МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ Филиппович А.Ю.

"01" сентября 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Техническая защита информации»

по направлению подготовки 10.05.03

«Информационная безопасность автоматизированных систем»

Образовательная программа (профиль):

«Обеспечение информационной безопасности распределенных информационных систем»

Квалификация (степень) выпускника

Специалист

Форма обучения

Очная

Год приема – 2019

Москва 2019 г.

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Техническая защита информации» следует отнести:

- теоретическую и практическую подготовленность специалиста к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации.

К **основным задачам** освоения дисциплины «Техническая защита информации» следует отнести:

- ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;

- ознакомление с техническими каналами утечки акустической (речевой) информации;

- изучение способов и средств защиты информации, обрабатываемой техническими средствами;

- изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;

- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;

- обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

2. Место дисциплины в структуре ООП специалитета

Дисциплина «Техническая защита информации» относится к числу профессиональных учебных дисциплин базовой части цикла (Б.1.1.33) основной образовательной программы специалитета.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Математический анализ», «Теория вероятностей» и «Математическая статистика», «Электроника и схемотехника», «Основы информационной безопасности», «Физические основы информационной безопасности».

3. Перечень планируемых результатов обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ОПК-8	способностью к освоению новых образцов программных, технических средств и информационных технологий	**знать:** современные программные, технические средства и информационные технологии **уметь:** осваивать современные программные, технические средства и информационные технологии
ПК - 3	способностью проводить анализ защищенности автоматизированных систем	**знать:** нормативные и методические документы ФСТЭК по оценке защищенности АС **уметь:** организовывать проведение анализа защищенности автоматизированных систем
ПК - 13	способностью участвовать в проектировании средств защиты информации автоматизированной	**знать:** международные и российские стандарты по безопасности информации, а также специальные требования и рекомендации по защите конфиденциальной информации

	системы	**уметь:** анализировать угрозы безопасности информации и соответствующие им уязвимости на объектах информатизации предприятий, участвовать в проектировании средств защиты информации
ПК - 14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	**знать:** нормативные и методические документы ФСТЭК по контролю защищенности АС и средств вычислительной техники **уметь:** проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации с оценкой достоверности полученных результатов
ПК – 17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	**знать:** особенности функционирования автоматизированных систем с разными уровнями конфиденциальности информации и соответствующий им полный набор функций по защите информации **уметь:** формировать предложения по оптимизации процесса инструментального мониторинга защищенности информации в автоматизированной системе **владеть:** навыками инструментального мониторинга защищенности информации АС и анализа ее функционального состояния

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов. Из них 72 часа составляют аудиторные занятия (лабораторные занятия – 72 часа) и самостоятельная работа - 72 часа. Форма контроля – экзамен в 5 семестре.

Структура и содержание дисциплины «Техническая защита информации» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Тема 1. Место технической защиты информации в государственной системе защиты информации в Российской Федерации

Цели и задачи защиты информации от утечки информации по техническим каналам (технической защиты информации). Нормативные документы по технической защите информации.

Термины и определения в области технической защиты информации: объект информатизации, выделенное помещение, основные технические средства и системы, вспомогательные технические средства и системы, утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получения информации, посторонние проводники, контролируемая зона, технический канал утечки информации.

Тема 2. Технические каналы утечки акустической (речевой) информации

Характеристики речевого сигнала. Общая характеристика и классификация технических каналов утечки акустической информации. Прямые акустические каналы утечки речевой информации. Акустовибрационные каналы утечки речевой информации. Акустооптический (оптикоэлектронный, лазерный) канал утечки речевой информации. Акустоэлектрические каналы утечки речевой информации. Акустоэлектромагнитные каналы утечки речевой информации. Средства акустической разведки и их технические характеристики.

Тема 3. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений. Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ. Технический канал утечки информации создаваемый путем внедрения в СВТ электронных устройств негласного получения информации.

Тема 4. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Классификация способов и средств защиты объектов информатизации. Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств. Требования к системам электропитания и заземления основных технических средств и систем. Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по

установке). Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке). Защищённые средства вычислительной техники.

Тема 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Звукоизоляция выделенных помещений. Звукопоглощающие материалы. Системы и средства виброакустической маскировки (принципы построения, основные характеристики, требования по установке). Способы и средства защиты вспомогательных технических средств и систем. Специальные технические средства подавления электронных устройств перехвата речевой информации (широкополосные генераторы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи).

Тема 6. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам

Показатели эффективности защиты речевой информации. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции. Методика расчета словесной разборчивости речи. Методика оценки возможностей средств акустической разведки по перехвату речевой информации. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

Тема 7. Методы и средства выявления электронных устройств негласного получения информации

Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля, программно-аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгено-телевизионные комплексы. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации.

Тема 8. Организация технической защиты информации

Лицензирование деятельности по технической защите информации. Сертификация технических средств защиты информации.

Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях на различных этапах жизненного цикла объекта защиты. Порядок ввода объекта информатизации и системы технической защиты информации в эксплуатацию.

Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации. Порядок документального оформления результатов аттестационных испытаний и соответствия объекта информатизации требованиям по безопасности информации.

5. Образовательные технологии.

Методика преподавания дисциплины «Техническая защита информации» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование

следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- проведение интерактивных лекционных и практических занятий с использованием интерактивной доски;

- обсуждение и защита рефератов по темам дисциплины;

- подготовка, представление и обсуждение презентаций на семинарских занятиях.

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 40 % аудиторных занятий. Занятия лекционного типа составляют 60 % от объема аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- подготовка рефератов и их защита;

- экзамен.

Темы рефератов, контрольных вопросов и заданий для проведения текущего контроля, экзаменационных билетов приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК - 8	способностью к освоению новых образцов программных, технических средств и информационных технологий
ПК - 3	способностью проводить анализ защищенности автоматизированных систем
ПК - 13	способностью участвовать в проектировании средств защиты информации автоматизированной системы

ПК - 14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации
ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины, описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

ОПК-8 способность к освоению новых образцов программных, технических средств и информационных технологий				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: современные программные, технические средства и информационные технологии	Обучающийся демонстрирует полное отсутствие или недостаточное знание современных **о**бразцов программных, технических средств и информационных технологий	Обучающийся демонстрирует частичное знание современных **о**бразцов программных, технических средств и информационных технологий и испытывает значительные затруднения при сравнительной оценке их характеристик	Обучающийся демонстрирует полное знание **о**бразцов программных, технических средств и информационных технологий, но допускает незначительные ошибки, неточности.	Обучающийся демонстрирует полное знание **о**бразцов программных, технических средств и информационных технологий, свободно оперирует приобретенными знаниями. Допускаются незначительные неточности

уметь: осваивать современные программные, технические средства и информационные технологии	Обучающийся не умеет или в недостаточной степени умеет осваивать современные программные, технические средства и информационные технологии	Обучающийся демонстрирует частичное умение осваивать современные программные, технические средства и информационные технологии	Обучающийся демонстрирует полное умение осваивать современные программные, технические средства и информационные технологии, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное и свободное умение осваивать современные программные, технические средства и информационные технологии Допускаются незначительные неточности
ПК – 3 способность проводить анализ защищенности автоматизированных систем				
знать: виды и методы контрольных проверок эффективности применяемых мер и средств защиты информации	Обучающийся демонстрирует полное отсутствие или недостаточное знание видов и методов контрольных проверок эффективности защиты информации	Обучающийся демонстрирует частичное знание видов и методов контрольных проверок эффективности защиты информации. Испытывает затруднения при оперировании терминами и понятиями	Обучающийся демонстрирует полное знание видов и методов контрольных проверок эффективности защиты информации, но допускает незначительные ошибки, неточности	Обучающийся демонстрирует полное знание видов и методов контрольных проверок эффективности защиты информации. Свободно оперирует терминами и понятиями. Допускаются незначительные неточности
уметь: организовывать и сопровождать контроль эффективности технических средств защиты информации	Обучающийся не умеет или в недостаточной степени умеет организовывать сопровождение контроля эффективности защиты информации	Обучающийся демонстрирует частичное умение организовывать и сопровождать контроль эффективности защиты информации. Допускаются значительные ошибки,	Обучающийся демонстрирует полное умение организовывать и сопровождать контроль эффективности защиты информации. Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное умение организовывать и сопровождать контроль эффективности защиты информации. Допускаются незначительные неточности

ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы				
знать: международные и российские стандарты по безопасности информации, а также специальные требования и рекомендации по защите конфиденциальной информации	Обучающийся демонстрирует полное незнание международных и российских стандартов по безопасности информации, а также специальных требований и рекомендаций по защите конфиденциальной информации	Обучающийся демонстрирует частичное знание международных и российских стандартов по безопасности информации, а также специальных требований и рекомендаций по защите конфиденциальной информации	Обучающийся демонстрирует полное знание международных и российских стандартов по безопасности информации, а также специальных требований и рекомендаций по защите конфиденциальной информации, но допускает незначительные ошибки, неточности	Обучающийся демонстрирует полное знание международных и российских стандартов по безопасности информации, а также специальных требований и рекомендаций по защите конфиденциальной информации Допускаются незначительные неточности
уметь: анализировать угрозы безопасности информации и соответствующие им уязвимости на объектах информатизации предприятий, участвовать в проектировании средств защиты информации	Обучающийся демонстрирует полное неумение анализировать угрозы безопасности информации и соответствующие им уязвимости на объектах информатизации	Обучающийся демонстрирует частичное умение анализировать угрозы безопасности информации и соответствующие им уязвимости на объектах информатизации. Может участвовать в проектировании средств защиты информации	Обучающийся демонстрирует полное умение анализировать угрозы безопасности информации и соответствующие им уязвимости на объектах информатизации. Может участвовать в проектировании средств защиты информации, но допускает незначительные ошибки, неточности	Обучающийся демонстрирует полное умение анализировать угрозы безопасности информации и соответствующие им уязвимости на объектах информатизации. Может участвовать в проектировании средств защиты информации. Допускаются незначительные неточности

ПК-14 способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации				
знать: нормативные и методические документы ФСТЭК по контролю защищенности АС и средств вычислительной техники	Обучающийся демонстрирует полное незнание нормативных и методических документов ФСТЭК по контролю защищенности АС и средств вычислительной техники	Обучающийся демонстрирует частичное знание нормативных и методических документов ФСТЭК по контролю защищенности АС и средств вычислительной техники	Обучающийся демонстрирует полное знание нормативных и методических документов ФСТЭК по контролю защищенности АС и средств вычислительной техники, но допускает незначительные ошибки, неточности	Обучающийся демонстрирует полное знание нормативных и методических документов ФСТЭК по контролю защищенности АС и средств вычислительной техники.Допускаются незначительные неточности
уметь: проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации с оценкой достоверности полученных результатов	Обучающийся демонстрирует полное неумение проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Обучающийся демонстрирует частичное умение проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации с оценкой достоверности полученных результатов	Обучающийся демонстрирует полное умение проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации с оценкой достоверности полученных результатов, но допускает незначительные ошибки, неточности	Обучающийся демонстрирует полное умение проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации с оценкой достоверности полученных результатов Допускаются незначительные неточности
ПК-17 способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации				

знать: особенности функционирования автоматизированных систем с разными уровнями конфиденциальности информации и соответствующий им полный набор функций по защите информации	Обучающийся демонстрирует полное непонимание особенностей функционирования автоматизированных систем с разными уровнями конфиденциальности информации	Обучающийся демонстрирует частичное понимание особенностей функционирования автоматизированных систем с разными уровнями конфиденциальности информации. Имеет представление о полном наборе функций по защите информации	Обучающийся демонстрирует полное понимание особенностей функционирования автоматизированных систем с разными уровнями конфиденциальности информации. Имеет представление о полном наборе функций по защите информации, но допускает незначительные ошибки, неточности	Обучающийся демонстрирует полное понимание особенностей функционирования автоматизированных систем с разными уровнями конфиденциальности информации. Имеет представление о полном наборе функций по защите информации, допускает незначительные неточности
уметь: формировать предложения по оптимизации процесса инструментального мониторинга защищенности информации в автоматизированной системе	Обучающийся демонстрирует полное неумение формировать предложения по оптимизации процесса инструментального мониторинга защищенности информации в автоматизированной системе	Обучающийся демонстрирует частичное умение формировать предложения по оптимизации процесса инструментального мониторинга защищенности информации в автоматизированной системе	Обучающийся демонстрирует полное умение формировать предложения по оптимизации процесса инструментального мониторинга защищенности информации в автоматизированной системе, но допускает незначительные ошибки, неточности	Обучающийся демонстрирует полное умение формировать предложения по оптимизации процесса инструментального мониторинга защищенности информации в автоматизированной системе, но допускает незначительные неточности
владеть: навыками инструментального мониторинга защищенност	Обучающийся демонстрирует полное отсутствие навыков инструментального мониторинга	Обучающийся демонстрирует частичное владение навыками инструментального мониторинга	Обучающийся демонстрирует полное владение навыками инструментального мониторинга	Обучающийся демонстрирует полное владение навыками инструментальн

и информации АС и анализа ее функциональ ного состояния	защищенности информации АС и анализа ее функционального состояния	защищенности информации АС и анализа ее функционального состояния	защищенности информации АС и анализа ее функционального состояния, но допускает незначительные ошибки, неточности	ого мониторинга защищенности информации АС и анализа ее функционально го состояния, но допускает незначительные неточности

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине проводится преподавателем, ведущим занятия по дисциплине методом экспертной оценки. По итогам промежуточной аттестации по дисциплине выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.

Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонд оценочных средств представлен в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература

1. Рагозин Ю.Н. Инженерно-техническая защита информации: учебное пособие/ИЦ Санкт-Петербург, 2018 – 168 с. **(50 экз)**

2. Рагозин Ю.Н. Инженерно-техническая защита информации: лаб. практикум. - М.: МГИУ, 2008. **(49 экз.)**

3. Хорев А.А. Техническая защита информации: учеб. пособие для вузов: в 3 т Т.1: Технические каналы утечки информации. - М.: НПЦ "Аналитика", 2008. **(49 экз.)**

4. Торокин А.А. Инженерно-техническая защита информации :учеб. пособие для вузов. - М.: Гелиос АРВ, 2005 Гриф УМО **(49 экз.)**

б) дополнительная литература

в) программное обеспечение и интернет-ресурсы:

- специальное программное обеспечение СПО «СПРУТ-мини» для проверки выполнения норм эффективности защиты речевой информации от её утечки по акустическому и виброакустическому каналам;

- специальное программное обеспечение СПО «Навигатор» для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ;

- специальное программное обеспечение СПО «Крона +» для радиомониторинга защищаемых помещений;

- Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). - http://www.fstec.ru.
- Портал технического комитета по стандартизации «Защита информации». – http://tk.gost.ru/wps/portal/tk362

- Информационно-аналитический Интернет-портал ISO27000.ru. – http://www.iso27000.ru/

- Портал по безопасности. – http://www.sec.ru/.

-http://uchebnik.online/uchebnik-predprinimatelstvo/elektromagnitnyie-kanalyi-... Электромагнитные каналы утечки информации

- Научная электронная библиотека eLIBRARY.RU – http://elibrary.ru/

8. Материально-техническое обеспечение дисциплины

Для проведения занятий лекционного типа необходимо презентационное оборудование (мультимедийный проектор, ноутбук, экран) – 1 комплект.

Для проведения лабораторных (практических) занятий необходимы:

- анализатор спектра с демодуляторами с полосой частот 9КГц-3ГГц;

- интерфейс анализатора спектра с компьютером (GPIB, USB);

- набор электрических и магнитных антенн (полоса частот 9КГц-3ГГц);

- эквивалент сети;

- генераторы пространственного и линейного электромагнитного зашумления;

- генераторы акустического и виброакустического зашумления;

- программно-аппаратный комплекс «СПРУТ-мини»;

- многофункциональный поисковый прибор SN-031 «Пиранья»;

- измеритель спектра вторичных полей (детектор нелинейных переходов).

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются занятия лекционного типа, лабораторные работы и самостоятельная работа студентов с основной литературой и интернет-ресурсами.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Лабораторные работы проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков работы с программно-аппаратными

комплексами, предназначенных для профессиональной деятельности будущего специалиста по информационной безопасности автоматизированных систем..

Практическое занятие предполагает также проведение творческих дискуссий, активный обмен мнениями по рассматриваемым вопросам, заслушивание и обсуждение докладов (презентаций) по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме лабораторной работы и дать перечень литературы по теме. При проведении практического занятия преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, помогает с развертыванием и включением в работу программно-аппаратных комплексов, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на практическом занятии учитывается при определении итоговой оценки его знаний по дисциплине на экзамене.

Самостоятельная работа по дисциплине предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением практических занятий и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;

- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки специалистов **10.05.03 «Информационная безопасность автоматизированных систем».**

Программу составил: доцент, к.э.н. Рагозин Ю.Н.

Программа утверждена на заседании кафедры “Информационная безопасность”

«29» августа 2019 г., протокол № 1

Заведующий кафедрой

«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль): «Обеспечение информационной безопасности распределенных информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: научно-исследовательская; проектно-конструкторская; контрольно-аналитическая; организационно-управленческая; эксплуатационная.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Техническая защита информации»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Темы докладов (презентаций)

Экзамен

Составители: доцент к.э.н., Рагозин Ю.Н.

Москва, 2019 год

Таблица

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Техническая защита информации					
ФГОС ВО 10.05.03 «Информационная безопасность автоматизированных систем»					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценочного средств**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				
ОПК - 8	способность к освоению новых образцов программных, технических средств и информационных технологий	**знать:** современные программные, технические средства и информационные технологии **уметь:** осваивать современные программные, технические средства и информационные технологии	Лабораторные и практические занятия, самостоятельная работа	экзамен	**Базовый уровень:** Способен самостоятельно осваивать современные программные, технические средства и информационные технологии.

ПК - 3	способность проводить анализ защищенности автоматизированных систем	**знать:** нормативные и методические документы ФСТЭК по оценке защищенности АС **уметь:** организовывать проведение анализа защищенности автоматизированных систем	Лабораторные и практические занятия, самостоятельная работа	экзамен	**Базовый уровень**: способен организовывать и проводить анализ защищенности автоматизированных систем в соответствии с требованиями нормативные и методические документы ФСТЭК по оценке защищенности АС

ПК - 13	способность участвовать в проектировании средств защиты информации автоматизированной системы	**знать:** международные и российские стандарты по безопасности информации, а также специальные требования и рекомендации по защите конфиденциальной информации **уметь:** анализировать угрозы безопасности информации и соответствующие им уязвимости на объектах информатизации предприятий, участвовать в проектировании средств защиты информации	Лабораторные и практические занятия, самостоятельная работа	экзамен	**Базовый уровень:** способен принимать участие в проектировании средств защиты информации автоматизированной системы Повышенный уровень: способен самостоятельно проектировать средства защиты информации автоматизированной системы

ПК-14	способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	**знать:** нормативные и методические документы ФСТЭК по контролю защищенности АС и средств вычислительной техники **уметь:** проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации с оценкой достоверности полученных результатов	Лабораторные и практические занятия, самостоятельная работа	экзамен	**Базовый уровень**: способен самостоятельно проводить контрольные проверки работоспособности применяемых в АС программно-аппаратных, криптографических и технических средств защиты информации

ПК-16	способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	**знать:** нормативно-правовые акты и нормативно-методические документы ФСБ и ФСТЭК Российской Федерации в области безопасности информации АС **уметь:** организовывать аттестацию автоматизированных систем с учетом нормативных документов по защите информации **владеть:** навыками практической работы с приборами и аппаратурой при аттестации АС	Лабораторные и практические занятия, самостоятельная работа	экзамен	**Базовый уровень:** способен принимать участие в проведении экспериментально - исследовательских работ при аттестации автоматизированных систем

ПК-17	способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	**знать:** особенности функционирования автоматизированных систем с разными уровнями конфиденциальности информации и соответствующий им полный набор функций по защите информации **уметь:** формировать предложения по оптимизации процесса инструментального мониторинга защищенности информации в автоматизированной системе **владеть:** навыками инструментального мониторинга защищенности информации АС и анализа ее функционального состояния	Лабораторные и практические занятия, самостоятельная работа	экзамен	**Базовый уровень**: способен самостоятельно проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации

Оценочные средства для текущей аттестации

Примерные темы презентаций (докладов):

1. Современные цифровые диктофоны.
2. Типы микрофонных систем и их технические характеристики.
3. Область применения электронных стетоскопов (радиостетоскопов).
4. и их конструктивные особенности.
5. Лазерные акустические систем разведки.
6. Цифровые анализаторы спектра.
7. Векторные анализаторы сигналов.
8. Измерительные цифровые приемники.
9. Измерительные антенны, токосъемники, пробники для проведения специальных исследований средств вычислительной техники.
10. Программно-аппаратные комплексы для проведения специальных исследований СВТ на ПЭМИН.
11. Портативные шумомеры и вибромеры.
12. Аудиоанализаторы и область применения.
13. Программно-аппаратные комплексы для проведения акустических и виброакустических измерений.
14. Программно-аппаратные комплексы для выявления акустоэлектромагнитных (акустопараметрических) каналов утечки информации.
15. Программно-аппаратные комплексы для оценки защищенности вспомогательных технических средств и систем от акустоэлектрических преобразований.
16. Индикаторы электромагнитного поля.
17. Радиочастотомеры.
18. Сканирующие радиоприемники.
19. Специальные поисковые приемники ближней зоны и интерсепторы.
20. Программно-аппаратные комплексы радиомониторинга.
21. Анализаторы проводных линий.
22. **Программно-аппаратные комплексы для исследования проводных линий.**
23. Нелинейные радиолокаторы.
24. Рентгенотелевизионные комплексы.
25. Портативные металлоискатели.
26. Эндоскопы.
27. Нормативно-методические документы ФСТЭК в области технической защиты информации.

Оценочные средства для промежуточной аттестации

Экзамен

Список вопросов для экзамена по дисциплине

1. Объект информатизации (определение). Основные технические средства и системы (ОТСС).
2. Вспомогательные технические средства и системы (ВТСС). Технический канал утечки информации (определение). Схема технического канала утечки информации
3. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).

4. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений.

5. Схема технического канала утечки информации, возникающего за счет наводок побочных электромагнитных излучений.

6. Линейные и энергетические характеристики акустического поля. Основные характеристики речи и речевого сигнала. Разборчивость речи.

7. Классификация технических каналов утечки акустической (речевой) информации и способов перехвата речевой информации.

8. Средства акустической разведки: цифровые диктофоны, направленные микрофоны (классификация, характеристики, основные возможности, схема канала перехвата). Дальность перехвата речевого сигнала средством акустической разведки направленными микрофонами.

9. Схемы перехвата речевой информации по акустовибрационному каналу утечки речевой информации.

10. Основные характеристики и возможности электронных стетоскопов и радиостетоскопов.

11. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами.

12. Экранирующие материалы, их основные характеристики. Формула для расчета коэффициента экранирования для электрической и магнитной составляющей электромагнитного поля.

13. Экранированные помещения и экранированные камеры (классификация, состав, основные характеристики).

14. Основные требования к заземлению технических средств. Схемы заземлителей. Схемы заземления технических средств. Схемы измерения сопротивления заземления технических средств.

15. Основные требования к системе пространственного электромагнитного зашумления. Схема установки системы пространственного зашумления на объекте информатизации.

16. Основные требования по установке системы пространственного зашумления на объекте информатизации. Основные характеристики генераторов шума.

17. Основные требования к системе электропитания технических средств. Способы защиты цепей электропитания технических средств от утечки информации, возникающей за счет наводок побочных электромагнитных излучений.

18. Основные требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания технических средств. Основные характеристики фильтров нижних частот (ФНЧ). Схемы установки помехоподавляющих фильтров на объекте информатизации.

19. Характеристики речевого сигнала. Разборчивость речи.

20. Классификация пассивных и активных способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.

21. Средства звуко- и виброизоляции выделенных помещений. Звукоизолирующие кабины. Специальные защищенные помещения.

22. Порядок проведения контроля эффективности защиты ВТСС. Состав и основные требования к аппаратуре контроля при контроле ВТСС на подверженность акустоэлектрическим преобразованиям.

23. Схема измерительной установки при контроле ВТСС на подверженность акустоэлектрическим преобразованиям. Порядок проведения проверки ВТСС на подверженность акустоэлектрическим преобразованиям.

24. Состав и основные требования к аппаратуре контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН

25. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.

26. Сканирующие приемники (принцип работы, основные характеристики). Этапы выявления радиозакладок.

27. Методы обнаружения, идентификации радиозакладных устройств и определения их местоположения.

28. Порядок организации защиты информации на объектах информатизации.

29. Предварительное специальное обследование объекта информатизации.

30. Аналитическое обоснование необходимости создания СТЗИ объекта (содержание, порядок проведения).

31. Замысел создания СТЗИ. Техническое задание на разработку СТЗИ объекта информатизации.

32. Организация аттестации объекта информатизации по требованиям безопасности информации.

33. Перечень документов, предоставляемых Заявителем для проведения аттестации объекта информатизации.

34. Порядок проведения аттестации объекта информатизации по требованиям безопасности информации.

35. Заключение по результатам аттестационной проверки объекта информатизации.

36. Аттестат соответствия объекта информатизации требованиям безопасности информации..

Пример билета.

1. Акустоэлектромагнитный канал утечки речевой информации

2. Организация аттестации объекта информатизации по требованиям безопасности информации. Перечень документов, предоставляемых Заявителем для проведения аттестации объекта информатизации.

3. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений.

Структура и содержание дисциплины «Техническая защита информации»

по направлению подготовки

10.05.03 «Информационная безопасность автоматизированных систем»

(специалист)

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
1.1	Цели и задачи защиты информации от утечки информации по техническим каналам (технической защиты информации). Нормативные документы по технической защите информации. Термины и определения в области технической защиты информации: объект информатизации, выделенное помещение, основные технические средства и системы, вспомогательные технические средства и системы, утечка	5	1			4	4								

	по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получения информации, посторонние проводники, контролируемая зона, технический канал утечки информации. Место технической защиты информации в государственной системе защиты информации в Российской Федерации														
1.2	Характеристики речевого сигнала. Общая характеристика и классификация технических каналов утечки акустической информации. Прямые акустические каналы утечки речевой информации. Акустовибрационные каналы утечки речевой информации. Акустооптический (оптикоэлектронный, лазерный) канал утечки речевой информации. Акустоэлектрические каналы утечки речевой информации. Акустоэлектромагнитные каналы утечки речевой информации. Средства акустической разведки и их технические характеристики.	5	2-3			8	8					+			

1.3.	Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений. Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ. Технический канал утечки информации создаваемый путем внедрения в СВТ электронных устройств негласного получения информации.	5	4-6			12	12					+			
1.4	Классификация способов и средств защиты объектов информатизации. Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств. Требования к системам электропитания и заземления основных технических	5	7-9			12	12					+			

	средств и систем. Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке). Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке). Защищённые средства вычислительной техники.														
1.5	Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Звукоизоляция выделенных помещений. Звукопоглощающие материалы. Системы и средства виброакустической маскировки (принципы построения, основные характеристики, требования по установке). Способы и средства защиты вспомогательных технических средств и систем. Специальные технические средства подавления электронных устройств перехвата речевой информации (широкополосные генераторы шума, блокираторы средств	5	10-12			12	12		-			+			

	сотовой связи, активные средства защиты телефонных линий связи).														
1.6	Показатели эффективности защиты речевой информации. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции. Методика расчета словесной разборчивости речи. Методика оценки возможностей средств акустической разведки по перехвату речевой информации. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.	5	13-14			8	8					+			
1.7	Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля, программно-	5	15-17			12	12					+			

	аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгено-телевизионные комплексы. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации.														
1.8	Лицензирование деятельности по технической защите информации. Сертификация технических средств защиты информации. Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях на различных этапах жизненного цикла объекта защиты. Порядок ввода объекта информатизации и системы технической защиты информации в эксплуатацию. Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации. Порядок документального оформления результатов аттестационных испытаний и соответствия объекта информатизации требованиям по безопасности	5	18			4	4					+			

	информации.														
	Форма аттестации													Э	
	Всего часов по дисциплине					**72**	**72**								