

## Аннотация дисциплины

Наименование дисциплины	<b>Защита и обработка конфиденциальных документов</b>
Содержание	<p>Понятие «конфиденциальные документы». Нормативные материалы по организации режима «коммерческой тайны». Структура защищенного документооборота, документопотоки. Принципы учета конфиденциальных документов. Технология издания и обработки подготовленных конфиденциальных документов. Состав технологический этапов и операций. Порядок работы персонала с конфиденциальными документами. Контроль исполнения документов. Порядок составления и оформления номенклатуры дел. Формирование и хранение дел, содержащих конфиденциальные документы. Проверка наличия конфиденциальных документов. Хранение конфиденциальных дел в архиве. Особенности защиты информации в системах электронного документооборота.</p>
Реализуемые компетенции	<p>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 (ОПК-7)</p> <p>способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)</p> <p>способностью разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение (ПСК-5)</p>
Результаты освоения дисциплины (модуля)	<p><b>ОПК-7</b>  <b>Знать:</b> нормативные требования по защите информации;          - классификацию конфиденциальной информации.  <b>Уметь:</b> анализировать и оценивать угрозы информационной безопасности объекта;  <b>Владеть:</b> навыками выявления и уничтожения компьютерных вирусов;</p> <p><b>ПК-4</b>  <b>Знать:</b> основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;          - правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;          - принципы и методы организационной защиты информации;  <b>Уметь:</b> формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;          - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;</p>

	<p>- анализировать и оценивать угрозы информационной безопасности объекта;</p> <p><b>Владеть:</b> навыками работы с нормативными правовыми актами;</p> <p>- навыками организации и обеспечения режима секретности;</p> <p>- методами формирования требований по защите информации;</p> <p>- методами организации и управления деятельностью служб защиты информации на предприятии;</p> <p>- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;</p> <p><b>ПСК-5</b></p> <p><b>Знать:</b> Методы разработки комплекса организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение.</p> <p><b>Уметь:</b> разрабатывать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение.</p> <p><b>Владеть:</b> Навыками разработки комплекса организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение.</p>
Трудоемкость, з.е.	4 з.е.
Форма отчетности	Зачет с оценкой – 5 семестр
<b>Перечень основной и дополнительной литературы, необходимой для освоения дисциплины</b>	
Основная литература	<ol style="list-style-type: none"> <li>1. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие/ В. Ф. Шаньгин- М.: ИНФРА-М, 2012.</li> <li>2. Куняев Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник/Н.Н. Куняев, А.С. Демущкин, А.Г. Фабричнов; под общ.ред. Н.Н. Куняева. – М.: Логос, 2011. – 452 с.</li> </ol>
Дополнительная литература	<ol style="list-style-type: none"> <li>1. Емельянова, Н.З. Защита информации в персональном компьютере: учеб. пособие/ Н. З. Емельянова, Т. Л. Партыка, И. И. Попов- М.: ФОРУМ, 2012.</li> <li>2. Делопроизводство: Образцы, документы. Организация и технология работы. Более 120 документов: с учетом нового ГОСТ Р 6.30-2003 "Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов" [Текст] : справочное издание.- 2-е изд., перераб. и доп. - М. : ТК Велби : Изд-во Проспект, 2012. - 456 с..</li> <li>3. Кузнецов А.А. Защита деловой информации (секреты безопасности) – М.: Изд-во «Экзамен», 2013. – 255 с.</li> <li>4. Корнеев, И.К. Защита информации в офисе: учебник/ И. К. Корнеев, Е. А. Степанов- М.: ТК Велби, 2013.</li> </ol>