Аннотация к рабочей программе дисциплины

Автор: Урбан В.А, доцент, канд.техн.наук
Наименование дисциплины: Б1.О.06 Организационное и правовое обеспечение информационной безопасности
Цель освоения дисциплины: заключается в совершенствовании знаний, умений и навыков обучающихся, а также получение ими дополнительных знаний, умений и навыков по вопросам организационного и правового обеспечения информационной безопасности.

1. Требования к результатам освоения дисциплины:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине (модулю)**
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1 Проводит анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	*Знать:* возможных источники информационных угроз, цели, пути реализации и виды ущерба *Уметь:* проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба *Владеть:* методикой определения актуальных угроз
	ОПК-2.2 Формирует предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям	*Знать:* меры и мероприятия по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям *Уметь:* работать с нормативно-методической базой, в которой отображены меры и мероприятия по повышению устойчивости объектов защиты к деструктивным воздействиям *Владеть:* методами по оптимизации структуры и функциональных

		процессов объекта защиты
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.3 Разрабатывает, внедряет и сопровождает комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	*Знать:* комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности *Уметь:* использовать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности *Владеть:* методами обеспечения безопасности объекта защиты
	ОПК-2.4 Проводит аудит защищенности объекта информатизации в соответствии с нормативными документами	*Знать:* Нормативно-методические документы и стандарты в области проведения аудита информационной безопасности *Уметь:* проводить аудит защищенности объекта информатизации в соответствии с нормативными документами *Владеть:* Методами проведения аудита защищенности объектов информатизации
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.1 Применяет математические модели и решать задачи помехоустойчивого кодирования при проектировании защищенных автоматизированных систем	*Знать:* математические модели при проектировании защищенных автоматизированных систем *Уметь:* использовать математические модели и решать задачи при проектировании защищенных автоматизированных систем *Владеть:* Методами проектирования защищенных автоматизированных систем
	ОПК-5.2 Применяет технологии защиты информации при создании защищенных автоматизированных систем	*Знать:* технологии защиты информации при создании защищенных автоматизированных систем *Уметь:* применять

		нормативно-методическую базу при построении защиты информации при создании защищенных автоматизированных систем *Владеть:* владеть технологиями защиты информации при создании защищенных автоматизированных систем
	ОПК-5.3 Осуществляет эксплуатацию и проводить техническое обслуживание защищенных автоматизированных систем	*Знать:* нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по эксплуатации и техническому обслуживанию защищенных автоматизированных систем *Уметь:* применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по эксплуатации и техническому обслуживанию защищенных автоматизированных систем *Владеть:* нормативными правовыми актами, нормативными и методическими документами при эксплуатации и обслуживании защищенных автоматизированных систем
	ОПК-5.4 Проводит мониторинг функционирования защищенных автоматизированных систем	*Знать:* нормативные правовые акты, нормативные и методические документы, регламентирующие мониторинг функционирования защищенных автоматизированных систем *Уметь:* применять нормативные правовые акты, нормативные и методические документы, регламентирующие мониторинг функционирования защищенных автоматизированных систем *Владеть:* методами мониторинга функционирования

		защищенных автоматизированных систем

2. Содержание дисциплины:

Тема1. Понятие, структура информационного правоотношения. Стратегия национальной безопасности Российской Федерации. Обеспечение национальной безопасности Российской Федерации. Концепция национальной безопасности Российской Федерации. Стратегии развитияинформационного общества в РоссийскойФедерации.

Тема 2. Общаяхарактеристика информационно- правовых норм. Органызаконодательства, регламентирующие деятельность по информационной безопасности. Структура органов власти по защите информации в Российской Федерации. Совет Безопасности Российской. Федерации. Межведомственные и государственные комиссии, создаваемыеПрезидентом Российской Федерациии Правительством Российской Федерации,решают в соответствиис предоставленными имполномочиями задачи обеспечения информационной безопасности Российской Федерации.Федеральная служба безопасности Российской Федерации(ФСБ). Федеральная Служба по техническому и экспортному контролюРФ (ФСТЭК РФ). Комитет по вопросам информационной безопасности. Понятиеи виды защищаемойинформации по российскому законодательству. Информация как объектгражданских прав.

Тема 3. Регуляторы в области защиты ПДн. Требования материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Особенности обработки персональных данных,осуществляемой безиспользования средств автоматизации.

Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данныхпри их обработке в информационных системах персональныхданных. Базовая модельугроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методика определения актуальных угрозбезопасности персональных данныхпри их обработке в информационных системах персональных данных. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке винформационных системах персональныхданных с использованием средств автоматизации.

Тема 4. Режим защиты государственных информационныхсистем.

Тема 5.Интеллектуальная собственность

Тема 6. Коммерческая тайна. Сущность, задачи и особенности защиты коммерческой тайны. Меры по обеспечению защиты коммерческой тайны. Классификация мер защиты коммерческой тайны. Ответственность за нарушение коммерческой тайны.

Тема 7. Служебная тайна. Профессиональная тайна. Тайна следствия судопроизводства. Отличие служебной тайны от профессиональной. Требования к защите служебной и профессиональной тайны. Ответственность за нарушение области защиты служебной и профессиональной тайн.

Тема 8. Режимзащиты государственной тайны

3. Общая трудоемкость дисциплины: 5 ЗЕ