Аннотация рабочей программы дисциплины «Обеспечение безопасности информации в автоматизированных системах» 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:

Практическое закрепление знаний и навыков проектной, научно-исследовательской и организационной деятельности по основным направлениям информационной безопасности, овладение студентами практическими навыками, методами и средствами по обеспечению информационной безопасности в организациях и на предприятиях различных направлений и различных форм собственности.

Задачи изучения дисциплины:

В результате освоения дисциплины студент должен:

- знать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
- знать содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации;
- применять основные меры по защите информации в автоматизированных системах;
- знать содержание эксплуатационной документации автоматизированной системы.
- знать типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
- знать критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем;
- знать содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем.
- уметь определять подлежащие защите информационные ресурсы автоматизированных систем;
- разрабатывать политики безопасности информации автоматизированных систем;
- определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы;
- осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации;
- 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;
- создавать, удалять и изменять учетные записи пользователей автоматизированной системы;
- устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации;
- регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах;
- применять типовые программные средства резервирования и восстановления информации в автоматизированных системах;
- документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы.
- уметь осуществлять автономную наладку технических и программных средств системы защиты информации автоматизированной системы;
- уметь устанавливать обновления программного обеспечения автоматизированной системы;
- уметь обнаруживать и устранять неисправности в работе системы защиты

информации автоматизированной системы.

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

2.1 Профессиональные компетенции и индикаторы их достижения

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
ПК-2 Способен принимать участие в организации и проведения аудита защищенности информации в автоматизированных системах	ИД-1ПК-2- знать: методы контроля эффективности защиты информации от утечки по техническим каналам ИД-2ПК-2- уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем ИД-3ПК-2 - иметь навык применения инструментальных средств контроля защищенности информации в автоматизированных системах
ПК-5 Способен управлять защитой информации в автоматизированных системах	ИД-1ПК-5- знать: методы защиты информации от утечки по техническим каналам, национальные, межгосударственные и международные стандарты в области защиты информации, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах ИД-2ПК-5- уметь: Оценивать информационные риски в автоматизированных системах, классифицировать и оценивать угрозы безопасности информации ИД-3ПК-5 - иметь навык анализа воздействия изменений конфигурации автоматизированной системы на ее защищенность, анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации
ПК-6 Способен внедрять организационные меры по защите информации в автоматизированных системах	ИД-1ПК-6- знать: организационные меры по защите информации ИД-2ПК-6- уметь: реализовывать правила разграничения доступа персонала к объектам доступа, анализировать программные и программно- аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах ИД-3ПК-6 - иметь навык: подготовки документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом

	требований по защите информации

3. Содержание дисциплины

Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети. Основные механизмы защиты. Мониторинг и оперативное управление. Централизованная инвентаризация ресурсов локальной сети. Инспекции в автоматизированных системах. Централизованная защита от вирусов в локальной сети. Управление системой безопасности автоматизированной системы. Централизованный учет и управление программно-аппаратными средствами защиты информации. Управление жизненным циклом и аудит средств аутентификации. Нормативные требования по управлению средствами защиты информации.