АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«СЕРТИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ»
по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Безопасность открытых информационных систем»

ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Учебная дисциплина «Сертификация средств защиты информации» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Основной целью освоения дисциплины «Сертификация средств защиты информации» является формирование у студентов знаний по основам организации сертификации средств защиты информации по требованиям безопасности информации, а также навыков и умений в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач сертификации по требованиям безопасности информации с учетом требований системного подхода.

Задачи освоения дисциплины:

Основные задачи дисциплины – дать знания:

- по основам сертификации по требованиям безопасности информации;
- по основам проведения сертификационных испытаний;
- по программным средствам сертификационных испытаний и анализа безопасности программного кода;
- по методическому обеспечению сертификации по требованиям безопасности информации.

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Сертификация средств защиты информации» изучается в 8 семестре и относится к вариативной части дисциплин блока Б1 специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Курс учебной дисциплины тесно связан с другими учебными дисциплинами, в первую очередь с курсами «Криптографические методы защиты информации», «Безопасность операционных систем», «Безопасность вычислительных сетей», позволяющими понять физическую сущность процесса сертификации по требованиям безопасности информации.

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

знание базовых понятий в области вычислительной техники, электроники и схемотехники;

способность использовать нормативные правовые документы;

способность анализировать проблемы и процессы;

способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Разработка и эксплуатация автоматизированных систем в защищенном исполнении», «Аттестация объектов информатизации», при прохождении технологической, преддипломной практик, выполнении научно-исследовательской работы.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

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	**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 **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 **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
ПК-2 - Способен осуществлять тестирова-ние систем защиты информации автоматизированных систем	**Знает:** Принципы построения и функционирования систем и сетей передачи информации Эталонную модель взаимодействия открытых систем Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах **Умеет:** Применять действующую нормативную базу в области обеспечения безопасности информации Контролировать безотказное функционирование технических средств защиты информации **Владеет:** Навыками подбора инструментальных средств тестирования систем защиты информации автоматизированных систем
ПК-3 - Способен раз-	**Знать:**

рабатывать проектные решения по защите информации в автоматизированных системах	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем Принципы формирования политики информационной безопасности в автоматизированных системах **Уметь:** Применять действующую нормативную базу в области обеспечения защиты информации Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе **Владеть:** Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 2 зачетных единицы (72 часа).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии: лекционные занятия, интерактивный опрос в ходе лекций, отчёты лабораторных работ, 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, лабораторных занятиях, написание рефератов.

Промежуточная аттестация проводится в форме зачёта.