

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

**АННОТАЦИЯ  
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ  
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»  
по направлению бакалавриата 09.03.03 «Прикладная информатика»,  
профиль «Информационная среда» (Квалификация (степень) - «бакалавр»)**

**ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

**Цели освоения дисциплины:**

Цель курса - заложить методически правильные основы знаний в области информационной безопасности, необходимые будущим специалистам в области прикладной информатики.

Информационная безопасность (ИБ)- сравнительно молодая, быстро развивающаяся область информационных технологий (ИТ), для успешного освоения которой важно с самого начала усвоить современный, согласованный с другими ветвями ИТ, базис. Это - первая задача курса, для решения которой привлекается объектно-ориентированный подход.

Успех в области ИБ может принести только комплексный подход. Описание общей структуры и отдельных уровней такого подхода - вторая задача курса. Для ее решения рассматриваются меры законодательного, административного, процедурного и технического уровней.

Предполагается, что большинство понятий, введенных в данном курсе, станет предметом более детального рассмотрения в других, специальных курсах.

**Задачи освоения дисциплины:**

дать основы: методологии создания систем защиты информации и обеспечения информационной безопасности информационных систем.

**МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО**

Дисциплина «Информационная безопасность» (Б1.Б) изучается в 7 семестре и относится к числу базовых дисциплин блока 1 «Дисциплины (модули)», предназначенного для студентов, обучающихся по направлению подготовки бакалавриата **09.03.03** «Прикладная информатика».

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов: «Информатика и программирование»; «Информационные системы и технологии»; «Проектирование информационных систем»; «Администрирование информационных систем»; «Информационные сети»; «Разработка и стандартизация программных средств и информационных систем»; «Защита в операционных системах»; «Защита в компьютерных сетях».

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


знание базовых понятий в области физики, вычислительной техники, электроники и схемотехники;

способность использовать нормативные правовые документы;

способность анализировать 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: «Информационные ресурсы общества»; «Информатизация общества»; «Экспертные системы»; «Интернет-программирование»; «Интеллектуальные информационные системы»; «Разработка мобильных приложений»; «Открытые технологии разработки программного обеспечения».

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

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:


Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
1	2
ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<p><b>Знать:</b> Основные требования информационной безопасности в ходе решения стандартных задач профессиональной деятельности</p> <p><b>Уметь:</b> Решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности</p> <p><b>Владеть:</b> Методологией настройки информационных систем в процессе защиты информации</p>
ПК-7 - способность настраивать, эксплуатировать и сопровождать информационные системы и сервисы	<p><b>Знать:</b> Основные современные информационные системы и сервисы в области защиты информации</p> <p><b>Уметь:</b> Настраивать, эксплуатировать и сопровождать типовые средства защиты информации от несанкционированного доступа</p> <p><b>Владеть:</b> Навыками администрирования основных подсистем информационной безопасности объекта защиты</p>
ПК-8 - способность проводить тестирование компонентов программного обеспечения ИС	<p><b>Знать:</b> Основные требования информационной безопасности в ходе тестирования программного обеспечения ИС</p> <p><b>Уметь:</b> Проводить тестирование компонентов программного обеспечения ИС с учетом основных требований информационной безопасности</p> <p><b>Владеть:</b> Методологией тестирования компонентов программного обеспечения ИС в процессе защиты информации</p>

### 4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зачетные 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.

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

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, рефераты на заданные темы и отчёты на лабораторных работах.

Промежуточная аттестация проводится в форме зачёта.