Аннотация к рабочей программе дисциплины «Безопасность операционных систем»

по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация «Информационная безопасность АС на транспорте»).

Общая трудоемкость дисциплины составляет 9 зачетных единиц (324 часов).

Предполагаемые семестры: 5,6

Форма контроля: зачет, экзамен

Цель:

освоение дисциплины «Безопасность операционных систем» - теоретическая и практическая подготовка специалистов в области эксплуатации современных операционных систем (ОС) для обеспечения их эффективного применения с учетом требований информационной безопасности и привитие навыков в использовании методов обеспечения защиты информации в ОС.

Задачи дисциплины:

- изучение назначения и функций ОС;
- приобретение навыков управления ресурсами и задачами в ОС;
- освоение администрирования ОС;
- изучение требований к защите ОС;
- изучение методов и средств разграничения доступа в ОС;
- изучение аудита в ОС;
- формирование специальных теоретических и практических знаний, обеспечивающих возможность планирования политики безопасности ОС;
- приобретение навыков эффективной и безопасной эксплуатации ОС автоматизированных систем;
- приобретение навыков эффективного применения информационно-технологических ресурсов ОС;
- формирование специальных теоретических и практических знаний, позволяющих администрировать подсистему информационной безопасности автоматизированной системы;
- формирование теоретических и практических знаний, позволяющих обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

Учебная дисциплина «Безопасность операционных систем» относится к числу дисциплин базовой части профессионального цикла. Изучение этой дисциплины базируется на знании следующих дисциплин:

- «Информатика» - знать формы и способы представления данных в персональном компьютере, классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; уметь применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев и т.п.), владеть навыками поиска и обмена информацией в глобальной информационной сети Интернет.
- «Языки программирования» - знать общие принципы построения и использования современных языков программирования высокого уровня (объектно-ориентированное программирование); уметь работать с интегрированной средой разработки программного обеспечения, использовать динамически подключаемые библиотеки; владеть навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования.
- «Основы информационной безопасности» - знать основные средства и способы обеспечения информационной безопасности, принципы построения защиты информации; уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; владеть профессиональной терминологией в области информационной безопасности.

Дисциплина «Безопасность операционных систем» является предшествующей для изучения следующих базовых дисциплин: «Безопасность систем баз данных», «Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности».

Краткое содержание дисциплины:
Основы функционирования ОС, безопасность ОС.

В результате изучения дисциплины, специалист должен обладать следующими профессиональными компетенциями (ПК):
ПК-4: способность проводить анализ защищенности автоматизированных систем;
ПК-9: способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем (АС);
ПК-10: способность участвовать в разработке защищенных АС по профилю своей профессиональной деятельности;
ПК-11: способность участвовать в разработке компонентов АС в сфере профессиональной деятельности;
ПК-12: способность разрабатывать политики информационной безопасности АС;
ПК-13: способность участвовать в проектировании системы управления информационной безопасностью АС;
ПК-14: способность участвовать в проектировании средств защиты информации и средств контроля защищенности АС.

В результате изучения дисциплины специалист должен:

Знать:

- принципы построения и функционирования, примеры реализаций современных операционных систем;
- функции ОС, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами;
- критерии оценки эффективности и надежности средств защиты ОС;
- принципы организации и структуру подсистем защиты ОС семейств UNIX и Windows;

Уметь:

- использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;
- оценивать эффективность и надежность защиты операционных систем;
- планировать политику безопасности операционных систем;

Владеть:

- навыками работы с операционными системами семейств Windows и UNIX с учетом требований по обеспечению информационной безопасности.

.