

Аннотация к рабочей программе дисциплины

Автор: В.А.Урбан

Наименование дисциплины: Б1.Б.13 Основы информационной безопасности

Цель освоения дисциплины:

- формирование знаний основных составляющих информационной безопасности государства, общества и личности;
- выработка умений и навыков использования организационных, правовых, инженерно-технических и аппаратно-программных методов и средств при построении систем информационной безопасности;
- развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры;
- развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления;
- привитие стремления к поиску оптимальных, простых и надежных решений;
- расширение кругозора.

1. Требования к результатам освоения дисциплины:

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ОК-5- Способностью понимать социальную значимость своей будущей профессии и обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Этап 1: Цели, задачи, принципы и основные направления обеспечения информационной безопасности государства	Этап 1: Проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня защиты с учетом развития всех видов обеспечений вычислительных систем	Этап 1: Профессиональной терминологией и методами теоретического обоснования в выборе оптимальной концепции информационной безопасности
ОК-5- Способностью понимать социальную значимость своей будущей профессии и обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и госу-	Этап 2: Современные подходы к построению систем защиты информации	Этап 2: Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.	Этап 2: Владеть методологическими принципами оценки защищенности объектов информатизации и обеспечения требуемого уровня защиты

дарства, соблюдать нормы профессиональной этики			
---	--	--	--

4.2. Содержание дисциплины:

Раздел 1 Основы информационной безопасности. Общие положения. Основные понятия. Аттестация объектов информатизации по требованиям безопасности информации. Защита сведений, составляющих государственную тайну.

Тема 1 Основные понятия, термины и определения. Основы государственной политики в области информационной безопасности.

Тема 2 Аттестация объектов информатизации по требованиям безопасности информации.

Тема 3 Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне». Организационно-технические меры защиты сведений, составляющих государственную тайну.

Раздел 2 Защита коммерческой тайны.

Тема 4 Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации». Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне». Организационно-технические меры защиты коммерческой тайны.

Тема 5 Государственные информационные системы. Защита персональных данных, обрабатываемых в информационных системах персональных данных. Защита данных, обрабатываемых в государственных информационных системах.

Тема 6 Защита информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

Тема 7 Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных». Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Раздел 3 Классификация мер обеспечения безопасности.

Тема 8 Нормативно-правовые, морально-этические, административные, физические и технические меры.

3. Общая трудоёмкость дисциплины: 4 ЗЕ