Аннотация рабочей программы дисциплины
«Защищенные информационные системы и управление информационной безопасностью»

Направление подготовки – 09.04.04 «Программная инженерия»
Направленность (профиль) - «Программные средства обеспечения кибербезопасности»
Уровень образования – магистр.
Форма обучения – очная.

1. Цели и задачи дисциплины

Цель модуля - освоение навыков осуществления информационной безопасности в защищенных информационных системах.

Задачи дисциплины на основе знания способов организации и управления информационной безопасностью в защищенных информационных системах сформировать – способность осуществлять информационной безопасностью в защищенных информационных системах.

2. Место дисциплины в структуре ОП

Модуль относится к части программы, формируемой участниками образовательных отношений, и направлен на формирование компетенции ПК-1 «Способен осуществлять организацию и управление информационными процессами», в части ПК-1.ЗИСиУИБ «Способен применять знания способов организации и управления информационными процессами в защищенных информационных системах и методов обеспечения информационной безопасности для решения профессиональных задач» и ПК-2 «Способен участвовать в программной реализации информационных систем и создании программного обеспечения для анализа, распознавания и обработки информации в сфере кибербезопасности» в части ПК-2.ЗИСиУИБ «Способен использовать методы управления информационной безопасностью в защищенных информационных системах для решения профессиональных задач».

Для освоения модуля необходима сформированность компетенций, определяющих готовность использовать современные технологии объектно-ориентированного программирования, применять их в практической деятельности, применять основные концепции, принципы обеспечения кибербезопасности.

В результате освоения модуля студент должен приобрести:

Знания: способов организации и управления информационной безопасностью в защищенных информационных системах; методов управления информационной безопасностью и в защищенных информационных системах;

Умения: осуществлять информационной безопасностью в защищенных информационных системах; обоснованно выбирать методы управления информационной безопасности;

Опыт: управления информационной безопасностью в защищенных информационных системах и управления информационной безопасностью; оценивать риски информационной безопасности.

3. Краткое содержание дисциплины

Модуль включает следующие разделы: «Введение в информационную безопасность», «Методы и системы защиты информации», «Ограничения доступа Методы идентификации», «Методы и модели управления рисками информационной безопасности».

Разработчик:
доцент СПИНТех, к.т.н. В.Г. Дорогов