Аннотация к рабочей программе дисциплины
Автор: Урбан В.А.
Наименование дисциплины: Б1.Б.1.25 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	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

государства, соблюдать нормы профессиональной этики			
ОПК-5 Способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Этап 1 Знать основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики.	Этап 1 Уметь взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности в научных исследованиях и проектно-конструкторской деятельности, а также в управлении технологическими, экономическими и социальными системами	Этап 1 Навыки строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач.
ОПК-5 Способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Этап 2 Знать принципы и методы разработки и применения систем обеспечения информации в научных исследованиях и в управлении технологическими, организационно-экономическими и социальными системами	Этап 2 Использовать полученные знания при реализации реальных проектов.	Этап 2 Навыки пользования библиотеками прикладных программ для решения прикладных математических задач
ПК-4 Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной	Этап 1 Угрозы безопасности и методы защиты информации в банковских ин-формационных системах	Этап 1 Выявлять угрозы системе информационной безопасности разрабатывать комплекс мер по ее совершенствовани ю	Этап 1 Оценки эффективности систем защиты информации автоматизированны х систем

безопасности объекта защиты			
ПК-4 Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Этап 2 Основные правила разработки политики безопасности организации. Компоненты политики безопасности	Этап 2 Умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	Этап 2 Навыки применения комплексного подхода к обеспечению информационной безопасности автоматизированных систем
ПК-5 Способностью проводить анализ рисков информационной безопасности автоматизированной системы	Этап 1 Знать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ	Этап 1 Определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	Этап 1 Навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности
ПК-5 Способностью проводить анализ рисков информационной безопасности автоматизированной системы	Этап 2 Знать цели и задачи, решаемые разрабатываемыми процессами управления ИБ	Этап 2 Оценивать информационные риски в автоматизированных системах	Этап 2 Навыками и методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем, методы оценки информационных рисков
ПК-11 Способностью разрабатывать	Этап 1 Основные правила разработки	Этап 1 Умения разработки политики	Этап 1 Внедрения политики

политику информационной безопасности автоматизированной системы	политики организации. Компоненты политики безопасности	безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю;	безопасности в организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю
ПК-11 Способностью разрабатывать политику информационной безопасности автоматизированной системы	Этап 2 Принципы и методы противодействия несанкционированному информационному воздействию на информационные системы и системы передачи информации.	Этап 2 Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.	Этап 2 Навыки применения комплексного подхода к обеспечению информационной безопасности объекта защиты
ПК-22 Способностью участвовать в формировании политики	Этап 1 Основные правила разработки политики безопасности	Этап 1 Умения разработки политики безопасности организации,	Этап 1 Внедрения политики безопасности в организации,

информационной безопасности организации и контролировать эффективность ее реализации	организации. Компоненты политики безопасности	согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю
ПК-22 Способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Этап 2 Принципы и методы противодействия несанкционированному информационному воздействию информационные системы	Этап 2 Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.	Этап 2 Навыки применения комплексного подхода к обеспечению информационной безопасности объекта защиты

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.
Раздел 3 Государственные информационные системы. Защита персональных данных, обрабатываемых в информационных системах персональных данных. Защита данных, обрабатываемых в государственных информационных системах.
Тема 5 Защита информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.
Тема 6 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 4 Классификация мер обеспечения безопасности.
Тема 7 Нормативно-правовые, морально-этические, административные, физические и технические меры.

3. Общая трудоёмкость дисциплины: 2 ЗЕ