Аннотация рабочей программы дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем» для направления подготовки 10.03.01 Информационная безопасность.
Направленность (профиль) образовательной программы - Безопасность автоматизированных систем (по отраслям или в сфере профессиональной деятельности)

1. Цели и задачи освоения дисциплины

Цель изучения дисциплины:

изучение основ проектирования комплексной системы информационной безопасности (КСИБ), соотношения программных, аппаратных и организационных средств и методов в комплексной деятельности по защите информации (ЗИ) в автоматизированных системах (АС).

Задачи изучения дисциплины:

-освоение способов выделения информации в АС, подлежащей защите;
-изучение критериев защищённости АС, методологии построения современных КСИБ, технологий проектирования систем защиты информации;
-формирование комплексного подхода к обеспечению информационной безопасности АС.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины и индикаторы их достижения

2.1 Общепрофессиональные компетенции и индикаторы их достижения

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ИД-1ОПК-10- знать: цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью, принципы формирования политики информационной безопасности объекта информатизации, принципы организации информационных систем в соответствии с требованиями по защите информации, особенности комплексного подхода к обеспечению информационной безопасности организации ИД-2ОПК-10- уметь: разрабатывать модели угроз и модели нарушителя объекта информатизации, оценивать информационные риски объекта информатизации, определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ИД-3ОПК-10- иметь навыки: участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;
ОПК-4.3. Способен выполнять	ИД-1ОПК-4.3знать: основные меры по защите

работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	информации в автоматизированных системах, содержание эксплуатационной документации автоматизированной системы ИД-2ОПК-4.3уметь: устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств ИД-3ОПК-4.3владеть: навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы

3. Содержание дисциплины

Постановка задачи комплексного обеспечения ИБ АС. Методология формирования задач защиты; интеграция средств защиты в технологическую среду. Типовая структура КСИБ; методы проектирования и оценки качества КСИБ. Этапы проектирования КСИБ и требования к ним. Структура политики информационной безопасности организации .