


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

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ «АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ»

по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Безопасность открытых информационных систем»

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Учебная дисциплина «Аттестация объектов информатизации» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом и имеет целью:

обучить студентов обеспечению безопасности автоматизированных систем на соответствие требованиям отечественным и зарубежным стандартам в области информационной безопасности;

Задачи освоения дисциплины:

сформировать практические навыки аттестации объектов информатизации и выделенных помещений;

дать методологию организации работ по выполнению режима защиты информации, в том числе, ограниченного доступа.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО


Дисциплина «Аттестация объектов информатизации» относится к числу прикладных дисциплин и занимает важное место в блоке дисциплин Б1.В, предназначенных для подготовки студентов по специальности – 10.05.03 "Информационная безопасность автоматизированных систем".

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов: «Информатика»; «Теория информации», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

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


знание базовых понятий в области информатики и теории информации;
 способность использовать нормативные правовые документы;
 способность анализировать социально-значимые проблемы и процессы;
 способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования.

Основные положения дисциплины будут использоваться в дальнейшем при проведении производственных и преддипломных практик, стажировок и в последующей профессиональной деятельности по обеспечению защиты информации.

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

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

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
1	2
ПК-1 - Способен организовать работы по выполнению в информационной системе требований защиты информации ограниченного доступа	<p>Знать: Источники и классификацию угроз информационной безопасности Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Нормативные правовые акты в области защиты информации</p> <p>Уметь: Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации Организовывать реализацию мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты Организовывать процесс применения защищенных протоколов, межсетевых экранов, средств обнаружения вторжений для защиты информации в сетях</p> <p>Владеть: Навыками организации применения защищенных протоколов, межсетевых экранов и средств обнаружения вторжений для защиты информации в сетях Навыками управления процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем</p>
ПК-6 - Способен проводить контроль защищенности информации от НСД	<p>Знать: Методы защиты информации от несанкционированного доступа и специальных программных воздействий на нее Методы и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий</p> <p>Уметь: Проводить оценку защищенности информации от несанкционированного доступа и специальных воздействий Проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воздействий, выполнение правил их эксплуатации</p> <p>Владеть: Навыками проведения контроля защищенности информации от несанкционированного доступа и специальных воздействий</p>

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

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зачетных 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.

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.

Промежуточная аттестация проводится в форме зачёта.