Аннотация к рабочей программе дисциплины
«Информационная безопасность автоматизированных систем»

Рабочая программа по курсу «Информационная безопасность автоматизированных систем» разработана для студентов по направлению 10.03.01 «Информационная безопасность».

Учебным планом предусмотрены лекционные занятия (36 часов), практические занятия (18 часов), лабораторные работы (72 часа) самостоятельная работа студентов (54 часа). Дисциплина «Информационная безопасность автоматизированных систем» реализуется на 3 курсе в 6 семестре.

Цель дисциплины - раскрыть содержание основных понятий, методов и механизмов обеспечения информационной безопасности автоматизированных систем.

Задачи дисциплины – дать основы:

- системного и комплексного подхода к анализу и обеспечению

информационной безопасности АС в процессах их создания и эксплуатации (администрирования);

- представления, анализа и обоснования моделей, методов и механизмов

обеспечения информационной безопасности АС;

- практических навыков работы с нормативно-методическими документами(стандартами) в сфере информационной безопасности автоматизированных информационных систем.

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные/ общепрофессиональные/ профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-2) способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знает	Программные средства системного, прикладного и специального назначения для защиты информации, а так же современные инструментальные средства, языки и системы программирования
	Умеет	Применять для различных целей программные средства системного, прикладного и специального назначения
	Владеет	Современными и широко используемыми языками и системами программирования для решения профессиональных задач
(ПК-8) способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Знает	Принципы и методы проектирования подсистем и средств обеспечения информационной безопасности
	Умеет	Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности систем
	Владеет	Методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов и технико-экономической экспертизы
(ПК-9) способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знает	Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области
	Умеет	Пользоваться нормативными и техническими документами по защите информации
	Владеет	Навыками работы с нормативными правовыми актами, способностью оформлять рабочую техническую документацию
(ПК-16) способность принимать участие в формировании,	Знает	Ролевую политику и технологии индивидуально-группового доступа к разделяемым информационным ресурсам;

организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Умеет	Вырабатывать перечень процедур и работ по администрированию защищенных АС.
	Владеет	Навыками работы с нормативно-методическими документами в сфере информационной безопасности автоматизированных информационных систем.

Для формирования вышеуказанных компетенций в рамках дисциплины «Информационная безопасность автоматизированных систем» применяются следующие методы активного/ интерактивного обучения: лекция – беседа, лекция – пресс-конференция.