

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

## АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Компьютерная безопасность

**по направлению/специальности 11.03.02 Инфокоммуникационные технологии и системы.**

### 1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

Дисциплина «Компьютерная безопасность» имеет целью обучить студентов:

- принципам инженерно-технической защиты информации;
- основам построения технических средств защиты информационных сетей.

Задачи освоения дисциплины:

- дать основы:
- инженерно-технической защиты информации;
- организации работ по технической защите информации

### 2. Место дисциплины в структуре ООП ВО (ВПО)

Дисциплина «Компьютерная безопасность» относится к числу дисциплин блока М2.В.4 профессионального цикла, предназначенного для магистров, обучающихся по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи.

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов «Нормативно-правовое обеспечение информационной безопасности»; «Теория построения инфокоммуникационных сетей и систем».

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Перспективные сетевые технологии»; «Теория электромагнитной совместимости радиоэлектронных средств и систем».

### 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способность совершенствовать и развивать свой интеллектуальный и общекультурный уровень (ОК-1);
- способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности (ОК-2);
- способность свободно пользоваться русским и мировым иностранным языками как средством делового общения (ОК-3);
- готовность осваивать современные перспективные направления развития телекоммуникационных систем и сетей; способность реализовывать новые принципы построения телекоммуникационных систем различных типов, передачи и распределения информации в сетях связи (ПК-1);
- способность к разработке моделей различных технологических процессов и

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

проверке их адекватности на практике; готовность использовать пакеты прикладных программ анализа и синтеза телекоммуникационных систем и сетей (ПК-2);

- готовность разрабатывать системы, средства и методы защиты информации в телекоммуникационных устройствах и сетях (ПК-6);

- готовность использовать современные достижения науки и передовые инфокоммуникационные технологии, методы проведения теоретических и экспериментальных исследований в научно-исследовательских работах в области техники и технологий электросвязи (ПК-8);

- способность самостоятельно выполнять экспериментальные исследования для решения научно-исследовательских и производственных задач с использованием современной аппаратуры и методов исследования; способность участвовать в научных исследованиях в группе, ставить задачи исследования, выбирать методы экспериментальной работы (ПК-9).

В результате изучения дисциплины студент должен:

• **иметь представление:**

- о целях, задачах и принципах инженерно-технической защиты информации;
- о принципах организации работ по технической защите информации;
- об основных технических средствах разведки;

• **знать:**

- основы организации работ по инженерно-технической защите информации;
- основные демаскирующие признаки объектов защиты и носителей информации;
- типовые технические каналы утечки информации;
- основные способы и типовые средства защиты информации;
- основные средства обнаружения и противодействия утечкам информации;

• **уметь:**

- выявлять и оценивать угрозы безопасности информации на объектах информатизации;
- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;
- применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований;
- использовать типовые средства обнаружения и противодействия утечкам информации и защиты информации от несанкционированного доступа (НСД);

• **приобрести навыки:**

- применения полученных знаний на практике;
- формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем;
- применения типовых технических средств обнаружения и противодействия утечкам информации и защиты информации от несанкционированного доступа (НСД);

• **владеть, иметь опыт:**

- профессиональной терминологией в области информационной безопасности;
- работы с типовыми техническими средствами защиты информации от НСД.

#### 4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет   2   зачетных единиц (  72   часа)

#### 5. Образовательные технологии

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

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии: интерактивные (информационные технологии, работа в команде, контекстное обучение).

При организации самостоятельной работы занятий используются следующие образовательные технологии: интерактивные (опережающая самостоятельная работа, междисциплинарное изучение, проблемное изучение).

## **6. Контроль успеваемости**

Программой дисциплины предусмотрены следующие виды текущего контроля: лабораторные работы, рефераты.

По данной дисциплине предусмотрена форма отчетности: лабораторным работам, доклады.

Промежуточная аттестация проводится в форме зачета.