

Аннотация к рабочей программе дисциплины

Автор: Урбан В.А, доцент, канд.техн.наук

Наименование дисциплины: Б1.В.04 Технология построения защищенных автоматизированных систем

Цель освоения дисциплины: заключается в подготовке бакалавра к построению автоматизированных систем в защищенном исполнении, в освоении принципов системного подхода при создании сложных систем, современные тенденции программной инженерии, нормативно-методического обеспечения и принципов создания автоматизированных систем, стандарт жизненного цикла автоматизированных систем, модели жизненного цикла автоматизированных систем, оценку процессов создания автоматизированных систем, проблематика комплексного обеспечения информационной безопасности автоматизированных систем, особенности синтеза комплексных систем информационной безопасности, методы и методики их оценки, аттестацию по требованиям безопасности, особенности эксплуатации комплексных систем информационной безопасности на объекте защиты, модели защиты информации и реализацию систем управления доступом.

1. Требования к результатам освоения дисциплины:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)
ПК-1 Способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	ПК-1.1 Разрабатывает предложения по совершенствованию системы управления защиты информации автоматизированных систем	<p><i>Знать:</i> основные составляющие политики безопасности</p> <p><i>Уметь:</i> разрабатывать политику безопасности</p> <p><i>Владеть:</i> навыками разработки политики безопасности</p>
	ПК-1.2 Применяет технические средства контроля эффективности мер защиты информации	<p><i>Знать:</i> принципы разработки политики безопасности</p> <p><i>Уметь:</i> применять комплексный подход к обеспечению информационной безопасности</p> <p><i>Владеть:</i> навыками применения комплексного подхода к обеспечению информационной безопасности</p>

ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	ПК-4.1 Оценивает информационные риски в автоматизированных системах	<p><i>Знать:</i> основные требования безопасности информации к объектам информатизации</p> <p><i>Уметь:</i> разрабатывать требования безопасности информации</p> <p><i>Владеть:</i> навыками в формировании требований безопасности информации</p>
	ПК-4.2 Способен классифицировать и оценивать угрозы безопасности информации	<p><i>Знать:</i> основные этапы аттестации объектов информатизации по требованиям безопасности информации</p> <p><i>Уметь:</i> разрабатывать методику аттестации объектов информатизации</p> <p><i>Владеть:</i> навыками в проведении аттестации объектов информатизации</p>
ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	ПК-4.3 Определяет подлежащие защите информационные ресурсы автоматизированных систем	<p><i>Знать:</i> основные этапы проектирования подсистемы информационной безопасности</p> <p><i>Уметь:</i> разрабатывать основные подсистемы безопасности информации</p> <p><i>Владеть:</i> навыками разработки подсистем информационной безопасности</p>
	ПК-4.4 Применяет нормативные документы по противодействию технической разведки	<p><i>Знать:</i> основные методы технико – экономического обоснования проектных решений</p> <p><i>Уметь:</i> проводить технико – экономическое обоснование проектных решений</p> <p><i>Владеть:</i> навыками технико – экономического обоснования проектных решений</p>

2. Содержание дисциплины:

Тема 1. Методологии проектирования автоматизированных систем

Тема 2. Проектирование комплексного обеспечения информационной безопасности

3. Общая трудоемкость дисциплины: 3 ЗЕ