МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ
Директор института энергетики, информационных технологий и управляющих систем
_____ Белоусов А.В.
«20» 09 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Защита информации от утечки по техническим каналам

направление подготовки:

10.05.03 Информационная безопасность автоматизированных систем

Специализация программы:

Безопасность открытых информационных систем

Квалификация

Специалист по защите информации

Форма обучения

очная

Институт энергетики, информационных технологий и управляющих систем

Кафедра Программного обеспечения вычислительной техники и автоматизированных систем

Белгород 2021

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки России от 26.11.2020 №1457
- учебного плана, утвержденного ученым советом БГТУ им. В.Г. Шухова в 2021 году.

Составитель: к.т.н., доцент _____ (Гаврющенко А.П.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа обсуждена на заседании кафедры

«14» 05 2021 г., протокол № 8

Заведующий кафедрой: к.т.н., доцент _____ (Поляков В.М.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой программного обеспечения вычислительной техники и автоматизированных систем
(наименование кафедры/кафедр)

об Заведующий кафедрой: к.т.н., доцент _____ (Поляков В.М.)
(ученая степень и звание, подпись) (инициалы, фамилия)

«14» 05 2021 г.

Рабочая программа одобрена методической комиссией института

«20» 05 2021 г., протокол № 9

Председатель к.т.н., доцент _____ (Семернин А.Н.)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания результата обучения по дисциплине
Общепрофессиональные компетенции	ОПК 6. Способен при решении профессиональных задач организовать защиту информации ограниченного доступа в АС в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ и ФСТЭК	ОПК 6.2. Решает профессиональные задачи по защите информации ограниченного доступа в автоматизированных системах в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знать:** - методы контроля эффективности ЗИ от утечки по ТКУИ; - основные меры по ЗИ в АС; **Уметь:** - регистрировать события, связанные с ЗИ в АС; - анализировать события, связанные с ЗИ в АС; **Владеть:** - выполнением установленных процедур обеспечения безопасности информации с учетом требований эффективного функционирования АС; - оценкой последствий от реализации угроз ИБ в АС.
Общепрофессиональные компетенции	ОПК-13 Способен организовать и проводить диагностику и тестирование систем Защиты информации АС, проводить анализ уязвимостей систем ЗИ АС	ОПК-13.1 Организует и проводит диагностику и тестирование систем защиты информации автоматизированных систем	**Знать:** технические средства контроля эффективности мер ЗИ; - организационные меры по ЗИ **Уметь:** - контролировать функционирование технических средств ЗИ; - применять действующую нормативную базу в области обеспечения безопасности информации **Владеть:** - выявлением основных угроз безопасности информации АС; - подбором инструментальных средств тестирования систем ЗИ АС
		ОПК-13.2 Проводит анализ уязвимостей систем защиты информации автоматизированных систем	**Знать:** - методы и технологии проектирования, моделирования, исследования систем защиты информации АС; - руководящие и методические документы уполномоченных органов по ЗИ - принципы и методы построения средств ЗИ от НСД и утечки по ТКУИ **Уметь:** - разрабатывать модели угроз безопасности и нарушителей в АС; - классифицировать и оценивать угрозы безопасности информации для АС **Владеть:** - разработкой аналитических и компьютерных моделей угроз ИБ ; - разработкой модели угроз безопасности ИБ и нарушителей в АС

Общепрофес-сиональные компетенции	ОПК 15. Способен осуществлять администрирование и контроль функционирования средств и систем ЗИ АС, инструментальный мониторинг защищенности АС	ОПК 15.3. Осуществляет инструментальный мониторинг защищенности АС	**Знать:** -методы ЗИ от утечки по ТКУИ; - организационные меры по ЗИ; **Уметь:** - применять технические средства контроля эффективности мер ЗИ; - контролировать события безопасности и действия пользователей АС; **Владеть:** - выявлением угроз Безопасности информации в АС; - принятием мер ЗИ при выявлении новых угроз безопасности информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1. Компетенция ОПК-6. Способен при решении профессиональных задач организовать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Организационное и правовое обеспечение информационной безопасности
2.	Защита информации от утечки по техническим каналам
3.	Подготовка к процедуре защиты и защита выпускной квалификационной работы

2. Компетенция ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Защита информации от утечки по техническим каналам
2.	Программно-аппаратные средства защиты информации
3.	Моделирование угроз информационной безопасности
4.	Информационная безопасность открытых информационных систем
5.	Подготовка к процедуре защиты и защита выпускной квалификационной работы

2. Компетенция ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Защита информации от утечки по техническим каналам
2.	Программно-аппаратные средства защиты информации
3.	Администрирование информационных систем и служб
4.	Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. ОБЪЁМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зач. единиц, 180 часов.

Вид учебной работы	Всего часов	Семестр № 7
Общая трудоемкость дисциплины, час	180	180
Контактная работа (аудиторные занятия), в т.ч.:	90	90
лекции	34	34
лабораторные	34	34
практические	17	17
групповые консультации в период теоретического обучения и промежуточной аттестации	5	5
контроль самостоятельной работы	-	-
Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:	90	90
Курсовой проект	-	-
Курсовая работа	-	-
Расчетно-графическое задания	-	-
Индивидуальное домашнее задание	18	18
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)	36	36
Экзамен	36	36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Наименование тем, их содержание и объем

Курс 4 Семестр № 7

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1.	Технические каналы утечки информации, обрабатываемой СВТ				

	Вводная лекция. Цели и задачи защиты информации от утечки информации по техническим каналам. Термины и определения в области защиты информации от утечки по техническим каналам: объект информатизации, выделенное помещение, ОТСС, ВТСС, посторонние проводники, контролируемая зона, утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получения информации, технический канал утечки информации. Цели и задачи защиты информации от утечки информации по техническим каналам. Содержание и порядок изучения дисциплины. Электромагнитные технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ). Классификация технических каналов утечки информации, обрабатываемой СВТ. Причины возникновения побочных электромагнитных излучений (ПЭМИ) СВТ. Принципы построения средств перехвата ПЭМИ СВТ. Опасная зона R2. Схема технического канала утечки информации, возникающего за счет ПЭМИ СВТ. Электрические и специально создаваемые технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ). Причины возникновения электрических технических каналов утечки информации, обрабатываемой СВТ. Случайные антенны. Причины возникновения наводок информативных сигналов в случайных антеннах. Опасная зон r1. Схема технического канала утечки информации, возникающего за счет наводок ПЭМИ СВТ в случайных антеннах. Причины возникновения наводок информативных сигналов в линиях электропитания и цепях заземления СВТ. Схемы технических каналов утечки информации, возникающих за счет наводок ПЭМИ СВТ в линиях электропитания и цепях заземления СВТ. Схема перехвата информации путем «высокочастотного облучения» СВТ. Принципы построения аппаратуры «высокочастотного облучения». Схема перехвата информации путем внедряемых в СВТ электронных устройств перехвата информации. Основные виды электронных устройств перехвата информации, внедряемых в СВТ.	4	3	2	5
2.	Технические каналы утечки акустической (речевой) информации				
	Характеристики речи. Классификация технических каналов утечки акустической (речевой) информации. Акустические сигналы. Линейные и энергетические характеристики акустического поля. Характеристики речи (семантические, фонетические, физические). Спектр и типовые уровни речевого сигнала. Разборчивость речи. Методы оценки разборчивости речи. Общая характеристика и классификация технических каналов утечки акустической (речевой) информации	4	2	4	4

	Прямые акустические каналы утечки речевой информации. Схемы перехвата информации по прямым акустическим каналам утечки информации. Средства акустической разведки с датчиками микрофонного типа: цифровые диктофоны, электронные устройства перехвата речевой информации, направленные микрофоны. Акустовибрационные, акустооптический, акустоэлектрические и акустоэлектромагнитные каналы утечки речевой информации. Схемы перехвата речевой информации по акустовибрационным каналам. Электронные стетоскопы. Радиостетосскопы. Схема перехвата речевой информации по акустооптическому каналу. Лазерные акустические системы разведки. Причины возникновения акустоэлектрических каналов утечки речевой информации. Акустоэлектрические преобразователи генераторного типа. Акустоэлектрические преобразователи модуляторного типа. Схема пассивного акустоэлектрического канала утечки речевой информации. Схема активного акустоэлектрического канала утечки речевой информации.				
3.	Способы и средства защиты объектов информатизации от утечки информации по техническим каналам				
	Классификация способов и средств защиты объектов информатизации от утечки информации по техническим каналам. Пассивные способы и средства защиты объектов информатизации от утечки информации по техническим каналам. Активные способы и средства защиты объектов информатизации от утечки информации по техническим каналам. Защищенные ПЭВМ. Экранирование и заземление технических средств. Экранирование технических средств их соединительных линий. Экранирующие материалы. Экранированные помещения (экранированные камеры). Заземление технических средств. Требования к заземлению ОТСС. Схемы заземления ОТСС. Методы и средства измерения сопротивления заземления ОТСС. Системы пространственного электромагнитного зашумления. Требования к системе пространственного электромагнитного зашумления. Принципы построения широкополосных генераторов шума. Системы пространственного электромагнитного зашумления типа А (состав, основные характеристики, требования по установке). Особенности зашумления инженерных коммуникаций. Способы и средства защиты объектов информатизации от утечки информации по цепям электропитания и заземления. Требования к системе электропитания ОТСС. Требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания СВТ. Принципы построения, основные характеристики и требования по установке помехоподавляющих фильтров. Системы линейного электромагнитного зашумления типа	4	2	4	5

	Б (состав, основные характеристики, требования по установке).				
4.	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. Пассивные способы защиты выделенных помещений от утечки речевой информации по техническим каналам. Активные способы защиты выделенных помещений от утечки речевой информации по техническим каналам. Звуко- и виброизоляция выделенных помещений, глушители шума. Звукопоглощающие материалы. Специальные защищенные помещения. Системы и средства виброакустической маскировки. Требования к системе виброакустической маскировки. Принципы построения низкочастотных генераторов шума. Принципы построения акустических излучателей и виброизлучателей. Системы виброакустической маскировки типа А. Системы виброакустической маскировки типа Б. Особенности установки акустических излучателей и виброизлучателей. Специальная аппаратура для ведения конфиденциальных переговоров. Средства защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам. Пассивные способы защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам (ограничение сигналов малой амплитуды, фильтрация высокочастотных сигналов навязывания, отключение акустоэлектрических преобразователей опасных сигналов). Активные способы защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам. Принципы построения и основные характеристики средств защиты ВТСС, основанных на использовании ограничителей малой амплитуды и фильтров нижних частот. Принципы построения основные характеристики средств защиты ВТСС, основанных на отключении акустоэлектрических преобразователей. Принципы построения основные характеристики средств защиты ВТСС, основанных на использовании низкочастотных генераторов шума. Специальные технические средства подавления электронных устройств перехвата речевой информации. Принципы построения и основные характеристики подавителей диктофонов. Принципы построения и основные характеристики широкополосных генераторы шума. Принципы построения и основные характеристики блокираторов средств сотовой связи.	6	2	8	6
5.	Методы и средства контроля защищенности информации, обрабатываемой СВТ				
	Методы и средства контроля эффективности защиты информации, обрабатываемой СВТ: Показатели эффективности защиты информации, обрабатываемой СВТ, от утечки по техническим каналам. Методы контроля	2	2	4	4

	эффективности защиты информации, обрабатываемой СВТ. Требования к средствам измерения ПЭМИН СВТ и условиям проведения измерений. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН: Порядок проведения аттестационных испытаний СВТ при контроле эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИ. Порядок проведения аттестационных испытаний СВТ при контроле эффективности защиты СВТ от утечки информации, возникающей за счет наводок информативных сигналов на токопроводящие коммуникации.				
6. Методы и средства контроля защищенности речевой информации от утечки по техническим каналам					
	Методы и средства контроля выполнения норм защищенности речевой информации от утечки по техническим каналам: Показатели защищенности речевой информации от утечки речевой информации по техническим каналам. Методы контроля эффективности защиты ВП от утечки речевой информации по техническим каналам. Требования к средствам измерения при контроле выполнения норм защищенности речевой информации от утечки по прямым акустическим, акустовибрационным и акустооптическому каналам. Требования к средствам измерения при контроле выполнения норм защищенности речевой информации от утечки по акустоэлектрическим каналам. Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по техническим каналам: Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по прямым акустическим каналам. Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по акустовибрационным и акустооптическому каналам. Порядок проведения контроля ВТСС на подверженность акустоэлектрическим преобразованиям. Порядок проведения контроля ВТСС на подверженность «высокочастотному навязыванию».	2	2	8	4
7. Методы и средства выявления электронных устройств перехвата информации					
	Классификация методов поиска электронных устройств перехвата информации: Демаскирующие признаки электронных устройств перехвата информации. Классификация методов и средств поиска электронных устройств перехвата информации. Порядок специального обследования ВП на наличие возможно внедренных закладочных устройств. Методы и средства поиска электронных устройств перехвата информации средствами индикаторного типа: Методы и средства выявления скрытых систем	6	2	-	4

	видеонаблюдения. Методы выявления закладочных устройств с использованием ИЭМП. Методы выявления закладочных устройств с использованием нелинейных локаторов и рентгено-телевизионных комплексов. Методы выявления закладочных устройств с использованием сканирующих приемников и программно-аппаратных комплексов контроля. Методы выявления закладочных устройств с использованием сканирующих приемников и программно-аппаратных комплексов радиоконтроля. Сканирующие приемники и интерсепторы (основные характеристики). Программно-аппаратные комплексы радиоконтроля (состав, основные характеристики). Методы и средства выявления закладочных устройств, подключаемым к проводным коммуникациям. Программно-аппаратные комплексы анализа проводных коммуникаций (состав, основные характеристики).				
8. Организация защиты информации от утечки по техническим каналам на объектах информатизации					
	Организация защиты информации от утечки по техническим каналам: Порядок организации защиты информации от утечки по техническим каналам. Содержание технического задания на создание системы защиты информации от утечки по техническим каналам (СЗИУТК). Содержание технического проекта СЗИУТК. Порядок ввода в эксплуатацию объекта информатизации и СЗИУТК. Аналитическое обоснование необходимости создания СЗИУТК. Предпроектное специальное обследование объекта информатизации. Обоснование состава СЗИУТК. Организация аттестации объектов информатизации: Порядок организации аттестации объекта информатизации по требованиям безопасности информации. Подготовка к проведению аттестации объекта информатизации. Программа и методика аттестационных испытаний объекта информатизации Порядок проведения аттестации объекта информатизации	6	2	4	4
	ВСЕГО	34	17	34	36

4.2. Содержание практических (семинарских) занятий

№ п/п	Наименование раздела дисциплины	Тема практического занятия	К-во часов	К-во часов СРС
семестр № 7				
1	Технические каналы утечки информации, обрабатываемой СВТ.	Электромагнитные технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ). Классификация технических каналов утечки информации, обрабатываемой СВТ. Электрические и специально создаваемые технические	3	1

		каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ). Причины возникновения электрических технических каналов утечки информации, обрабатываемой СВТ. Схема перехвата информации путем «высокочастотного облучения» СВТ. Принципы построения аппаратуры «высокочастотного облучения».		
2	Технические каналы утечки акустической (речевой) информации.	Характеристики речи (семантические, фонетические, физические). Спектр и типовые уровни речевого сигнала. Разборчивость речи. Схемы перехвата информации по прямым акустическим каналам утечки информации. Акустовибрационные, акустооптический, акустоэлектрические и акустоэлектромагнитные каналы утечки речевой информации. Схемы перехвата речевой информации по акустовибрационным каналам.	2	1
3	Способы и средства защиты объектов информатизации от утечки информации по техническим каналам.	Пассивные способы и средства защиты объектов информатизации от утечки информации по техническим каналам. Активные способы и средства защиты объектов информатизации от утечки информации по техническим каналам. Способы и средства защиты объектов информатизации от утечки информации по цепям электропитания и заземления.	2	1
4	Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.	Пассивные способы защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам (ограничение сигналов малой амплитуды, фильтрация высокочастотных сигналов навязывания, отключение акустоэлектрических преобразователей опасных сигналов). Активные способы защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам.	2	1
5	Методы и средства контроля защищенности информации, обрабатываемой СВТ.	Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН	2	1
6	Методы и средства контроля защищенности речевой информации от утечки по техническим каналам	Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по техническим каналам	2	1

7	Методы и средства выявления электронных устройств перехвата информации	Методы и средства выявления закладочных устройств, подключаемым к проводным коммуникациям.	2	1
8	Организация защиты информации от утечки по техническим каналам на объектах информатизации	Порядок организации аттестации объекта информатизации по требованиям безопасности информации.	2	1
		ИТОГО:	17	8
			ВСЕГО:	25

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
семестр № 7				
1	Тема 1. Технические каналы утечки информации, обрабатываемой СВТ	Оценка возможностей по перехвату ПЭМИ СВТ средствами разведки. Расчет опасной зоны R2. Расчет опасной зоны r1.	2	2
2	Тема 2. Технические каналы утечки акустической (речевой) информации	Оценка возможностей по перехвату речевой информации средства акустической разведки. Оценка возможности непреднамеренного прослушивания речи. Оценка возможности перехвата речевой информации направленными микрофонами.	2	1
		Исследование акустоэлектрических каналов утечки информации Исследование пассивного акустоэлектрического канала утечки информации Исследование канала утечки информации, создаваемого методом «высокочастотного навязывания»	2	1
3	Тема 3. Способы и средства защиты объектов информатизации от утечки информации по техническим каналам	Исследование характеристик систем пространственного электромагнитного зашумления. Исследование характеристик генератора шума системы пространственного электромагнитного зашумления. Расчет напряженности поля помехового сигнала, создаваемого системой пространственного электромагнитного зашумления	2	2
		Исследование характеристик помехоподавляющих фильтров Исследование характеристик помехоподавляющего фильтра ФП-8. Исследование характеристик помехоподавляющего фильтра ФСП-1Ф10А.	2	1
4	Тема 4. Способы и средства защиты	Исследование характеристик систем виброакустической защиты. Исследование характеристик генератора низкочастотного шума	2	1

	выделенных помещений от утечки речевой информации по техническим каналам	системы виброакустической защиты. Расчет звукового давления, создаваемого акустической колонкой системы виброакустической защиты. Оценка возможности непреднамеренного прослушивания речи при использовании системы виброакустической защиты.		
		Изучение возможностей, принципов и тактики работы специальных комплексов и приборов комплексного контроля:		
		-ST 031 «Пиранья-1»	2	1
		- ST 131 «Пиранья-2»	2	1
		- нелинейного локатора «Обь»	2	1
5	Тема 5. Методы и средства контроля защищенности информации, обрабатываемой СВТ	Оценка выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИН: Оценка выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИ при использовании системы пространственного электромагнитного зашумления. Оценка выполнения норм защищенности СВТ от утечки информации, возникающей за счет наводок ПЭМИ в линиях электропитания и в токопроводящих коммуникациях при использовании системы линейного электромагнитного зашумления.	4	2
6	Тема 6. Методы и средства контроля защищенности речевой информации от утечки по техническим каналам	Оценка выполнения норм защищенности речевой информации от утечки по техническим каналам: Оценка выполнения норм защищенности речевой информации от утечки по прямым акустическим каналам. Оценка выполнения норм защищенности речевой информации от утечки по акустовибрационным и акустооптическому каналам.	4	2
		Порядок и правила проведения специальных поисковых исследований и особенности их реализации	4	2
7	Тема 8. Организация защиты информации от утечки по техническим каналам на объектах информатизации	Предпроектное специальное обследование объекта информатизации Предпроектное специальное обследование объекта информатизации Предпроектное специальное обследование выделенного помещения	2	2
		Разработка программы и методики аттестационных испытаний объекта информатизации Разработка методики аттестационных испытаний объекта информатизации. Разработка методики аттестационных испытаний выделенного помещения.	2	1
		ИТОГО:	34	20
			ВСЕГО:	54

4.4. Содержание курсового проекта/работы

Не предусмотрено учебным планом

4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий

Выполнение практико-ориентированного индивидуального домашнего задания № 1 по темам:

1. Цели специальных поисковых работ и особенности их реализации
2. Поисковые исследования, проводимые при базовой мотивации – «утеря конкретных конфиденциальных материалов», их особенности и реализация
3. Поисковые исследования, проводимые при базовой мотивации – «проявление заинтересованности со стороны конкурирующей организации к определенным конфиденциальным материалам или к коммерческой деятельности в целом», их особенности и реализация
4. Поисковые исследования, проводимые при базовой мотивации – «предупреждающие профилактические действия», их особенности и реализация
5. Обеспечение конспирации и легендирования поисковых работ на всех этапах их осуществления, предлагаемые мероприятия, порядок их оформления и утверждения
6. Изучение объекта поиска и его окружения, уточнение технических и профессиональных возможностей источника угроз, анализ режимных процедур на объекте, планирование технических и информационных процедур на объекте поиска для подготовки плана поисковых исследований
7. Разработка плана поисковых исследований и подготовка к их проведению, содержание работ на каждом этапе, моделирование возможных вариантов их выполнения, перечень используемой поисковой техники на каждом из этапов, планирование линии поведения каждого участника поисковой бригады
8. Осмотр и проверка предметов быта и интерьера, находящихся на объекте поиска, визуальный осмотр – от общего к частному, используемая поисковая техника, методики проверки
9. Поиск устройств съема информации, внедренных в электронные приборы. Перечень используемой поисковой техники, алгоритм поиска, оформление результатов
10. Исследование электромагнитной обстановки в помещениях, автомашинах и на открытой местности, моделирование возможных каналов утечки информации по каждом из перечисленных вариантов, перечень поисковой техники, определение возможных мест размещения пунктов приема и контроля, порядок их выявления, оформление результатов проведенных работ
11. Поиск устройств съема информации в проводных коммуникациях, особенности проведения поисковых работ по проверке электрической сети, абонентской и офисной телефонной сети, радиотрансляционной сети, сетей охранной и пожарной сигнализации
12. Обследование элементов строительных конструкций, обследование оградительных элементов строительных конструкций, обследование окон, вентиляционных каналов, водопроводных и теплопроводных коммуникаций, выработка рекомендаций по защите информации
13. Подведение итогов поисковых исследований, описание проведенных поисковых исследований, оформление акта проведения исследований, предложения по нейтрализации возможных каналов утечки
14. Обзор представленных на рынке современных технических средств поиска каналов утечки информации
15. Обзор представленных на рынке современных технических средств защиты информации, контроля и блокировки сетей передачи информации, определения местоположения источников излучения, ложных станций сотовой связи.

Выполнение практико-ориентированного индивидуального домашнего задания № 2 по темам:

Тема домашнего задания № 2 «Анализ потенциальных технических каналов утечки информации на объекте информатизации организации».

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1. Реализация компетенций

1. Компетенция ОПК 6. Способен при решении профессиональных задач организовать защиту информации ограниченного доступа в АС в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ и ФСТЭК

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК 6.2. Решает профессиональные задачи по защите информации ограниченного доступа в АС в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ и ФСТЭК	устный опрос, индивидуальное домашнее задание, экзамен

2. Компетенция ОПК-13 Способен организовать и проводить диагностику и тестирование систем Защиты информации АС, проводить анализ уязвимостей систем ЗИ АС

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-13.1 Организует и проводит диагностику и тестирование систем ЗИ АС	устный опрос, экзамен
ОПК-13.2 Проводит анализ уязвимостей систем ЗИ АС	устный опрос, экзамен

3. Компетенция ОПК 15. Способен осуществлять администрирование и контроль функционирования средств и систем ЗИ АС, инструментальный мониторинг защищенности АС

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК 15.3. Осуществляет инструментальный мониторинг защищенности АС	устный опрос, индивидуальное домашнее задание, экзамен

5.2. Типовые контрольные задания для промежуточной аттестации

5.2.1. Перечень контрольных вопросов (типовых заданий) для экзамена

№ п/п	Наименование вопросов
1.	Объекты защиты информации.

2.	Основные технические средства приёма, обработки и хранения информации (ОТСС).
3.	Вспомогательные технические средства и системы (ВТСС).
4.	Дайте определение контролируемой зоне.
5.	Объясните физическую сущность возникновения побочных электромагнитных излучений и наводок (ПЭМИН).
6.	Потенциально возможные технические каналы утечки информации.
7.	Технические каналы утечки речевой информации.
8.	Как реализуется метод высокочастотного навязывания.
9.	Каковы основные акустические параметры речевых сигналов.
10.	Электромагнитные каналы утечки информации.
11.	Какие элементы строительных конструкций наиболее опасны с точки зрения несанкционированного съема информации
12.	Виды средств обнаружения радиозакладочных устройств.
13.	Типовой состав автоматизированных комплексов радиомониторинга.
14.	Принцип действия и назначение нелинейного локатора. Типы нелинейных локаторов.
15.	Особенности канала утечки речевой информации за счет акустоэлектрических преобразований.
16.	На чем основывается реализация лазерного канала утечки информации
17.	Основные задачи, решаемые физическими средствами защиты.
18.	Состав системы обеспечения безопасности объектов.
19.	Пассивные и активные методы технической защиты объектов
20.	Сущность контроля эффективности защиты информации.
21.	Нормы эффективности защиты информации.
22.	Метод контроля эффективности защиты информации.
23.	Виды контроля защищенности объектов от разведки по ПЭМИН.
24.	Порядок инструментального контроля ПЭМИН.
25.	Какие возможные технические каналы утечки учитываются при оценке мероприятий по информационной защите помещений
26.	Что понимают под аттестацией объектов информатизации
27.	С какой целью проводятся специальные исследования объектов
28.	Что представляют собой специальные проверки объекта защиты

5.3. Типовые контрольные задания (материалы) для текущего контроля в семестре

Текущий контроль осуществляется в течение семестра в форме собеседования и устного опроса, а также в ходе выполнения Индивидуальных домашних заданий.

Собеседования и устные опросы направлены на проверку степени усвоения материала и понимания теоретических сведений, используемых в процессе выполнения работы.

Перечень тестовых вопросов для промежуточного контроля результатов достижения индикаторов компетенции:

1. Что такое технический канал утечки информации:
   - Физический путь утечки информации
   - Утечка информации через технические средства
   - Несанкционированное получение охраняемых сведений с использованием технических средств
   - Физический путь от источника информации к злоумышленнику, по которому возможна утечка или несанкционированное получение сведений

2. Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими субъектами:
   - конфиденциальная информация
   - банковская тайна
   - коммерческая тайна
   - служебная информация

3. Каналы утечки информации можно разделить на следующие группы (с учетом физической природы образования):
   - Акустические
   - Разговорные
   - Стеганографические
   - Криптографические
   - Визуально-оптические
   - Электромагнитные
   - Магнито-электрические
   - Материально-вещественные
   - Радиологические

4. Какими бывают технические каналы утечки информации:
   - Акустическими
   - Физическими
   - Вещественными
   - Криптографическими
   - Визуально-оптическими
   - Электромагнитными
   - Материально-вещественными

5. По какому признаку можно классифицировать визуально-оптические ТКУИ:
   - по используемым средствам поиска и контроля

- по среде распространения
- по сложности обнаружения
- по диапазону излучения
- по природе образования

6. Акустические каналы утечки информации образуются:
   - за счет распространения звуковых колебаний в свободном воздушном пространстве
   - за счет воздействия звуковых колебаний на системы защиты информации
   - за счет воздействия звуковых колебаний на элементы и конструкции зданий
   - за счет воздействия звуковых колебаний на технические средства и системы
   - за счет воздействия звуковых колебаний на дистанционные средства съема информации

7. Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми, - это:
   - принцип системности
   - принцип комплексности
   - принцип непрерывности
   - принцип разумной достаточности
   - принцип гибкости системы

8. По какому признаку можно классифицировать электромагнитные ТКУИ:
   - по природе образования
   - по сложности обнаружения
   - по диапазону излучения
   - по используемым средствам поиска и регистрации
   - по среде распространения

9. По какому признаку можно классифицировать материально-вещественные ТКУИ:
   - по физическому состоянию
   - по используемым средствам поиска и контроля
   - по физической природе
   - по среде распространения

10. Источники электромагнитных каналов утечки информации:
    - акусто-электрические преобразователи информации
    - визуально-оптические преобразователи информации
    - излучатели электромагнитных сигналов
    - активные приемники сигналов
    - паразитные связи и наводки

11. Каковы причины и условия возникновения каналов ТКУИ за счет Побочных ЭлектроМагнитных Излучений и Наводок (ПЭМИН):
    - несовершенство схемных решений – конструктивные
    - несовершенство схемных решений – технологические
    - эксплуатационный износ элементов – изменения параметров
    - эксплуатационный износ элементов - аварийный выход из строя
    - изменения условий эксплуатации

12. Дайте определение :

- Риск – это способ определения сильных и слабых сторон существующих и предлагаемых мер защиты.
- Риск – это определение мероприятий по оценке угроз и разработке новых, более эффективных методов и средств защиты от них.
- Риск - это стоимостное выражение вероятностного события, ведущего к потерям.
- Риск - это процесс получения количественной или качественной оценки ущерба, который может произойти в случае реализации угрозы безопасности ИС.

13. Дайте определение показателя эффективности системы защиты информации

- Сравнительная характеристика системы защиты информации и возможностей нарушителя по ее преодолению.
- Совокупность свойств, определяющих степень ее приспособленности к выполнению поставленных перед нею задач. В некоторых работах указанная совокупность свойств названа термином "качество".
- Ее влияние на достижение (при прочих равных условиях) конечных целей функционирования системы обработки информации или на степень использования потенциальных боевых возможностей группировки войск в данной конкретной обстановке.
- Численная мера, количественно характеризующая степень выполнения системой защиты целей своего функционирования.

14. Чем объяснима необходимость криптографии информации, курсирующей в вычислительной сети?

- Сложность управления и контроля доступа к системе.
- Разделение совместно используемых ресурсов.
- Данные IP, и TCP-протокола полностью прозрачны для злоумышленника.
- Множество точек атаки.

15. Проранжируйте роли по возрастанию риска информационной безопасности

- - пользователь сети, - менеджер программного обеспечения, - оператор системы, администратор баз данных, - администратор безопасности.
- - пользователь сети, - администратор баз данных, - менеджер программного обеспечения,- оператор системы, - администратор безопасности.
- - администратор безопасности, - оператор системы, - менеджер программного обеспечения, - администратор баз данных, - пользователь сети.
- - оператор системы, - менеджер программного обеспечения, - администратор безопасности, - пользователь сети, администратор баз данных.

16. Проранжируйте компоненты ИС по возрастанию риска информационной безопасности

- 1.
  - - сотрудники — пользователи и обслуживающий персонал.
  - - данные — временные, хранимые постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
  - - оборудование — ЭВМ и их составные части (процессоры, мониторы, терминалы, рабочие станции), периферийные устройства (дисководы,

устройства back-up, порты ввода-вывода, принтеры, кабели, контроллеры, линии связи) и т.д.;
        - - программное обеспечение — исходные, объектные, загрузочные модули, приобретенные программы, «домашние» разработки, утилиты, операционные системы и системные программы (компиляторы, компоновщики и др.), диагностические программы и т.д.;
    - 2.
        - - оборудование — ЭВМ и их составные части (процессоры, мониторы, терминалы, рабочие станции), периферийные устройства (дисководы, устройства back-up, порты ввода-вывода, принтеры, кабели, контроллеры, линии связи) и т.д.; -
        - программное обеспечение — исходные, объектные, загрузочные модули, приобретенные программы, «домашние» разработки, утилиты, операционные системы и системные программы (компиляторы, компоновщики и др.), диагностические программы и т.д.;
        - - данные — временные, хранимые постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
        - - сотрудники — пользователи и обслуживающий персонал.
    - 3.
            - - сотрудники — пользователи и обслуживающий персонал;
        - - данные — временные, хранимые постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
            - - программное обеспечение — исходные, объектные, загрузочные модули, приобретенные программы, «домашние» разработки, утилиты, операционные системы и системные программы (компиляторы, компоновщики и др.), диагностические программы и т.д.;
        - - оборудование — ЭВМ и их составные части (процессоры, мониторы, терминалы, рабочие станции), периферийные устройства (дисководы, устройства back-up, порты ввода-вывода, принтеры, кабели, контроллеры, линии связи) и т.д.
    - 4.
        - - данные — временные, хранимые постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
        - - сотрудники — пользователи и обслуживающий персонал.
        - - оборудование — ЭВМ и их составные части (процессоры, мониторы, терминалы, рабочие станции), периферийные устройства (дисководы, устройства back-up, порты ввода-вывода, принтеры, кабели, контроллеры, линии связи) и т.д.;
        - - программное обеспечение — исходные, объектные, загрузочные модули, приобретенные программы, «домашние» разработки, утилиты, операционные системы и системные программы (компиляторы, компоновщики и др.), диагностические программы и т.д.;

17. Назовите основные угрозы информационной безопасности ИС:
    - Нарушение конфиденциальности информации. Информация, хранимая и обрабатываемая в ИС, может иметь большую ценность для ее владельца. Ее использование другими лицами наносит значительный ущерб интересам владельца.
    - Нарушение целостности информации. Потеря целостности информации (полная или частичная, компрометация, дезинформация) -угроза близкая к ее раскрытию.

- Нарушение (частичное или полное) работоспособности ИС (нарушение доступности).
- Несанкционированный доступ (НСД). Он заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности.

18. Какие бывают методы защиты речевой информации:
    - Математические
    - Физические
    - Пассивные
    - Активные
    - Открытые
    - Стеганографические

19. Пассивные методы защиты речевой информации предполагают:
    - Пассивное реагирование на угрозы информации
    - Регистрацию инцидентов безопасности и контроль всех событий
    - Ослабление непосредственно акустических сигналов, а также продуктов электроакустических преобразований
    - Устранение всех активных методов воздействия на речевую информацию

20. Активные методы защиты информации предполагают:
    - Активное устранение угроз безопасности
    - Уничтожение всех несанкционированных устройств
    - Создание маскирующих помех
    - Подавление устройств снятия информации и аппаратов звукозаписи

5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме экзамена используется следующая шкала оценивания: 2, 3, 4, 5.

Критериями оценивания достижений показателей являются:

Наименование показателя оценивания результата обучения по дисциплине	Критерий оценивания
Знания	Знание терминов, определений, понятий
	Знание основных закономерностей, соотношений, принципов
	Объем освоенного материала
	Полнота ответов на вопросы
	Четкость изложения и интерпретации знаний
Умения	Умение анализировать основные положения законодательства в области безопасности информации
	Умение использовать руководящие документы регуляторов в области информационной безопасности

Навыки	Владение навыками теоретического и экспериментального исследования объектов профессиональной деятельности
	Качество выполнения исследований объектов профессиональной деятельности
	Самостоятельность выполнения исследований объектов профессиональной деятельности

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю Знания.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Знание терминов, определений, понятий	Не знает терминов и определений	Знает термины и определения, но допускает неточности формулировок	Знает термины и определения	Знает термины и определения, может корректно сформулировать их самостоятельно
Знание основных закономерностей, соотношений, принципов	Не знает основные закономерности и соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний, их интерпретирует и использует	Знает основные закономерности, соотношения, принципы построения знаний, может самостоятельно их получить и использовать
Объем освоенного материала	Не знает значительной части материала дисциплины	Знает только основной материал дисциплины, не усвоил его деталей	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Полнота ответов на вопросы	Не дает ответы на большинство вопросов	Дает неполные ответы на все вопросы	Дает ответы на вопросы, но не все - полные	Дает полные, развернутые ответы на поставленные вопросы
Четкость изложения и интерпретации знаний	Излагает знания без логической последовательности	Излагает знания с нарушениями в логической последовательности	Излагает знания без нарушений в логической последовательности	Излагает знания в логической последовательности, самостоятельно их интерпретируя и анализируя
	Не иллюстрирует изложение поясняющими схемами, рисунками и примерами	Выполняет поясняющие схемы и рисунки небрежно и с ошибками	Выполняет поясняющие рисунки и схемы корректно и понятно	Выполняет поясняющие рисунки и схемы точно и аккуратно, раскрывая полноту усвоенных знаний
	Неверно излагает и интерпретирует знания	Допускает неточности в изложении и интерпретации знаний	Грамотно и по существу излагает знания	Грамотно и точно излагает знания, делает самостоятельные выводы

Оценка сформированности компетенций по показателю Умения.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Умение анализировать основные положения законодательства в области безопасности информации	Не умеет анализировать основные положения законодательства в области безопасности информации	Допускает неточности в анализе основных положений законодательства в области безопасности информации	Умеет анализировать основные положения законодательства в области безопасности информации	Умеет анализировать основные положения законодательства в области безопасности информации и делать обобщающие выводы
Умение использовать руководящие документы регуляторов в области информационной безопасности	Не умеет использовать руководящие документы регуляторов в области информационной безопасности	Использование руководящих документов регуляторов в области информационной безопасности вызывает затруднения	Умеет использовать руководящие документы регуляторов в области информационной безопасности	Умело использует руководящие документы регуляторов в области информационной безопасности

Оценка сформированности компетенций по показателю Навыки.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Владение навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Не владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Не достаточно хорошо владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Профессионально владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности
Качество выполнения исследований объектов профессиональной деятельности	Не качественно выполняет исследования объектов профессиональной деятельности, допускает грубые ошибки	Не достаточно качественно выполняет исследования объектов профессиональной деятельности, допускает и исправляет ошибки с посторонней помощью	Не достаточно качественно выполняет исследования объектов профессиональной деятельности, допускает и исправляет ошибки самостоятельно	Качественно выполняет исследования объектов профессиональной деятельности
Самостоятельность выполнения исследований	Не может самостоятельно выполнять	Выполняет исследования объектов	При выполнении исследования объектов	Самостоятельно выполняет исследования

объектов профессиональной деятельности	исследования объектов профессиональной деятельности	профессиональной деятельности с посторонней помощью	профессиональной деятельности иногда требуется посторонняя помощь	объектов профессиональной деятельности

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

6.1. Материально-техническое обеспечение

№	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1.	Учебная аудитория для проведения лекционных занятий	Специализированная мебель. Мультимедийная установка, экран, доски
2.	Учебная аудитория для проведения практических занятий	Специализированная мебель. Компьютеры на базе процессоров Intel или AMD.
3.	Читальный зал библиотеки для самостоятельной работы	Специализированная мебель. Компьютерная техника, подключенная к сети интернет и имеющая доступ в электронно-образовательную среду.

6.2. Лицензионное и свободно распространяемое программное обеспечение

№	Перечень лицензионного программного обеспечения.	Реквизиты подтверждающего документа
1	Microsoft Windows 10 Корпоративная	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
2	Microsoft Office Professional Plus 2016	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
3	Kaspersky Endpoint Security «Стандартный Russian Edition»	Сублицензионный договор № 102 от 24.05.2018. Срок действия лицензии до 19.08.2020 Гражданско-правовой Договор (Контракт) № 27782 «Поставка продления права пользования (лицензии) Kaspersky Endpoint Security от 03.06.2020. Срок действия лицензии 19.08.2022г.
4	Среды программирования Free Pascal, Dev C++ или CodeBlocks	Свободно распространяемое ПО согласно условиям лицензионного соглашения

6.3. Перечень учебных изданий и учебно-методических материалов

6.1. Перечень основной литературы

1. Зайцев А.П. Технические средства и методы защиты информации : Учебник / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд. - М. : Горячая линия-Телеком, 2016. - 442 с.

2. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам / Г. А. Бузов. - Москва : Горячая линия - Телеком, 2017. - 585 с

3. Хорев А.А. Техническая защита информации : Учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А.А. Хорев; М-во образования и науки РФ, Федеральное агентство по образованию, МИЭТ(ТУ). - М. : НПЦ Аналитика, 2008. - 436 с. - ISBN 978-59901488-1-9 .

6.2. Периодические издания

1. ЗАЩИТА ИНФОРМАЦИИ. INSIDE : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 15.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582.

2. Безопасность информационных технологий : научный журнал / ФГАОУ ВО "Национальный исследовательский ядерный университет "МИФИ". - Москва : НИЯУ МИФИ, 1994 - . - URL: https://bit.mephi.ru/index.php/bit/index (дата обращения: 10.03.2021). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online).

3. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 15.03.2021). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813..

4. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011 - 2018. - URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 16.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print).

6.3. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы

1. Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации, Гостехкомиссия России, 2002.

2. Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации, Гостехкомиссия России, 2002.

3. Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам, Гостехкомиссия России, Москва, 2002.

4. Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах», Гостехкомиссия России, Москва, 2002.

5. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения Protection of information. Object of informatisation. Factors influencing the information. General: Национальный стандарт РФ: Введ.

01.02.2008.- М.: Стандартинформ, (Переиздание) 2018. -URL: https://docs.cntd.ru/document/1200057516 (дата обращения: 16.03.2021)

6. Рекомендации по стандартизации Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации Information technologies. Basic terms and definitions in scope of technical protection of information, Национальный стандарт РФ: Введ. 01.01.2006.- М.: Стандартинформ, 2018.

7. Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения: Technical information protection. Terms and definitions Национальный стандарт РФ: Введ. 01.06.2006.- М.: Стандартинформ, 2006.

8. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Одобрены решением коллегии Гостехкомиссии России от 2 марта 2001 г. № 7.2.

9. Федеральный закон от 27 июля 2006 г. N 149-ФЗ: с изм. на 02 июля 2021 г.- «Об информации, информационных технологиях и о защите информации»; Текст: электронный // Техэксперт : – URL: https://docs.cntd.ru/document/901990051 - (дата обращения 15.03.2021).-Текст электронный .

6.4. Перечень профессиональных баз данных, информационных справочных систем

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 16.03.2021).
2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021).
3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchitainformatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 10.03.2021)

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Средства обеспечения освоения дисциплины.

Мультимедийное оборудование: компьютер с программным обеспечением, возможностью подключения к сети Интернет и обеспечением доступа в электроннообразовательную среду БГТУ; проектор; акустическое оборудование (микрофон, звуковые колонки), веб камера с микрофоном). Учебная доска.

Программное обеспечение - Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Fire-fox/Google Chrome /Explorer).

Для лабораторных занятий используется Лаборатория Технических средств защиты информации: ГК 425.

Состав оборудования:

- Многофункциональное поисковое устройство ST 131 Пиранья II;
- Многофункциональное поисковое устройство ST 031 Пиранья I;
- Нелинейный локатор «Обь»;
- ЛГШ-513 Комбинированное устройство защиты от утечки информации по цепям электропитания, заземления и ПЭМИ

- Имитатор нелегальных средств съема информации "Шиповник"
- Устройство защиты от утечки информации «Аллигатор»
- Комплект типового лабораторного оборудования ПРОФИСТЕНД, включающее:
    - Исследование цифрового согласованного фильтра;
    - Исследование широкополосных сигналов;
    - Изучение устройства перемежения символов;
    - Изучение кодирования и декодирования сообщений;
    - Изучение основы криптографии;
    - Исследование структурных помех
    - Осциллографы SDS 1022DL – 5 шт.

ПРИЛОЖЕНИЯ

Приложение №1.

Методические указания для обучающегося по освоению дисциплины

Примерным учебным планом на изучение дисциплины отводится один семестр. В качестве итогового контроля предусмотрен экзамен. Форма проведения экзамена - устный опрос по билетам.

В процессе изучения дисциплины упор делается на сочетание методов активизации познавательной деятельности с лекционными и лабораторными занятиями.

Во введении отмечается значение информации в жизни общества, даются основные термины технической защиты информации, упоминаются нормативные и правовые акты, регулирующие данную сферу деятельности.

В первом разделе приводится информация о технических каналах утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Отдельно следует выделить технические каналы утечки речевой информации.

Во втором разделе изучаются способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами, способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.

В третьем разделе объясняются методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами, методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам, а также методы и средства выявления электронных устройств негласного получения информации.

Четвертый раздел включает в себя основы физической защиты объектов информатизации, а также принципы организации технической защиты информации на объектах информатизации.

Приложение № 2

Методические указания студентам по подготовке практико-ориентированных индивидуальных домашних заданий

Задачи выполнения практико-ориентированных индивидуальных домашних заданий:

- обучение студентов самостоятельному применению полученных знаний для решения конкретных практических задач защиты информации от утечки по техническим каналам;
- развитие навыков подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по организации, способам и средствам защиты информации на объектах информатизации;
- овладение методами анализа потенциальных технических каналов утечки информации на объектах информатизации и в выделенных помещениях;
- привитие навыков проведения аналитического обоснования необходимости создания подсистемы защиты информации от утечки по техническим каналам на объектах информатизации учреждения (предприятия);
- привитие навыков разработки предложений в техническое задание на создание подсистемы защиты объекта информатизации организации от утечки информации по техническим каналам.

Каждое домашнее задание направлено на формирование отдельных умений, необходимых для формирования общепрофессиональных и профессиональных компетенции.

Домашние задания выполняются каждым студентом индивидуально. По результатам выполнения каждого домашнего задания студент оформляет и представляет отчет. При защите отчетов по домашним заданиям преподаватель разбирает типовые ошибки и указывает их причины.

Домашнее задание № 1

Темы домашнего задания № 1:

1. Цели специальных поисковых работ и особенности их реализации
2. Поисковые исследования, проводимые при базовой мотивации – «утеря конкретных конфиденциальных материалов», их особенности и реализация
3. Поисковые исследования, проводимые при базовой мотивации – «проявление заинтересованности со стороны конкурирующей организации к определенным конфиденциальным материалам или к коммерческой деятельности в целом», их особенности и реализация
4. Поисковые исследования, проводимые при базовой мотивации – «предупреждающие профилактические действия», их особенности и реализация
5. Обеспечение конспирации и легендирования поисковых работ на всех этапах их осуществления, предлагаемые мероприятия, порядок их оформления и утверждения
6. Изучение объекта поиска и его окружения, уточнение технических и профессиональных возможностей источника угроз, анализ режимных процедур на объекте, планирование технических и информационных процедур на объекте поиска для подготовки плана поисковых исследований
7. Разработка плана поисковых исследований и подготовка к их проведению, содержание работ на каждом этапе, моделирование возможных вариантов их выполнения, перечень

используемой поисковой техники на каждом из этапов, планирование линии поведения каждого участника поисковой бригады

8. Осмотр и проверка предметов быта и интерьера, находящихся на объекте поиска, визуальный осмотр – от общего к частному, используемая поисковая техника, методики проверки
9. Поиск устройств съема информации, внедренных в электронные приборы. Перечень используемой поисковой техники, алгоритм поиска, оформление результатов
10. Исследование электромагнитной обстановки в помещениях, автомашинах и на открытой местности, моделирование возможных каналов утечки информации по каждом из перечисленных вариантов, перечень поисковой техники, определение возможных мест размещения пунктов приема и контроля, порядок их выявления, оформление результатов проведенных работ
11. Поиск устройств съема информации в проводных коммуникациях, особенности проведения поисковых работ по проверке электрической сети, абонентской и офисной телефонной сети, радиотрансляционной сети, сетей охранной и пожарной сигнализации
12. Обследование элементов строительных конструкций, обследование оградительных элементов строительных конструкций, обследование окон, вентиляционных каналов, водопроводных и теплопроводных коммуникаций, выработка рекомендаций по защите информации
13. Подведение итогов поисковых исследований, описание проведенных поисковых исследований, оформление акта проведения исследований, предложения по нейтрализации возможных каналов утечки
14. Обзор представленных на рынке современных технических средств поиска каналов утечки информации
15. Обзор представленных на рынке современных технических средств защиты информации, контроля и блокировки сетей передачи информации, определения местоположения источников излучения, ложных станций сотовой связи.

Объем домашнего задания составляет 3 - 4 страницы машинописного текста пояснительной записки и других материалов, выполненных на стандартных листах формата А4.

Пояснительная записка оформляется в редакторе Word, шрифт Times New Roman размер – 12-14 интервал – полуторный (30 строк по 60 печатных знаков в каждой строке, считая пробелы). Размеры полей следующие: левое – 30 мм, правое — не менее 10 мм, верхнее - не менее 20 мм, нижнее — не менее 20 мм. Отступ красной строки 1,25 см.

Структура отчета по домашнему заданию должна отвечать традиционным требованиям, предъявляемым к учебно-квалификационным работам и включать: титульный лист; содержание (оглавление); введение; основную часть; заключение; список литературы.

Домашнее задание № 2

Тема домашнего задания № 2 «Анализ потенциальных технических каналов утечки информации на объекте информатизации организации».

Защищаемый объект информатизации – помещение, предназначенное для ведения конфиденциальных переговоров, в котором установлено автоматизированное рабочее место для обработки конфиденциальной информации на базе ПЭВМ.

Для выполнения задания студентам выделяются реально существующие объекты информатизации предприятий (учреждений).

Объем домашнего задания составляет 8 - 10 страниц машинописного текста пояснительной записки и графических материалов, выполненных на стандартных листах формата А4.

Пояснительная записка оформляется в редакторе Word, шрифт Times New Roman размер – 12-14 интервал – полуторный (30 строк по 60 печатных знаков в каждой строке, считая пробелы). Размеры полей следующие: левое – 30 мм, правое — не менее 10 мм, верхнее - не менее 20 мм, нижнее — не менее 20 мм. Отступ красной строки 1,25 см.

Структура отчета по домашнему заданию должна отвечать традиционным требованиям, предъявляемым к учебно-квалификационным работам и включать: титульный лист; содержание (оглавление); введение; основную часть; заключение; список литературы.

В основной части задания:

- определяется назначение защищаемого объекта информатизации (далее по тексту – защищаемого объекта);
- проводится описание защищаемого помещения (входа в помещение, пола, потолка, стен, окон, системы вентиляции и кондиционирования);
- определяются технические средства, входящие в состав автоматизированного рабочего места для обработки конфиденциальной информации (далее по тексту – ОТСС), установленные на объекте информатизации и непосредственно участвующие в обработке конфиденциальной информации, составляется их перечень;
- определяются вспомогательные технические средства и системы (ВТСС), установленные на объекте информатизации, составляется их перечень;
- составляется схема расположения мебели, ОТСС и ВТСС в защищаемом помещении;
- проводится анализ местоположения защищаемого объекта на местности и определяется граница его контролируемой зоны;
- описывается система электропитания и заземления защищаемого объекта;
- определяются месторасположение трансформаторной подстанции и заземлителя относительно границы контролируемой зоны объекта;
- устанавливаются инженерные коммуникации и посторонние проводники, выходящие за пределы контролируемой зоны объекта;
- устанавливаются соединительные линии ВТСС, выходящие за пределы контролируемой зоны объекта;
- определяется наличие физической охраны здания, в котором расположено предприятие (учреждение);
- определяется наличие системы охранной сигнализации, охранного телевидения, системы контроля и управления доступом в служебные и технические помещения предприятия (учреждения);
- определяется возможность неконтролируемого доступа посторонних лиц к ограждающим конструкциям и окнам выделенного помещения;
- описывается порядок доступа сотрудников и посторонних лиц на предприятие (в учреждение);
- описывается порядок доступа сотрудников предприятия (учреждение), а также посторонних лиц на объект информатизации в служебное и неслужебное время;
- определяются помещения, смежные с защищаемым объектом информатизации, устанавливается их назначение и принадлежность;
- определяется возможность доступа посторонних лиц в смежные с защищаемым объектом информатизации помещения, а также к инженерным коммуникациям, проходящим через объект информатизации;
- описываются и анализируются организационные мероприятия по технической защите информации, реализуемые на предприятии (в учреждении);
- проводится анализ технических средств защиты объекта информатизации от утечки информации по техническим каналам;
- проводится анализ технических средств защиты выделенного помещения от утечки речевой информации по техническим каналам;

- разрабатывается модель противника (злоумышленника);
- проводится анализ возможностей заинтересованных субъектов по перехвату информации, обрабатываемой ПЭВМ, по каналу утечки информации, возникающему за счет побочных электромагнитных излучений (ПЭМИ) ПЭВМ и каналам утечки информации, возникающим за счет наводок ПЭМИ ПЭВМ на токопроводящие коммуникации, линии электропитания и цепи заземления;
- проводится анализ возможностей непреднамеренного прослушивания конфиденциальных разговоров, ведущихся в выделенном помещении, посторонними лицами;
- проводится анализ возможностей заинтересованных субъектов по перехвату конфиденциальных разговоров, ведущихся в выделенном помещении:
- с использованием лазерных акустических систем разведки (ЛАСР) и направленных микрофонов;
- электронных стетоскопов и радиостетоскопов;
- аппаратуры «высокочастотного навязывания» и средств, подключаемых к соедини-
- тельным линиям ВТСС;
- электронных устройств перехвата речевой информации, возможно внедренных в выделенное помещение;
- составляется перечень потенциальных технических каналов утечки информации, обрабатываемой ОСТТ с указанием возможных средства перехвата информации (стационарных, мобильных и портативных) и мест их возможной установки;
- составляется перечень потенциальных технических каналов утечки речевой информации из выделенных помещений (стационарных, мобильных и портативных) и мест их возможной установки.

Заключение содержит в сжатой форме теоретические выводы, полученные в результате выполнения задания. Заключение должно показать, насколько материал работы может быть использован в практике конкретной организации (предприятия).

Список использованной литературы включает источники и литературу, использованные студентом в ходе подготовки и написания домашнего задания.

Таблицы, схемы, рисунки, графики большого формата, фрагменты которых используются в основном тексте, могут быть вынесены в приложения к пояснительной записке.