Аннотация к рабочей программе дисциплины
Автор: В.С. Болотова
Наименование дисциплины: Б1.В.02 Теоретические основы защиты информации
Цель освоения дисциплины:

- ознакомить слушателей с современным состоянием проблемы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации в организациях и на предприятиях различных направлений деятельности и различных форм собственности, способов защиты от несанкционированного доступа к ней, рассмотреть на современном уровне вопросы разработки средств и систем сбора и защиты информации (ЗИ).

1. **Требования к результатам освоения дисциплины:**

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ОПК-7 - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Этап 1: принципы построения информационных систем;	Этап 1: использовать методы и средства разработки алгоритмов и программ, приемы структурного программирования,	Этап 1: методами анализа информационных процессов объекта.
ОПК-7 - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Этап 2: принципы организации информационных систем в соответствии с требованиями по защите информации.	Этап 2: использовать способы записи алгоритма на языке высокого уровня, способы отладки, испытания и документирования программ.	Этап 2: методами формализации информационных процессов объекта и связей между ними.
ПК-15 -	Этап 1:	Этап 1:	Этап 1:

способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	нормативные документы, регламентирующие работу ФСТЭК	проводить работы на автоматизированных системах специального назначения	основами инструментальными средствами проектирования аппаратных и программных средств автоматизированных систем специального назначения
ПК-15 - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Этап 2: нормативные документы, регламентирующие работу ФСБ	Этап 2: осуществлять инсталляцию, настройку и техническое сопровождение программного обеспечения	Этап 2: навыками оценки эффективности функционирования систем управления специального назначения

2. Содержание дисциплины:

Раздел 1 Введение. Основы криптологии

Тема 1 Проблема ЗИ. Место ЗИ в системе национальной безопасности. Системный анализ как составная часть безопасности. Риск. Группы риска. Пути несанкционированного получения информации. Цель и необходимость закрытия

информации. Объекты защиты, направления, методы и средства ЗИ. Комплексность и системность ЗИ. Законодательный, административный, процедурный и программно-технический уровни обеспечения безопасности. Основные понятия и определения теории ЗИ. Становление и развитие теории и техники ЗИ

Тема 2 Классификация методов ЗИ. Классификация по виду ЗИ, способу ЗИ, разновидности преобразования информации, способу реализации. Криптология, криптография и криптоанализ. Основные понятия криптологии. Стойкость, защищенность, имитостойкость, аутентичность

Раздел 2 Современные криптографические методы. Развитие и совершенствование криптографического закрытия информации

Тема 3 Криптография как наука. Понятие криптографического ключа. История криптографии и классические способы шифрования: замена, подстановка, перестановка, аналитическое преобразование, использование таблиц Вижинера, шифр Вернама, гаммирование, использование алгебры матриц. Комбинированное шифрование. Другие виды шифрования: рассечение-разнесение, сжатие-расширение. Современные системы шифрования. Основные принципы построения криптоалгоритмов

Тема 4 Методы исследования криптографических алгоритмов. Классические методы ЗИ и стойкость шифрования. Основные методы дешифрования. Шифры Цезаря, Виженера. Раскрытие несовершенных шифров. Криптографическая модель Шеннона. Теория криптоанализа. Стойкость шифра. Способы кодирования: смысловое, символьное

Раздел 3 Компьютерная организация информационных процессов и их защита от несанкционированного доступа. Разрушающие программные воздействия и защита от них

Тема 5 Защита файлов от изменения. Защита программ от несанкционированного копирования. Привязка программного обеспечения к аппаратному окружению и физическим носителям как единственное средство защиты от копирования программного обеспечения; привязка программ к гибким и жестким магнитным дискам

Тема 6 Компьютерные вирусы и антивирусные программы. Классификация вирусов. Изолированная программная среда и недопущение разрушающего воздействия

Раздел 4 Методы вскрытия защиты наборов данных на персональных компьютерах. Методы и механизмы защиты информации в компьютерных сетях

Тема 7 Фиксация доступа к файлам. Доступ к данным со стороны процесса. Понятие скрытого доступа. Особенности защиты исполняемых файлов от несанкционированного использования. Способы фиксации факта доступа. Надежность систем ограничения доступа. Пароли и ключи. Организация хранения ключей

Тема 8 Особенности защиты информации на узлах компьютерной сети. Способы защиты от нападений. Безопасное подключение к сети. Шифрование, контроль и разграничение доступа. Понятие корпоративной информационной системы. Защита сетевого файлового ресурса

3. Общая трудоёмкость дисциплины: 3E