Аннотация рабочей программы дисциплины
«Защита информации в операционных системах»
для направления подготовки 09.03.02 Информационные системы и технологии
Направленность (профиль) образовательной программы - Безопасность информационных систем

1. Цели и задачи освоения дисциплины

Цель дисциплины:

- расширение, углубление и развитие знаний и навыков из области информационной безопасности и защиты информации, приобретение знаний и навыков в области задач, механизмов, способов и средств защиты информации в контексте операционных систем.

Задачи дисциплины:

- развитие системы знаний и навыков общей теории информационной безопасности и защиты информации;
- формирование комплексных знаний об угрозах информационной безопасности в контексте операционных систем;
- формирование комплексных знаний о механизмах защиты информации, применяемых в операционных системах;
- формирование комплексных знаний и практических навыков решения задач защиты информации в операционных системах.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Изучение дисциплины обеспечивает овладение следующими компетенциями:

– понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны (ОПК-4);

– способность выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно-) для решения поставленной задачи (ОПК-6);

– способностью оценивать надежность и качество функционирования объекта проектирования (ПК-6);

– способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ДПК-1).

В результате освоения обучающийся должен демонстрировать следующие результаты образования:

1) Знать: основные виды и источники угроз информационной безопасности; основные виды ресурсов компьютера; основные подходы и методы защиты информации, применяемые в операционных системах; основные механизмы, реализующие данные подходы, и алгоритмы их работы; область применения, сильные и слабые стороны основных методов защиты информации; основные программные и программно-аппаратные средства, реализующие данные методы и механизмы.

2) Уметь: определять групп класса безопасности автоматизированных систем и средств вычислительной техники; выделять компьютерные ресурсы, требующие защиты; выбирать совокупность методов и механизмов, обеспечивающую требуемый уровень защиты; выбирать, устанавливать, настраивать и обслуживать программные и программно-аппаратные средства, реализующие необходимые компоненты системы защиты информации.

3) Владеть: основными методами, способами и средствами оценки, обеспечения и повышения уровня защищённости информации и компьютерных ресурсов.

3. Содержание дисциплины

Введение.

Управление доступом.
Идентификация и аутентификация.
Журнализация и аудит.
Замкнутая программная среда и контроль потоков информации.
Контроль целостности.
Резервное копирование.
Типовая модель угроз безопасности в ОС.
Вредоносное программное обеспечение и способы борьбы с ним.
Классы защищённости СВТ.
Классы защищённости АС.