УТВЕРЖДЕНО
решением Ученого совета ФМИАТ
от «16» мая 2023 г., протокол № 4/23
Председатель _____ Волков М.А.
(подпись, расшифровка подписи)
«16» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Инструментальные средства контроля защищённости информации
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	4

Специальность: 10.05.03 "Информационная безопасность автоматизированных систем"
(код специальности (направления), полное наименование)

Специализация: "Инструментальные средства контроля защищенности информации"
полное наименование

Форма обучения: очная
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: «01» 09 2023 г.

Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Иванцов Андрей Михайлович	ИБ и ТУ	Кандидат технических наук, доцент

СОГЛАСОВАНО
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
/ _____ / Андреев А.С. / *(подпись)* *(Ф.И.О.)* «11» 05 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

обучить студентов принципам контроля защищенности информации, подходам к анализу и решению задач контроля защищенности информации;

содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Задачи освоения дисциплины:

дать основы:

использования инструментальных средств контроля защищённости информации;

применения основных методов контроля защищённости информации

обучения инструментальному мониторингу защищённости информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Инструментальные средства контроля защищенности информации» изучается в 7-8 семестрах и относится к числу вариативных дисциплин блока Б1.В.2.ДВ, предназначенного для студентов, обучающихся по специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов: «Электроника и схемотехника»; «Организация ЭВМ и вычислительных систем», «Основы информационной безопасности», «Техническая защита информации», «Программно-аппаратные средства защиты информации», «Безопасность вычислительных сетей».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

знание базовых понятий в области информационной безопасности;

способность использовать нормативные правовые документы;

способность анализировать социально-значимые проблемы и процессы;

способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Разработка и эксплуатация автоматизированных систем в защищённом исполнении», «Безопасность открытых информационных систем», а в части выявления технических каналов утечки информации объекта информатизации, на дисциплинах, изучающих методы и средства защиты информации.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ПК-1 - Способен организовать работы по выполнению в информационной системе требований защиты информации ограниченного доступа	**Знать:** Источники и классификацию угроз информационной безопасности Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Нормативные правовые акты в области защиты информации **Уметь:** Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации Организовывать реализацию мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты Организовывать процесс применения защищенных протоколов, межсетевых экранов, средств обнаружения вторжений для защиты информации в сетях **Владеть:** Навыками организации применения защищенных протоколов, межсетевых экранов и средств обнаружения вторжений для защиты информации в сетях Навыками управления процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем
ПК-2 - Способен осуществлять тестирование систем защиты информации автоматизированных систем	**Знает:** Принципы построения и функционирования систем и сетей передачи информации Эталонную модель взаимодействия открытых систем Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах **Умеет:** Применять действующую нормативную базу в области обеспечения безопасности информации Контролировать безотказное функционирование технических средств защиты информации **Владеет:** Навыками подбора инструментальных средств тестирования систем защиты информации автоматизированных систем
ПК-6 - Способен проводить	**Знать:**

контроль защищенности информации от НСД	Методы защиты информации от несанкционированного доступа и специальных программных воздействий на нее Методы и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий **Уметь:** Проводить оценку защищенности информации от несанкционированного доступа и специальных воздействий Проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воздействий, выполнение правил их эксплуатации **Владеть:** Навыками проведения контроля защищенности информации от несанкционированного доступа и специальных воздействий

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 5.

4.2. Объем дисциплины по видам учебной работы (в часах):

Вид учебной работы	Количество часов (форма обучения ___очная_____)			
	Всего по плану	В т.ч. по семестрам		
		7 семестр	8 семестр	
Контактная работа обучающихся с преподавателем	108	54/54*	54/54*	
Аудиторные занятия:	108	54/54*	54/54*	
Лекции	36	18/18*	18/18*	
Практические и семинарские занятия				
Лабораторные работы (лабораторный практикум)	72	36/36*	36/36*	
Самостоятельная работа	36	18	18	
Форма текущего контроля знаний и контроля самостоятельной работы: Тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на семинарах; - вопросы при защите лабораторных работ	-Тестирование на семинарах; - вопросы при защите лабораторных работ	
Курсовая работа				
Виды промежуточной аттестации (экзамен,	Зачёт, экзамен	Зачет	Экзамен	

зачет)				
Всего часов по дисциплине	180	72	108	

* В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

4.3. Содержание дисциплины (модуля.) Распределение часов по темам и видам учебной работы:

Форма обучения _____очная_____

Название разделов и тем	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		лекции	Практич. занятия, семинары	Лабораторные работа			
Раздел 1. Теоретические основы обеспечения защищённости информации							
1. Классификация и основные характеристики технических каналов утечки информации	6	4				2	Тесты Т1
2. Каналы утечки информации, обрабатываемой техническими средствами обработки и передачи информации	6	4				2	Тесты Т2
3. Каналы утечки акустической речевой информации	6	4				2	Тесты Т3
4. Каналы утечки видовой информации	4	2				2	Тесты Т4
Раздел 2. Основные методы и инструментальные средства контроля защищённости информации							
5. Методы и инструментальные средства контроля защищённости информации для обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации	16	4		8		4	Тесты Т5 лаб. раб. № 1-2
6. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации.	12	4		4		4	Тесты Т6 лаб. раб. № 3
7. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации. Часть 3	20	4		12	8	4	Тесты Т7 лаб. раб. № 4-5
8. Методы и средства выявления электромагнитных каналов утечки информации технических средств	10	2		6	6	2	Тесты Т8 лаб. раб. № 6

обработки и передачи информации							
9. Методы и средства выявления электрических каналов утечки информации технических средств обработки и передачи информации	10	2		6	6	2	Тесты Т9 лаб. раб. № 7-8
10. Методы и средства выявления каналов утечки акустической речевой информации.	32	2		26		4	Тесты Т10 лаб. раб. № 9-11
Раздел 3. Основные мероприятия по выявлению технических каналов утечки информации							
11. Организация специальных обследований помещений и специальных проверок технических средств	10	2		4	4	4	Тесты Т11 лаб. раб. № 12
12. Организация специальных исследований технических средств и помещений.	12	2		6	6	4	Тесты Т12 лаб. раб. № 13
Итого:	144	36		72	30	36	Зачёт, экзамен

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Теоретические основы обеспечения защищённости информации

Тема 1. Классификация и основные характеристики технических каналов утечки информации.

Классификация технических каналов утечки информации (по причинам возникновения и виду информации). Каналы утечки информации, обрабатываемой техническими средствами обработки и передачи информации (ТС ОПИ). Каналы утечки акустической речевой информации (АРИ). Каналы утечки видовой информации. Модель технического канала утечки информации и основные характеристики.

Тема 2. Каналы утечки информации, обрабатываемой техническими средствами обработки и передачи информации.

Электромагнитные каналы утечки информации ТС ОПИ: побочные электромагнитные излучения (ПЭМИ) и паразитное электромагнитное излучение. Электрические каналы утечки информации ТС ОПИ: наводки в технических средствах, проводах, кабелях и иных околопроводящих коммуникациях и конструкциях, наводки в цепях электропитания и цепях заземления. Возможности технической разведки ПЭМИН.

Тема 3. Каналы утечки акустической речевой информации

Акустические каналы утечки АРИ. Виброакустические (вибрационные) каналы утечки АРИ. Оптико-электронные (лазерные) каналы утечки АРИ. Акустоэлектрические каналы утечки АРИ. Классификация акустоэлектрических преобразователей. Модуляция побочных электромагнитных излучений и паразитного электромагнитного излучения акустическими сигналами. Параметрические каналы утечки АРИ: ВЧ-облучение, ВЧ-прокачка, ВЧ-навязывание. Акустооптические каналы утечки АРИ.

Тема 4. Каналы утечки видовой информации.

Наблюдение за объектом. Съемка объектов. Электронные устройства негласного получения информации (ЭУНПИ). Видеозакладки (перехват видеоинформации), аудиозакладки (перехват аудиоинформации), аппаратные закладки (перехват информации, циркулирующей в ТС ОПИ). Возможности технической разведки ЭУНПИ.

Раздел 2. Основные методы и инструментальные средства контроля защищённости информации

Тема 5. Методы и инструментальные средства контроля защищённости информации для обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации.

Радиоконтроль (радиомониторинг) эфира и линий – методы выявления активных ЭУНПИ с передачей информации по радиоканалу (включая сотовые и беспроводные сети) и отходящим линиям. Основные характеристики современных автоматизированных поисковых комплексов российских производителей.

Тема 6. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации.

Активные методы выявления ЭУНПИ с дистанционным управлением и пассивных ЭУНПИ в эфире и отходящих линиях. Основные характеристики современных автоматизированных поисковых комплексов российских производителей.

Тема 7. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации. Часть 3.

Методы неразрушающего контроля – радиационный, визуальный, тепловой, вихретоковый. Метод оптической локации. Метод нелинейной локации. Рефлектометрический метод. Основные характеристики современной досмотровой техники.

Тема 8. Методы и средства выявления электромагнитных каналов утечки информации технических средств обработки и передачи информации.

Методика оценки защищенности интерфейсов ТС ОПИ от утечки конфиденциальной информации за счет побочных электромагнитных излучений. Предъявляемые требования к измерительной аппаратуре. Предъявляемые требования к средствам активной защиты информации.

Тема 9. Методы и средства выявления электрических каналов утечки информации технических средств обработки и передачи информации.

Методика оценки защищенности интерфейсов ТС ОПИ от утечки конфиденциальной информации за счет наводок побочных электромагнитных излучений. Предъявляемые требования к измерительной аппаратуре. Предъявляемые требования к пассивным средствам защиты информации.

Тема 10. Методы и средства выявления каналов утечки акустической речевой информации.

Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам акустоэлектрических преобразований. Предъявляемые требования к измерительной аппаратуре. Предъявляемые требования к средствам активной акустической и вибрационной защиты.

Раздел 3. Основные мероприятия по выявлению технических каналов утечки информации

Тема 11. Организация специальных обследований помещений и специальных проверок технических средств.

Порядок проведения специальной проверки технических средств. Алгоритм проведения специального обследования помещения. Документальное оформление результатов

работ.

Тема 12. Организация специальных исследований технических средств и помещений.

Порядок проведения специальных исследований средств вычислительной техники. Алгоритм проведения специальных исследований помещения. Документальное оформление результатов работ.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические и семинарские занятия не предусмотрены учебным планом дисциплины.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 2. Основные методы и инструментальные средства контроля защищённости информации

Тема 5. Методы и инструментальные средства контроля защищённости информации для обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации.

Лабораторная работа № 1 (4 часа). «Выявление радиосигналов электронных устройств негласного получения информации»

Цель работы: Ознакомление с техническими характеристиками поискового оборудования на примере широкодиапазонного радиоприемника «*AR-3000A*» (AOR Ltd. Япония) и спектрального коррелятора «*OSCOR-5000 DeLuxe+*» (REI, США), изучение правил эксплуатации, получение практических навыков работы с поисковым оборудованием.

Лабораторная работа № 2 (4 часа) «Выявление радиосигналов электронных устройств негласного получения информации использующих сотовую и беспроводную связь»

Цель работы: Ознакомление с техническими характеристиками поискового оборудования на примере детектора поля «*D-006*» (Россия), многофункционального поискового прибора «*ST-032 Пиранья*» (Россия), «*Поиск-GSM-M1*» (Россия) и «*AirMagnet Spectrum Analyzer Pro*» (Fluke Corporation, США), изучение правил эксплуатации, получение практических навыков работы с поисковым оборудованием.

Тема 6. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации.

Лабораторная работа № 3 (4 часа) «Выявление электронных устройств негласного получения информации активными методами»

Цель работы: Ознакомление с техническими характеристиками поискового оборудования на примере комплекса оценки защищенности «*Вепрь*» (Россия), изучение правил эксплуатации, получение практических навыков работы с поисковым оборудованием.

Тема 7. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации.

Лабораторная работа № 4 (6 часов) «Выявление электронных устройств негласного получения информации вихретоковым методом и методом нелинейной локации»

Цель работы: Ознакомление с техническими характеристиками поискового оборудования на примере металлоискателя и нелинейного радиолокатора «*NR-900EMS*» (Россия), изучение правил эксплуатации, получение практических навыков работы с поисковым оборудованием.

Лабораторная работа № 5 (6 часов) «Выявление электронных устройств негласного получения информации тепловым методом и методом оптической локации».

Ознакомление с техническими характеристиками поискового оборудования на примере многофункционального поискового прибора «*ST-032 Пиранья*» (Россия) и прибора обнаружения скрытых видеокамер «*Ворон*» (Россия), изучение правил эксплуатации, получение практических навыков работы с поисковым оборудованием.

Тема 8. Методы и средства выявления электромагнитных каналов утечки информации технических средств обработки и передачи информации

Лабораторная работа № 6 (6 часов) «Специальные исследования интерфейсов средств вычислительной техники на наличие побочных электромагнитных излучений»

Ознакомление с программами тестирования средств вычислительной техники и техническими характеристиками измерительного оборудования на примере программно-аппаратного комплекса «*Сигурд*» (Россия) и измерительных антенн, изучение правил эксплуатации, получение практических навыков работы с измерительным оборудованием.

Тема 9. Методы и средства выявления электрических каналов утечки информации технических средств обработки и передачи информации.

Лабораторная работа № 7 (4 часа) «Специальные исследования интерфейсов средств вычислительной техники на наличие наводок побочных электромагнитных излучений».

Ознакомление с программами тестирования средств вычислительной техники и техническими характеристиками измерительного оборудования на примере программно-аппаратного комплекса «*Сигурд*» (Россия) и измерительных токосъемников, изучение правил эксплуатации, получение практических навыков работы с измерительным оборудованием.

Лабораторная работа № 8 (2 часа) «Исследование средств защиты информации средств вычислительной техники».

Цель работы: Исследование возможностей средства активной защиты – «*Гром-ЗИ-4*» (Россия) и фильтра сетевого помехоподавляющего, получение практических навыков в работе по защите средств вычислительной техники.

Тема 10. Методы и средства выявления каналов утечки акустической речевой информации.

Лабораторная работа № 9 (8 часов) «Специальные исследования выделенных помещений»

Ознакомление с техническими характеристиками измерительного оборудования на примере программно-аппаратного комплекса «*Шёпот*» (Россия), изучение правил эксплуатации, получение практических навыков работы с измерительным оборудованием.

Лабораторная работа № 10 (8 часов) «Исследование средств защиты информации».

Цель работы: Исследование возможностей средств активной защиты помещений – генератор виброакустического шума «*ANG-200*0» (Россия) и виброакустический шумогенератор «*SI 3010*» (Россия), получение практических навыков в работе по защите выделенных помещений.

Лабораторная работа № 11 (10 часов) «Специальные исследования технических средств выделенных помещений»

Ознакомление с техническими характеристиками измерительного оборудования на примере селективного микровольтметра «*В6-9»* и исследование возможностей средств пассивной защиты технических средств выделенных помещений, изучение правил эксплуатации, получение практических навыков работы с измерительным оборудованием.

Раздел 3. Основные мероприятия по выявлению технических каналов утечки информации

Тема 11. Организация специальных обследований помещений и специальных проверок технических средств.

Лабораторная работа № 12 (4 часа). «Использование инструментальных средств для проведения специальных проверок и специальных обследований».

Цель: Изучить основные приборы, используемые в ходе проведения специальных проверок и специальных обследований. Результат: отчет.

Методические указания: основное внимание должно быть уделено методике использования основных инструментальных средств и первичным навыкам составления заключений по результатам проведенных мероприятий.

Тема 12. Организация специальных исследований технических средств и помещений..

Лабораторная работа № 13 (6 часов). «Использование инструментальных средств для проведения специальных исследований».

Цель: Изучить нормативные документы и основные приборы, используемые в ходе проведения специальных исследований. Результат: отчет.

Методические указания: основное внимание должно быть уделено методике использования основных инструментальных средств и первичным навыкам составления протоколов специальных исследований.

Все лабораторные работы проводятся в интерактивной форме, а именно используются:

диалоговое обучение, в ходе которого осуществляется взаимодействие между студентом и преподавателем, между самими студентами, группами студентов;

элементы деловых игр, «мозговой штурм» или дискуссии по рассматриваемым вопросам.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Курсовые, контрольные работы и рефераты не предусмотрены учебным планом дисциплины.

9.1 ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЁТУ

1. Классификация технических каналов утечки информации
2. Модель технического канала утечки информации
3. Основные характеристики источника информации, среды распространения и приемника информации
4. Каналы утечки информации, обрабатываемой техническими средствами обработки и передачи информации
5. Электромагнитные каналы утечки информации технических средств обработки и передачи информации
6. Побочные электромагнитные излучения и паразитное электромагнитное излучение
7. Электрические каналы утечки информации технических средств обработки и передачи информации
8. Наводки побочных электромагнитных излучений
9. Каналы утечки акустической речевой информации
10. Акустические, виброакустические (вибрационные), оптико-электронные (лазерные) каналы утечки акустической речевой информации
11. Акустоэлектрические каналы утечки акустической речевой информации. Классификация акустоэлектрических преобразователей. Модуляция побочных электромагнитных излучений и паразитного электромагнитного излучения акустическими сигналами.
12. Параметрические каналы утечки акустической речевой информации: ВЧ-облучение, ВЧ-прокачка, ВЧ-навязывание.
13. Каналы утечки видовой информации

14. Электронные устройства негласного получения информации
15. Радиоконтроль (радиомониторинг) эфира и линий
16. Активные методы выявления электронных устройств негласного получения информации
17. Методы неразрушающего контроля. Метод оптической локации. Метод нелинейной локации. Рефлектометрический метод
18. Методика оценки защищенности интерфейсов ТС ОПИ от утечки конфиденциальной информации за счет побочных электромагнитных излучений
19. Средства активной защиты информации, обрабатываемой техническими средствами обработки и передачи информации
20. Методика оценки защищенности интерфейсов ТС ОПИ от утечки конфиденциальной информации за счет наводок побочных электромагнитных излучений
21. Средства пассивной защиты информации, обрабатываемой техническими средствами обработки и передачи информации
22. Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам
23. Средства активной акустической и вибрационной защиты выделенных помещений
24. Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам акустоэлектрических преобразований
25. Средства пассивной защиты технических средств выделенных помещений
26. Организация специальных обследований помещений и специальных проверок технических средств
27. Организация специальных исследований технических средств и помещений

9.2 ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Классификация технических каналов утечки информации
2. Модель технического канала утечки информации
3. Основные характеристики источника информации, среды распространения и приемника информации
4. Каналы утечки видовой информации
5. Электронные устройства негласного получения информации
6. Методы выявления активных ЭУНПИ с передачей информации по радиоканалу (включая сотовые и беспроводные сети) и отходящим линиям. Типовые требования к автоматизированным поисковым комплексам
7. Активные методы выявления ЭУНПИ с дистанционным управлением и пассивных ЭУНПИ в эфире и отходящих линиях. Типовые требования к автоматизированным поисковым комплексам
8. Методы неразрушающего контроля. Метод оптической локации. Метод нелинейной локации. Рефлектометрический метод. Типовые требования к досмотровому оборудованию.
9. Каналы утечки информации, обрабатываемой техническими средствами обработки и передачи информации
10. Электромагнитные каналы утечки информации технических средств обработки и передачи информации
11. Побочные электромагнитные излучения и паразитное электромагнитное излучение
12. Электрические каналы утечки информации технических средств обработки и передачи информации
13. Наводки побочных электромагнитных излучений
14. Средства защиты информации от утечки по электромагнитным и электрическим каналам
15. Средства активной защиты информации, обрабатываемой техническими средствами

обработки и передачи информации
16. Средства пассивной защиты информации, обрабатываемой техническими средствами обработки и передачи информации
17. Методы и средства измерения уровня защищённости от утечки по электромагнитным и электрическим каналам. Типовые требования к автоматизированным комплексам
18. Каналы утечки акустической речевой информации
19. Акустические, виброакустические (вибрационные), оптико-электронные (лазерные) каналы утечки акустической речевой информации
20. Акустоэлектрические каналы утечки акустической речевой информации. Классификация акустоэлектрических преобразователей. Модуляция побочных электромагнитных излучений и паразитного электромагнитного излучения акустическими сигналами.
21. Параметрические каналы утечки акустической речевой информации: ВЧ-облучение, ВЧ-прокачка, ВЧ-навязывание.
22. Средства активной акустической и вибрационной защиты выделенных помещений
23. Средства пассивной защиты технических средств выделенных помещений
24. Методы и средства измерения уровня защищённости акустической речевой информации. Типовые требования к автоматизированным комплексам
25. Характеристика режимов обработки информации средств вычислительной техники при проведении специальных исследований
26. Цель и предназначение специальных исследований. Требования к порядку проведения специальных исследований средств вычислительной техники
27. Методика оценки защищенности интерфейсов ТС ОПИ от утечки конфиденциальной информации за счет побочных электромагнитных излучений. Разработка протокола.
28. Методика оценки защищенности интерфейсов ТС ОПИ от утечки конфиденциальной информации за счет наводок побочных электромагнитных излучений. отчетных документов по результатам выполненных работ
29. Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. отчетных документов по результатам выполненных работ
30. Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам акустоэлектрических преобразований. отчетных документов по результатам выполненных работ
31. Порядок проведения специальных проверок технических средств. отчетных документов по результатам выполненных работ
32. Порядок проведения специальных обследований помещений. отчетных документов по результатам выполненных работ

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Теоретические основы возникновения технических каналов утечки информации Тема 1. Классификация и основные характеристики технических каналов утечки информации	Подготовка к лекции, подготовка к сдаче зачёта	2	Тесты перед лекцией, зачёт, экзамен
Раздел 1. Тема 2. Каналы утечки информации, обрабатываемой техническими средствами обработки и передачи информации	Подготовка к лекции, подготовка к сдаче зачёта	2	Тесты перед лекцией, зачёт, экзамен
Раздел 1. Тема 3. Каналы утечки акустической речевой информации	Подготовка к лекции, подготовка к сдаче зачёта	2	Тесты перед лекцией, зачёт, экзамен
Раздел 1 Тема 4. Каналы утечки видовой информации	Подготовка к лекции, подготовка к сдаче зачёта	2	Тесты перед лекцией, зачёт, экзамен
Раздел 2. Основные методы и инструментальные средства контроля защищённости информации. Тема 5. Методы и инструментальные средства контроля защищённости информации для обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации	Подготовка к лекции, подготовка к лабораторным работам, подготовка к сдаче зачёта	4	Тесты перед лекцией, тесты и вопросы в ходе проведения лабораторных работ, зачёт, экзамен
Раздел 2. Тема 6. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации.	Подготовка к лекции, подготовка к лабораторным работам, подготовка к сдаче зачёта	4	Тесты перед лекцией, тесты и вопросы в ходе проведения лабораторных работ, зачёт, экзамен
Раздел 2. Тема 7. Методы и средства обнаружения технических каналов утечки информации за счет электронных	Подготовка к лекции, подготовка к лабораторным работам, подготовка к сдаче зачёта	4	Тесты перед лекцией, тесты и вопросы в ходе проведения лабораторных работ, зачёт, экзамен

устройств негласного получения информации.			
Раздел 2. Тема 8. Методы и средства выявления электромагнитных каналов утечки информации технических средств обработки и передачи информации	Подготовка к лекции, подготовка к лабораторным работам, подготовка к сдаче зачёта	2	Тесты перед лекцией, тесты и вопросы в ходе проведения лабораторных работ, зачёт, экзамен
Раздел 2. Тема 9. Методы и средства выявления электрических каналов утечки информации технических средств обработки и передачи информации	Подготовка к лекции, подготовка к лабораторным работам, подготовка к сдаче экзамена	2	Тесты перед лекцией, тесты и вопросы в ходе проведения лабораторных работ, зачёт, экзамен
Раздел 2. Тема 10. Методы и средства выявления каналов утечки акустической речевой информации	Подготовка к лекции, подготовка к лабораторным работам, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты и вопросы в ходе проведения лабораторных работ, зачёт, экзамен
Раздел 3. Основные мероприятия по выявлению технических каналов утечки информации. Тема 11. Организация специаль-ных обследований помещений и специ-альных проверок технических средств	Подготовка к лекции, подготовка к лабораторным работам, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты и вопросы в ходе проведения лабораторных работ, зачёт, экзамен
Раздел 3. Тема 12. Организация специаль-ных исследований технических средств и помещений	Подготовка к лекции, подготовка к лабораторным работам, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты и вопросы в ходе проведения лабораторных работ, зачёт, экзамен

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М.: Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - URL: http://www.studentlibrary.ru/book/ISBN9785991204705.html

2. Коваленко, Ю. И. Правовой режим лицензирования и сертификации в сфере информационной безопасности: учебное пособие/ Коваленко Ю.И.-Москва: Горячая линия - Телеком, 2012. - 140 с. - ISBN 978-5-9912-0261-9. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785991202619.html

3. Методы и средства защиты информации в государственном управлении / Царегородцев А. В., Тараскин М. М. - Москва: Проспект, 2017. - 208 с. - ISBN 978-5-392-20353-6. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785392203536.html

Дополнительная

1. Бузов Г.А., Практическое руководство по выявлению специальных технических средств несанкционированного получения информации/ Бузов Г.А. - М.: Горячая линия - Телеком, 2010. - 240 с. - ISBN 978-5-9912-0121-6 - URL:http://www.studentlibrary.ru/book/ISBN9785991201216.html

2. Некоммерческая интернет-версия СПС "КонсультантПлюс":

2.1 Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне». - URL: http://www.consultant.ru/document/cons_doc_LAW_2481/

2.2 Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации» - URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

2.3 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации") - URL: http://www.consultant.ru/document/cons_doc_LAW_208191/

2.4 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. - URL: http://www.consultant.ru/document/cons_doc_LAW_147084/

учебно-методическая

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Инструментальные средства контроля защищённости информации» для студентов специалитета по специальностям 10.05.03 очной формы обучения / А. М. Иванцов; УлГУ, ФМИиАТ. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 311 КБ). - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/8278

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. / _____ / 04.05.2023 /
должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2023]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство «ЮРАЙТ». – Москва, [2023]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО «Политехресурс». – Москва, [2023]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО «Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг». – Москва, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС «Лань». – Санкт-Петербург, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. / ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Инженер ведущий	/ Щуренко Ю.В.	/	/ 04.05.2023
Должность сотрудника УИТТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

- мультимедийные средства: компьютер и проектор;
- мультимедийные технологии. MS Office, Internet Explorer;
- система защиты конфиденциальной информации и персональных данных «Secret Disk. Базовый комплект с USB-ключом – 4 комплекта;
- электронный замок "Соболь" – 3 комплекта;
- персональные средства аутентификации и защищённого хранения данных - USB-ключи и смарт-карты eToken – 3 комплекта;
- система защиты от НСД «Dallas Lock». 4 комплекта;
- программно-аппаратный комплекс средств защиты информации от НСД “Аккорд–АМДЗ” – 1 комплект.

Аудитория для проведения занятий - 2/24б.

Аудитория 2/24б укомплектована специализированной мебелью, учебной доской, имеются мульт мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающимся) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических возможностей:

– для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик: _____ доцент кафедры Иванцов Андрей Михайлович
подпись должность ФИО