АННОТАЦИЯ
рабочей программы дисциплины «Организационное и правовое обеспечение информационной безопасности»
по направлению подготовки 10.03.01 Информационная безопасность

1. Цели освоения дисциплины.

Целями освоения учебной дисциплины «дисциплины «Организационное и правовое обеспечение информационной безопасности» являются раскрыть 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.

2. Требования к уровню освоения содержания дисциплины.

Процесс изучения дисциплины «Организационное и правовое обеспечение информационной безопасности» направлен на формирование следующих компетенций:

ОК – 2 – способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм.

ОК – 5 – способностью к кооперации с коллегами, работе в коллективе.

ОК – 6 – способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность.

ОК – 7 – способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства.

ОК – 8 – способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления

ПК-4 - способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.

ПК-8 -.способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия.

ПК-9 -способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия.

ПК-26 - способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

3. Требования к результатам освоения дисциплины.

В результате изучения дисциплины обучающиеся должны:

знать:

- содержание основных понятий по правовому обеспечению информационной безопасности;
- правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;
- понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации;
- основы правового регулирования взаимоотношений администрации и персонала в области защиты информации;

- правила лицензирования и сертификации в области защиты информации;
- виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений.

уметь:

- отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- применять действующую законодательную базу в области информационной безопасности;
- разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов.

владеть:

- понятиями информационного права как основы информационного общества;
- об информационном праве как основе информационного общества.

4. Содержание дисциплины.

Основные положения организации информационной безопасности. Угрозы информационной безопасности. Построение систем защиты от угроз нарушения конфиденциальности информации. Модели систем защиты. Организационные меры и меры обеспечения физической безопасности. Идентификация и аутентификация. Методы разграничения доступа. Методы защиты внешнего периметра автоматизированных вычислительных систем. Протоколирование и аудит. Построение систем защиты от угроз нарушения целостности информации. Принципы обеспечения целостности информации. Построение систем защиты от угроз нарушения доступности. Основы формальной теории защиты информации. Основные определения. Мониторинг безопасности обращений к вычислительным ресурсам. Совместное использование моделей безопасности. Стандарты в информационной безопасности. Общие сведения. «Оранжевая книга». Руководящие документы Гостехкомиссии России. Структура и содержание профиля защиты. Структура и содержание задания по безопасности. Основные нормативно-правовые документы обеспечения информационной безопасности.

Разработчик: Воробьева О.В.

Зав. информационной, техносферной безопасности и правовой защиты информации **О.В. Воробьева**

Председатель Межкафедрального координационного учебно-методического совета **И.В. Анциферова**