Аннотация дисциплины

Наименование дисциплины	**Комплексная система защиты информации на предприятии**
Содержание	Сущность и задачи комплексной системы защиты информации (КСЗИ). Принципы организации и этапы разработки КСЗИ. Факторы, влияющие на организацию КСЗИ. Определение и нормативное закрепление состава защищаемой информации. Определение объектов защиты. Анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию. Определение потенциальных каналов и методов несанкционированного доступа к защищаемой информации. Определение компонентов КСЗИ. Определение условий функционирования КСЗИ. Разработка модели КСЗИ. Технологическое и организационное построение КСЗИ. Кадровое обеспечение функционирования КСЗИ. Материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ. Назначение, структура и содержание управления КСЗИ. Принципы и методы планирования функционирования КСЗИ. Сущность и содержание контроля функционирования КСЗИ. Управление КСЗИ в условиях чрезвычайных ситуаций. Состав методов и моделей оценки эффективности КСЗИ.
Реализуемые компетенции	способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4) 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) способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1) способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2) способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3) способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4) способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7) способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8) способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)

	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13) 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 (ПК-15)
Результаты освоения дисциплины (модуля)	**ОК-4** **Знать** правовые основы защиты конфиденциальной информации и документов -структуру защищенного документооборота; -состав технологических этапов и операций; -правила подготовки и издания конфиденциальных документов; -организацию сохранности конфиденциальных документов; -порядок использования конфиденциальных архивных документов; -организационные методические проблемы автоматизации делопроизводственных операций по документам; **Уметь** работать с конфиденциальными управленческими (деловыми) и научно-техническими документами в соответствии с нормами и правилами Российского законодательства; -составлять и издавать конфиденциальные документы; **Владеть** способностью использовать основы правовых знаний в области защиты конфиденциальных документов **ОПК-7** **Знать:** нормативные требования по защите информации; - классификацию конфиденциальной информации. **Уметь:** анализировать и оценивать угрозы информационной безопасности объекта; **Владеть:** навыками выявления и уничтожения компьютерных вирусов; **ПК-1** **Знать:** требования по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; **Уметь: у**станавливать, настраивать и обслуживать программные, программно-аппаратные (в том числе криптографические) и технические средства защиты информации; **Владеть:** способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации **ПК-2** **Знать:** программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач **Уметь:** применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач **Владеть:** способностью применять программные средства системного, прикладного и специального назначения,

	инструментальные средства, языки и системы программирования для решения профессиональных задач **ПК-3** **Знать:** методы администрирования подсистемы информационной безопасности объекта защиты; **Уметь:** использовать методы администрирования подсистемы информационной безопасности объекта защиты; **Владеть:** методами администрирования подсистемы информационной безопасности объекта защиты. **ПК-4** **Знать:** 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; **Уметь:** 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; - анализировать и оценивать угрозы информационной безопасности объекта; **Владеть:** навыками работы с нормативными правовыми актами; - навыками организации и обеспечения режима секретности; - методами формирования требований по защите информации; - методами организации и управления деятельностью служб защиты информации на предприятии; - методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; **ПК-7** **Знать:** методы проведения анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; **Уметь:** применять методы проведения анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; **Владеть:** навыками проведения анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; **ПК-8** **Знать:** способы оформления рабочей технической документации; **Уметь:** оформлять рабочую техническую документацию; **Владеть:** навыками оформления рабочей технической документации; **ПК-12** **Знать:** нормативные требования по экспериментальным исследованиям системы защиты информации; **Уметь:** проводить экспериментальные исследования системы

	защиты информации; **Владеть:** навыком проведения экспериментальных исследований системы защиты информации; **ПК-13** **Знать:** нормативные требования по аттестации объектов информатизации; **Уметь:** проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; **Владеть:** способностью принимать участие в формировании, организовывать и поддержать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации; **ПК-15** **Знать:** нормативные и правовые акты, и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в обеспечении безопасности персональных данных в информационных системах; **Уметь:** нормативные и правовые акты, и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в обеспечении безопасности персональных данных в информационных системах; **Владеть:** способностью организовать технологический процесс защиты персональных данных в информационных системах в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
Трудоемкость, з.е.	3 з.е.
Форма отчетности	Зачет с оценкой – 8 семестр, Курсовая работа – 8 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Корнеев И.К. Защита информации в офисе.- Москва: ТК Велби, 2012. 2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах.- Москва: Инфра-М, 2013.
Дополнительная литература	1. Зайцев А.И. Технические средства и методы защиты информации.- Москва: Машиностроение, 2012.- 508 с. 2. Защита информации в операционных системах.- Ставрополь: СГУ, 2013.- 318 с.