


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

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ «Защита в операционных системах»

по направлению подготовки 09.03.03 Прикладная информатика (бакалавриат), профиль
информационная сфера

1. Цели и задачи освоения дисциплины

Дисциплина «Защита в операционных системах» рассматривает частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; навыками конфигурирования подсистем безопасности ОС Windows и Unix;

Целью преподавания дисциплины является: знакомство с основными методами и средствами обеспечения защиты информации при проектировании и использовании операционных систем.

Задачи курса: сформулировать политику безопасности ОС и уметь применять на практике защитные механизмы и средства обеспечения безопасности ОС.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Защита в операционных системах» относится к вариативной части Основной Профессиональной Образовательной Программы по направлению подготовки бакалавров 09.03.03 «Прикладная информатика».

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины в соответствии с ФГОС ВО по направлению подготовки 09.03.03 «Прикладная информатика» направлен на формирование следующих компетенций (элементов компетенций):

профессиональных (ПК):


ПК-7 – способность настраивать, эксплуатировать и сопровождать информационные системы и сервисы,

ПК-8 – способность проводить тестирование компонентов программного обеспечения ИС.

В результате освоения дисциплины студент должен:

Знать:

- ✓ защитные механизмы и средства обеспечения безопасности операционных систем;
- ✓ основные протоколы идентификации и аутентификации в ОС;
- ✓ основные виды политик управления доступом в ОС.

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

Уметь:

- ✓ формулировать и настраивать политику безопасности ОС Windows и Unix;
- ✓ разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками;

Владеть:

- ✓ навыками конфигурирования подсистем безопасности ОС Windows и Unix;
- ✓ методиками анализа журналов ОС.

4. Общая трудоемкость дисциплины

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

5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий применяются следующие образовательные технологии: лекции для изложения теоретического материала и практические лабораторные занятия, прохождение тестовых заданий по теоретической и практической части курса.

Самостоятельная работа студентов осуществляется в виде изучения теоретического материала, основной и дополнительной литературы, рекомендованной по дисциплине, выполнения самостоятельных работ по практической части дисциплины.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: текущий контроль успеваемости в форме тестирования и контрольных работ.

По данной дисциплине предусмотрена форма отчетности: 7 семестр – зачет.