

Аннотация рабочей программы дисциплины (модуля)

Б1.В.ДВ.01.01 Защита конфиденциальной информации в организации

1. Цель и задачи дисциплины

Цель дисциплины

Целью дисциплины «Защита конфиденциальной информации в организации» является обучение приемам и методам работы с конфиденциальной информацией в организациях; владение навыками применения комплексного подхода к обеспечению информационной безопасности конфиденциальных документов.

Задачи дисциплины

- Изучение правил и нормативных документов реализации политики информационной безопасности по защите и обработке конфиденциальных документов.
- Развитие знаний и умений в области документооборота при обращении с конфиденциальной информацией, анализировать возможные пути утечки информации и принимать меры по их устранению.
- Формирование компетенций в области сбора и анализа исходных данных для проектирования средств обеспечения информационной безопасности.
- Обеспечение условий для активизации познавательной деятельности студентов и формирования у них практического опыта работы с системами защиты конфиденциальной информации.

Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС–2	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ПКС-2.1 Знать способы решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации. ПКС-2.2 Уметь решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации ПКС-2.3 Иметь навыки решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации
ПКС–3	Способен осуществлять управление средствами защиты информации, в том числе осуществляющими непрерывный	ПКС-3.1 Знать программно-аппаратные средства защиты информации, современные подходы к разработке и эксплуатации автоматизированных систем, средства управления и защиты автоматизированных систем. ПКС-3.2 Уметь применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и

	мониторинг защищенности автоматизированных систем	дефрагментации диска), в том числе средства, осуществляющие непрерывный мониторинг защищенности автоматизированных систем. ПКС-3.3 Владеть навыками выбора программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.
--	---	---

Содержание разделов дисциплины

Тема 1. Введение в организацию конфиденциального делопроизводства и защиты коммерческой тайны

Законодательная сторона защиты конфиденциальной информации в организации. Иерархия законодательных органов, порядок создания законов и подзаконных актов, область действия по времени и месту. Охраняемые сведения, понятия тайны и ее виды применительно к различным организациям. Основные законы, связанные с конфиденциальным делопроизводством. Организация конфиденциального делопроизводства. Особенности организации конфиденциального делопроизводства с использованием электронного документооборота. ФСБ, ФСТЭК, Роскомнадзор, Роспатент и другие организации, являющиеся регуляторами по отношению к вопросам конфиденциального делопроизводства.

Тема 2. Жизненный цикл конфиденциального документа

Путь конфиденциального делопроизводства от создания до уничтожения. Составление номенклатур, формирование и оформление конфиденциальных дел. Подготовка конфиденциальных документов для архивного хранения и уничтожения. ГОСТ Р 51275-2006 Защиты информации. Защита конфиденциальной информации при ее передаче по сети. Система защищенного электронного документооборота. Основные задачи, решаемые системами электронного документооборота. Электронно-цифровая подпись.

Тема 3 Программные средства защиты конфиденциальной информации

Антивирусная защита. Межсетевые экраны как средство защиты от несанкционированного доступа. Криптографические средства. Сканеры уязвимостей. Системы обнаружения атак. Парольная защита. Идентификация и аутентификация. Модели разграничения доступа к информационным системам и ресурсам. Виды электронной подписи и принципы использования. Удостоверяющие центры и сертификат ключа. Квалифицированный сертификат.

Тема 4 Технические средства защиты конфиденциальной информации

Общетехнические средства контроля физического доступа к конфиденциальной информации. Разрешительная система доступа к конфиденциальной информации. Санкционированный и несанкционированный доступ. Электронные ключи и замки. Биометрические системы аутентификации. Система видеонаблюдения. Система охраны периметра.