

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

## АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Защита информации и информационная безопасность

**по направлению/специальности 110302 - "Инфокоммуникационные технологии и системы связи". Профиль "Инфокоммуникационные технологии в сервисах и услугах связи».**

### 1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

- заложить методически правильные основы знаний, необходимые будущим специалистам-практикам в области информационной безопасности (ИБ).

Задачи освоения дисциплины:

Иметь представление - описания общей структуры и отдельных уровней ИБ  
Уяснить: политику и программу безопасности, их типовые структуры, меры по их выработке и сопровождению; на процедурном уровне меры безопасности, имеющие дело с людьми; основные принципы, помогающие успеху таких мер.

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

Дисциплина «Защита информации и информационная безопасность» относится к числу дисциплин блока БЗ.В.7 профессионального цикла, предназначенного для студентов, обучающихся по направлению подготовки 110302 - "Инфокоммуникационные технологии и системы связи".

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов: «Информатика»; «Базы данных и хранение информации»; «Вычислительная техника и информационные технологии»; «Основы построения инфокоммуникационных систем и сетей»; «Основы сетевых технологий в инфокоммуникационных системах и сервисах».

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Корпоративные инфокоммуникационные системы и услуги»; «Системы и услуги документальной электросвязи»; «Технология программной защиты в интернете».

### 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения (ОК-1);
- уметь логически верно, аргументировано и ясно строить устную и письменную речь (ОК-2);
- осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности (ОК-7);
- использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования (ОК-9);
- способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом про-

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

пессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны; владеть основными методами, способами и средствами получения, хранения, переработки информации (ПК-1);

- иметь навыки самостоятельной работы на компьютере и в компьютерных сетях; осуществлять компьютерное моделирование устройств, систем и процессов с использованием универсальных пакетов прикладных компьютерных программ (ПК-2);

- готовность к созданию условий для развития российской инфраструктуры связи, обеспечения ее интеграции с международными сетями связи; готовностью содействовать внедрению перспективных технологий и стандартов (ПК-6);

- уметь организовать доведение услуг до пользователей услугами связи; быть способным провести работы по управлению потоками трафика на сети (ПК-11).

В результате изучения дисциплины студент должен:

- **иметь представление:**

о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства;

о методологии создания систем защиты информации;

о перспективных направлениях развития средств защиты информации;

- **знать:**

механизмы реализации информационной безопасности;

современные подходы к построению систем защиты информации;

инструментарий информационной безопасности;

направления информационной безопасности;

- **уметь:**

работать с типовыми средствами защиты информации;

анализировать признаки сетевых атак и принимать меры для их нейтрализации.

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.

#### 4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часов)

#### 5. Образовательные технологии

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 экзамен.