МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Технологии обеспечения информационной безопасности

Направление подготовки: 10.04.01 – Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

Форма обучения: Очная

Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины является:

изучение студентами теории и практики основ технологий обеспечения информационной безопасности в автоматизированных системах, создаваемых на базе аппаратно-программных платформ отечественного производства, предназначенных для защиты следующих видов информации:

-конфиденциальной информации;

-коммерческой тайны;

-персональных данных.

Под автоматизированной системой (далее – АС) обработки информации мы будем понимать совокупность следующих объектов:

-средств вычислительной техники, включающих в свой состав операционную систему со встроенным комплексом средств защиты информации;

-специального и прикладного программного обеспечения;

-каналов связи;

-информации на различных носителях;

-персонала и пользователей системы.

Информационная безопасность АС рассматривается как состояние системы, при котором:

-система способна противостоять дестабилизирующему воздействию внешних и внутренних угроз;

-функционирование и сам факт наличия системы не создают угроз для внешней среды и для элементов самой системы.

На практике информационная безопасность рассматривается как совокупность трех базовых свойств защищаемой информации – конфиденциальности, целостности и доступности.

Исходя из изложенного, студенты должны научиться использовать технологии из состава комплекса средств защиты информации, реализованные в отечественной защищенной операционной системе, прикладного программного обеспечения, а также предоставляемых средой разработки программного обеспечения для создания автоматизированных систем рассматриваемого класса.

В процессе освоения данной дисциплины обучаемый формирует и демонстрирует следующие профессиональные профильно-специализированные компетенции:

-способность понимать основные положения теории информационной безопасности, основы формальной теории защиты информации;

-способность понимать нормативно-правовую базу и стандарты в области информационной безопасности в автоматизированных системах.

-способность понимать архитектуру состав, принципы функционирования отечественных защищенных операционных систем и аппаратно-программных платформ на их основе, а также анализировать направления развития архитектуры отечественных средств вычислительной техники и информационных технологий в области создания АС;

-способность анализировать функциональные возможности, принципы реализации, состав контролируемых функций комплексом средств защиты информации, реализованного в защищенной операционной системе;

-способность пользовательской работы, основ администрирования и управления безопасностью в защищенной операционной системе;

-способность задания требований к системе обеспечения информационной безопасности АС, а также анализировать и выбирать конфигураций комплекса средств защиты информации, удовлетворяющих требованиям руководящих документов по созданию АС рассматриваемого класса защищенности.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач:

сбор и анализ исходных данных для проектирования;

разработка программ для решения прикладных задач с использованием высокопроизводительных систем в соответствии с техническим заданием с использованием;

изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

составление отчета по выполненному заданию, участие во внедрении результатов исследований и разработок.

Общая трудоемкость дисциплины (модуля) составляет 6 з.е. (216 академических часа(ов).