Б1.Б.25 Теория информационной безопасности и методология защиты информации

Объем дисциплины (модуля) **6 ЗЕТ (216 час)**

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
Цель дисциплины: Системно изложить современный подход к вопросам информационной безопасности и защиты информации в Российской Федерации. Задачи дисицлпниы: Получение навыков системного использования и применениея основных принципов и методологии построения эффективных систем защиты информации; изучение нормативных правовых документов, действующих в данной предметной области.

ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ
УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
УК-1.3: Выполняет поиск необходимой информации, ее критический анализ и обобщает результаты анализа для решения поставленной задачи
УК-10: Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности
УК-10.3: Идентифицирует и оценивает коррупционные риски в области профессиональной деятельности, анализирует документы, определяющие практику противодействия терроризму, экстремизму и коррупционному поведению в профессиональной деятельности и имеет навык их применения
ОПК-8: Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;
ОПК-8.2: Анализирует и обобщает научно-техническую литературу, нормативные и методические документы для решения поставленной задачи профессиональной деятельности
ОПК-8.1: Использует электронные информационные ресурсы для поиска научно-технической литературы, нормативных и методических документов в области профессиональной деятельности
ОПК-2.1: Способен 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;
ОПК(п)-2.1.2: Выявляет источники информационных угроз, их возможные цели, пути реализации
ОПК(п)-2.1.3: Оценивает предполагаемый ущерб от реализации информационных угроз
ОПК(п)-2.1.1: Знает функциональные процессы и информационные составляющие объектов защиты
ОПК-2.3: Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ОПК(п)-2.3.2: Знает и применяет международные и национальные стандарты в области информационной безопасности

В результате освоения дисциплины обучающийся должен

Знать: направления обеспечения информационной безопасности государства; основные термины по проблематике информационной безопасности; методологию создания систем защиты информации; перспективные направления развития средств и методов защиты информации; роль и место информационной безопасности в системе национальной безопасности; основы организационного и правового обеспечения информационной безопасности; классификацию защищаемой информации; классификацию угроз защищаемой информации.
Уметь: выбирать показатели качества и критерии оценки систем и средств защиты информации; пользоваться современной научно-технической информацией по вопросам безопасности; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и модели нарушителей информационной безопасности выявлять уязвимости информационных ресурсов, проводить мониторинг угроз информационной безопасности.
Владеть: навыками поиска нормативной правовой информации,необходимой для профессиональной деятельности; навыками обоснования, выбора, реализации и контроля результатов управленческого решения; навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; навыками работы с нормативными правовыми актами.

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Кнцептуальные понятия информационной безопасности
Раздел 2. Технология создания политики безопасности