

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

**АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«ОТКРЫТЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ»
по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Безопасность открытых информационных систем»**

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина имеет целью:

обучить студентов принципам построения открытых информационных систем с использованием различных технологических подходов;

ознакомить студентов с компонентами для доступа к объектам серверных систем и методам оптимизации информационных систем в архитектуре «клиент/сервер».

расширить кругозор, воспитать комплексное отношение к обеспечению информационной безопасности в открытых информационных системах в сочетании с получением необходимых практических навыков.

Для реализации названных целей необходимо решить следующие задачи:

дать основные понятия, свойства и элементы открытых информационных систем;

ознакомить студентов с основными моделями открытых информационных систем и технологиями их построения;

освоить программные интерфейсы взаимодействия с открытыми информационными системами и научиться разрабатывать мобильные приложения.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Открытые информационные системы» относится к числу дисциплин базового блока и занимает важное место в рамках образовательной программы подготовки по специальности - 10.05.03 "Информационная безопасность автоматизированных систем".

Дисциплина читается в 5-ом семестре студентам 3-го курса очной формы обучения и базируется на знаниях и умениях, приобретённых в результате освоения дисциплин: «Информатика»; «Языки программирования»; «Технологии и методы программирования»; «Безопасность операционных систем».

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Организация ЭВМ и вычислительных систем»; «Модели безопасности компьютерных систем»; «Сети и системы передачи информации»; «Безопасность открытых информационных систем»; «Безопасность сетей ЭВМ»; «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 анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач(ОПК-1);

- способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере

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

профессиональной деятельности, в том числе на иностранном языке (ПК-1);

- способность проводить анализ защищенности автоматизированных систем (ПК-3);
- способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);
- способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-4.1);
- способность разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.2);
- способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3).

В результате изучения дисциплины студент должен:

- **знать:**
причины и условия возникновения открытых информационных систем;
понятийный аппарат открытых информационных систем и элементов эталонной модели открытых систем;
основные функции и услуги уровней эталонной модели открытых систем;
- **уметь:**
разрабатывать политики информационной безопасности информационных систем, используя эталонную модель открытых систем;
реализовывать политики информационной безопасности в процессе использования открытых информационных систем;
разрабатывать приложения для мобильных платформ;
- **владеть:**
навыками разработки и реализации политик информационной безопасности открытых информационных систем.

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4зачетных единицы (144часа).

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.

6. КОНТРОЛЬ УСПЕВАЕМОСТИ

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

Промежуточная аттестация проводится в форме экзамена.