Аннотация к рабочей программе дисциплины «Организационное и правовое обеспечение информационной безопасности»

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

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов).

Предполагаемые семестры: 5.

Форма контроля: зачет

Целями освоения учебной дисциплины являются: изучение способов разработки и реализации мер по организации на предприятиях, государственных учреждениях информационной безопасности; решение задач, требующих классификации и структуризации объектов информационной безопасности от степени конфиденциальности.

Задачами курса являются: изучение основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, а также понятие и виды компьютерных преступлений.

Учебная дисциплина «Организационное и правовое обеспечение информационной безопасности» входит в математический и естественнонаучный цикл (базовая часть). Дисциплина является самостоятельным элементом в системе подготовки специалиста, относится к циклу Б.1.Б.26. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин: “Основы информационной безопасности”; “Информатика”.

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

- “Разработка и эксплуатация защищенных автоматизированных систем”;
- “Информационная безопасность автоматизированных транспортных систем”;
- “Информационная безопасность информационно-управляющих и информационно-логистических систем”.

Краткое содержание дисциплины:

Актуальность информационной безопасности (ИБ) для организаций.

Конфиденциальность информации.

Информационная инфраструктура организации.

Определение правил или политики ИБ в организациях и учреждениях.

Организация защиты информации и реализация подходов, определенных политикой ИБ (основные принципы).

Контроль или аудит ИБ, оценка уровня ИБ.

Управление ИБ.

Допуска к секретной (конфиденциальной) информации

Организация охраны объектов.

В результате изучения дисциплины специалист должен обладать следующими компетенциями:

ПК-4: способностью проводить анализ защищенности автоматизированных систем.

ПК-5: способностью разрабатывать модели угроз и модели нарушителя ИБ автоматизированной системы.

ПК-6: способностью проводить анализ рисков ИБ автоматизированной системы.

ПК-7: способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем.

ПК-8: способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ.

ПК-9: способностью проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем.

ПК-10: способностью участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности.

ПК-11: способностью участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности;

ПК-12: способностью разрабатывать политики ИБ автоматизированных систем;

ПК-13: способностью участвовать в проектировании системы управления ИБ автоматизированной системы;

ПК-14: способностью участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы;

ПК-15: способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

ПК-16: способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем;

ПК-17: способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации;

ПК-18: способностью проводить инструментальный мониторинг защищенности автоматизированных систем.

В результате изучения дисциплины специалист должен:

Знать:

- основы организационного и правового обеспечения ИБ;
- основные нормативные, правовые акты в области обеспечения ИБ и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;
- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;
- организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.

Уметь:

- применять нормативные правовые акты и нормативные методические документы в области обеспечения ИБ;
- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.

Владеть:

- навыками работы с нормативными правовыми актами;
- навыками организации и обеспечения режима секретности;
- методами организации и управления деятельностью служб защиты информации на предприятии;
- методами формирования требований по защите информации.