Аннотация к рабочей программе дисциплины

Автор: Урбан В.А, доцент, канд.техн.наук
Наименование дисциплины: Б1.О.38 Защита информации от утечки по техническим каналам
Цель освоения дисциплины: заключается в формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий, развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

1. Требования к результатам освоения дисциплины:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине (модулю)**
УК-2 Способен определятькруг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Формулирует в рамках поставленной целипроекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Определяет ожидаемые результаты решения выделенных задач	*Знать:* Установку, монтаж и настройки технических средств защиты информации *Уметь:* Применять технические средства для криптографической защиты информации конфиденциального характера *Владеть:* Возможностью технического обслуживания техническихсредств защиты информации
	УК-2.2 Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	*Знать:* Номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам *Уметь:* Применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническимисредствами *Владеть:* Навыками формирования и реализации политики информационной безопасности на защищаемом объекте
	УК-2.3 Решает конкретные задач проекта заявленного качества и за установленное время	*Знать:* Принципы организации информационной безопасности автоматизированных систем в соответствии с требованиями по защите информации

		Уметь: Пользоваться нормативными документами по противодействию технической разведке *Владеть:* Методами и средствами технической защиты информации
	УК-2.4 Публично представляет результаты решения конкретной задачи проекта	*Знать:* Возможности технических средствперехвата информации *Уметь:* Анализировать и оценивать угрозы информационной безопасностиобъекта *Владеть:* Методами установки и настройки криптографических и технических средств защиты информации
ОПК-3 Способен использовать необходимые математические методыдля решения задач профессиональной деятельности	ОПК-3.1 Проводит работыпо установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам	*Знать:* Принципы устройства и функционирования средств криптографической и технической защиты информации *Уметь:* Применять технические средства для криптографической защиты информации конфиденциального характера *Владеть:* Методами установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты
	ОПК-3.2 Проводит работыпо установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа	*Знать:* Принципы организации информационной безопасности автоматизированных систем в соответствии с требованиями по защите информации *Уметь:* Производить установку и настройку программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-

		техническимидокументами *Владеть:* Методикой контроля защищенности информации от несанкционированного доступа
	ОПК-3.3 Проводит контроль эффективности защиты информации отутечки по техническимканалам	*Знать:* Технические каналы утечки информации *Уметь:* Применять технические средства для защиты информации в условиях применения устройств обработки и передачи данных *Владеть:* Применением основных типов технических средств защиты информации
	ОПК-3.4 Проводит контроль эффективности защиты информации от несанкционированного доступа	*Знать:* Устранение выявленных неисправностей программно-технических средств защиты информации от несанкционированного доступа и при необходимости организация их ремонта с привлечением производителей этих средств *Уметь:* Производить установку и настройку программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами *Владеть:* Навыками испытания программно-технических средств защиты информации от несанкционированного доступа
ОПК-4 Способен применять необходимые физические законы и модели для решения задачпрофессиональной деятельности	ОПК-4.1 Проводит организационные мероприятия по обеспечению безопасности информациив автоматизированных системах;	*Знать:* Особенности организационного сопровождения разработки, отладки, модификации и поддержки информационных технологий исистем *Уметь:* Проводить организационное сопровождение разработки, отладки, модификации и

		поддержки информационных технологий исистем *Владеть:* Навыками проведения мероприятий организационного обеспечения информационной безопасности в процессе сопровождения разработки, отладки, модификации поддержки информационных технологий и систем
	ОПК-4.2 Способен администрировать операционные системы,системы управления базами данных, вычислительные сети	*Знать:* Администрирование локальных вычислительных сетей и принимать меры по устранению возможных сбоев *Уметь:* Администрировать сетевые ресурсы в информационных системах *Владеть:* Сбором данных для анализа использования и функционирования программно-технических средств компьютерных сетей
	ОПК-4.3 Выполняет работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	*Знать:* Основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации *Уметь:* выбирать, устанавливать и настраивать аппаратные средства защиты информации от несанкционированного доступа и соответствующее программное обеспечение *Владеть:* Основными методами, способами исредствами защиты информации отнесанкционированного доступа
	ОПК-4.4 Осуществляет диагностику и мониторинг систем защиты автоматизированных систем	*Знать:* Типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа *Уметь:* Осуществлять мониторинг и

		регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствийкомпьютерных атак *Владеть:* Установкой, настройкой программных средств защиты информации в автоматизированной системе
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1 Применяет математические модели ирешает задачи криптографического преобразования при решении задач защиты информации	*Знать:* Математические методы, необходимые для решения задач защиты информации *Уметь:* Использовать типовые математические методы и модели для решения задач *Владеть:* Подходами к решению стандартныхматематических задач, выполнениюрасчетов математических величин, применению математических методов обработки экспериментальных данных
	ОПК-9.2 Определяет и анализирует технические каналы утечки информации	*Знать:* Каналы утечки информации и методы их оценки *Уметь:* Изучать и анализировать характеристики и особенности применения основных приборов и оборудования, используемых для выявления каналов утечки информации *Владеть:* Расчетом контролируемой зоны, в пределах которой могут происходить утечки информации
	ОПК-9.3 Проводит работы по установке и настройкесредств технической защиты информации	*Знать:* Основные принципы действия и характеристики технических средств физической защиты *Уметь:* Применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом

		Владеть: Навыками проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации
ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.1 Проводит испытания по оценки защищенности объектов информатизации на основесуществующих методик ФСТЭК	*Знать:* Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасностиинформации *Уметь:* Прорабатывать общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России, модели угроз безопасности информации, разрабатываемые ФСТЭК России *Владеть:* Методиками для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенныхк государственным и муниципальныминформационным системам, информационным системам персональных данных, значимым объектам критической информационной инфраструктуры Российской Федерации
	ОПК-11.2 Способен проводить экспериментыпо заданной методике, обработку, оценку погрешности и достоверности их результатов	*Знать:* Основные понятия и методы математической статистики *Уметь:* Использовать математические методы и модели для решения прикладных задач *Владеть:* Методами количественного анализа процессов обработки, поиска ипередачи информации
	ОПК-11.3 Принимаетучастие в проведении экспериментальных исследований системы защиты информации	*Знать:* Основные алгоритмы и типовые модели, используемые при решении практических задач с помощью аппарата теории вероятностей, математической

		статистики *Уметь:* Логически мыслить, подбирать формулы, соответствующие типам задач *Владеть:* Навыками использования математических моделей теории вероятностей и математической статистики

2. Содержание дисциплины:

Тема 1. Характеристика инженерно- технической защиты информации как области информационной безопасности. Основные проблемы инженерно- технической защитыинформации. Представление сил и средств защитыинформации в видесистемы

Тема 2. Системный подход к защите информации. Понятие и особенности утечки информации. Структура, классификация иосновные характеристики технических каналов утечкиинформации. Простыеи составные технические каналыутечки информации

Тема 3. Распространение сигналов в техническихканалах утечки информации Распространение акустических сигналовв атмосфере, воде и втвердой среде.Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в светопроводах. Распространение радиосигналов различных диапазонов впространстве и понаправляющим линиям связи

Тема 4. Особенностиинформации какпредмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектовнаблюдения, сигналов ивеществ

Тема 5. Моделированиеслучайных величин.Законы распределения случайных величин. Статистические оценкии их точность. Аппроксимация результатов статистического моделирования

Тема 6. Основныепонятия теории случайных процессов, их классификация и основные характеристики. Марковские процессы с дискретными состояниями Марковские процессы сдискретными состояниями и непрерывным временем Стационарные случайные процессы

Тема 7. Моделирование инженерно- технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно- технической защиты информации. Принципы моделирования объектов защиты.Моделирование угроз безопасности информации. Методические рекомендации повыбору рациональных вариантов защиты

Тема 8. Задачи защиты информации ТКС в условиях конфликта. Понятие конфликта. Способы разрешения конфликта в ТКС

Тема 9. Контроль эффективности инженерно- технической защиты информации. Виды контроляэффективности инженерно- технической защиты информации. Виды зонконтроля. Требования по защите информации от утечки по техническим каналам. Видытехнического контроля

Тема 10. Методические рекомендации пооценке эффективностизащиты информации. Способы оценкиэффективности охраныобъектов защиты. Оценка эффективности защиты видовых признаковобъектов наблюдения

Тема 11. Основные задачи, структура и характеристика государственной системы противодействия технической защите. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке.Основные организационные и технические меры позащите информации

Тема 12. Физическиеосновы защитыинформации от технических разведок. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок. Принципы действия аппаратуры технических разведок. Классификация методов и средствзащиты информации оттехнических разведок

3. Общая трудоемкость дисциплины: 3 ЗЕ