу в области обеспечения ИБ при разработке проектов нормативных, правовых и методических материалов, регламентирующих работу по обеспечению ИБ предприятия;

• **владеть:**

профессиональной терминологией в области информационной безопасности;

навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем;

навыками применения типовых технических средств защиты информации;

навыками выбора, обоснования, реализации и контроля результатов управленческого решения.


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.

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

6. КОНТРОЛЬ УСПЕВАЕМОСТИ

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

Промежуточная аттестация проводится в форме зачёта.