Аннотация к рабочей программе дисциплины «Основы информационной безопасности»

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

Общая трудоемкость дисциплины составляет 4 зачетных единиц (144 часов).

Предполагаемые семестры: 4

Форма контроля: экзамен

Цель:

освоение учебной дисциплины (модуля): сформировать у студентов знания по основам обеспечения информационной безопасности в различных областях деятельности современного общества.

Задачи дисциплины:

Дать студентам необходимые знания, умения и навыки, в том числе:

теоретические и практические проблемы обеспечения информационной безопасности на предприятиях, транспорте и в бизнесе;

навыки самостоятельного, творческого использования теоретических знаний для предотвращения незаконного использования информации в практической деятельности.

Учебная дисциплина относится к циклу Б1. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- математика;
- физика;
- информатика.

В дисциплине «Основы информационной безопасности» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- организационное и правовое обеспечение информационной безопасности;
- программно-аппаратные средства обеспечения информационной безопасности;
- управление информационной безопасностью;
- разработка и эксплуатация защищенных автоматизированных систем;
- информационная безопасность автоматизированных транспортных систем;
- информационная безопасность информационно-управляющих и информационно - логистических систем;
- противодействие техническим разведкам.

Краткое содержание дисциплины:

Понятие национальной безопасности, основные понятия, общеметодологические принципы теории ИБ, государственная информационная политика; проблемы региональной информационной безопасности, анализ угроз ИБ и источников ИБ, проблемы информационной войны, методы и средства обеспечения ИБ.

В результате изучения дисциплины, специалист должен обладать следующими профессиональными компетенциями (ПК):

ПК-4: способностью проводить анализ защищенности автоматизированных систем.

ПК-19: способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности.

ПК-20: способностью разрабатывать оперативные планы работы первичных подразделений.

ПК-21: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы.

ПК-22: способностью организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности.

ПК-23: способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности .
ПК-24: способностью проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите.

ПК-25: способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации.
ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы.

В результате изучения дисциплины специалист должен:

Знать:

– место и роль информационной безопасности в системе национальной безопасности Российской федерации;
– основные нормативные правовые акты в области информационной безопасности и защиты, а также нормативные методические документы Федеральной службы безопасности Российской федерации;
– правовые основы организаци защиты государственной тайны и и конфиденциальной информации, задачи органов защиты государственной тайны;
– принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
– опасные и вредные факторы системы "человек - среда обитания", методы анализа антропогенных опасностей, научные и организационные сновы защиты окружающей среды и ликвидации последствий, аварий, катастроф, стихийных бедствий.

Уметь:

- анализировать и оценивать угрозы информационной безопасности объекта;
- пользоваться нормативными документами по защите информации;
- анализировать и оценивать степень риска проявления факторов опасности системы "человек - среда обитания", осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности.

Владеть:

- навыками работы с нормативными правовыми актами;
- профессиональной терминологией.

.