Аннотация дисциплины

Наименование дисциплины	**Методы проектирования систем технической охраны объектов информатизации**
Содержание	Анализ угроз на особо важных государственных объектах. Анализ угроз согласно принятых нормативных документов от проникновения на объект или его возгорания. Автоматизация выбора состава технических средств систем физической защиты. Анализ угроз при проектировании систем технических средств охраны. Принципы и методы построения комбинированных систем охраны. Средства охранно-пожарной сигнализации и технической укрепленности объектов. Условия для наступления противоправных действий. Условия для совершения противоправных действий. Способы предотвращения нанесения возможных потерь и убытков. Экономическое обоснование целесообразности проектирования автоматизированной комплексной системы безопасности. Классификация и состав систем безопасности объектов. Предпроектное обследование объектов. Требования к технической укрепленности объектов. Стадии и этапы создания систем безопасности при проектировании объектов. Перечень документов, включаемых в состав проектной и эксплуатационной документации по системам безопасности. Нормативная документация, используемая при проектировании пожарной сигнализации. ГОСТ Р 50776-95 «Системы тревожной сигнализации». СНиП 11-01-95 «О порядке разработки, согласования, утверждения и составе проектной документации на строительство предприятий, зданий и сооружений к проекту охранной системы». Состав проектной документации согласно ГОСТ Р 21.1101-2009 «Основные требования к проектной и рабочей документации». Принципы оформления пояснительной записки. Правила оформления рабочих чертежей. Размещение аппаратных и пультовых на объекте. Условия окружающей среды в аппаратных и пультовых.
Реализуемые компетенции	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1) 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 эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11) способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13) способностью участвовать в разработке и эксплуатации подсистемы управления информационной безопасностью (ПСК-1)
Результаты освоения	**ПК-1** **Знать:** требования по установке, настройке и обслуживанию

дисциплины (модуля)	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-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-11** **Знать:** методы и средства проведения экспериментов по заданной методике, обработки, оценки погрешности и достоверности их результатов. **Уметь:** использовать методы и средства проведения экспериментов по заданной методике, обработки, оценки погрешности и достоверности их результатов. **Владеть:** навыками проведения экспериментов по заданной методике, обработки, оценки погрешности и достоверности их результатов. **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; **ПСК-1** **Знать:** способы управления подсистемами информационной безопасности, **Уметь:** применять методы разработки и эксплуатации подсистемы управления информационной безопасностью, **Владеть:** навыками применения методы разработки и эксплуатации подсистемы управления информационной безопасностью.
Трудоемкость, з.е.	3 з.е.
Форма отчетности	Зачет с оценкой – 7 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Гафнер В.В. Информационная безопасность.- Ростов на Дону: Феникс, 2012.- 324 с. 2. Хорве П.Б. Программно-аппаратная защита информации.- Москва: Форум, 2012.- 352 с.
Дополнительная литература	1. Зайцев А.П. Технические средства и методы защиты информации.- Москва: Машиностроение, 2012.- 508 с. 2. ГОСТ Р 21.1101.-2009 Система проектной документации для строительства. Основные требования к проектной и рабочей документации. 3. ГОСТ Р 50776-95 «Системы тревожной сигнализации». 4. СНиП 11-01-95 «О порядке разработки, согласования, утверждения и составе проектной документации на строительство предприятий, зданий и сооружений к проекту охраны системы».