


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

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ «Аттестация объектов информатизации»

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

1. Цели и задачи освоения дисциплины

Целью дисциплины «Аттестация объектов информатизации» является формирование у студентов систематизированных знаний об организации мероприятий по информационной безопасности на объекте информатизации и об их правовом обеспечении. Дисциплина раскрывает основные понятия и виды защищаемой информации в соответствии с законодательством РФ, дает знания о системе защиты государственной тайны, конфиденциальной информации.

Задачами изучения дисциплины является формирование у студентов знаний в области:

- информационного законодательства РФ и международного законодательства в области защиты информации;
- организации государственного лицензирования в области защиты информации;
- организации системы сертификации и аттестации объектов информатизации

2. Место дисциплины в структуре ОПОП

Дисциплина «Аттестация объектов информатизации» относится к обязательным дисциплинам вариативной части Б1.В.ОД.7 Дисциплина «Аттестация объектов информатизации» дает студентам систематизированные знания по вопросам организации системы государственного лицензирования в области защиты информации, сертификации и аттестации объектов защиты информации и читается в 8 семестре 4 курса.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6)


способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

способностью проводить анализ защищенности автоматизированных систем (ПК-3);

способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);

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

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации (ПК-16);

способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22); способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-22);

способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

В результате освоения данной дисциплины студенты должны

иметь представление:

- об основах организации защиты информации на объектах информатизации;
- о назначении, задачах и структуре, средствах и способах работы подразделений службы безопасности;
- о правовом режиме участия в международном обмене.

знать:

- основные угрозы информационной безопасности объекта информатизации и их классификацию;
- классификацию мероприятий по защите информации;
- правила лицензирования и сертификации в области защиты информации;
- порядок проведения аттестации объектов информационной защиты;
- типовые методики испытаний объектов информатизации по требованиям защиты информации;
- типовые формы документов по подготовке и проведению сертификации и аттестации объектов защиты информации;
- специальные защитные знаки и их классификацию.

уметь:


- определять угрозы объекту информатизации;
- определять рациональные способы и средства защиты информации на объекте информатизации;
- организовывать мероприятия по защите информации на объекте информатизации.

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: лабораторных занятия, интерактивный опрос, эвристическая беседа, диалог, ознакомительные беседы с представителями потенциальных работодателей.

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

При организации самостоятельной работы занятий используются следующие образовательные технологии: развивающего, проблемного и проектного обучения.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: письменные и устные опросы на семинарских занятиях, опрос во время лекций, написание рефератов.

Промежуточная аттестация проводится в форме зачёта.