УТВЕРЖДЕНО
решением Ученого совета факультета математики,
информационных и авиационных технологий
от «_16_» __05_____2023_ г., протокол №_4/23_
Председатель _____М.А. Волков___
(подпись, расшифровка подписи)
«_16_»__05_____ 2023___г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Защита информации от утечки по техническим каналам
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	3

Специальность: 10.05.01 "Компьютерная безопасность"
код направления (специальности), полное наименование

Специализация: "Математические методы защиты 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.

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:

Учебная дисциплина «Защита информации от утечки по техническим каналам» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Основной целью освоения дисциплины «Защита информации от утечки по техническим каналам» является формирование у студентов знаний по основам технической защиты информации, а также навыков и умений в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач технической защиты информации с учетом требований системного подхода.

Задачи освоения дисциплины:

Основные задачи дисциплины – дать знания:

- по концепции и организационным основам инженерно-технической защиты информации;
- теоретическим и физическим основам технической защиты информации;
- по техническим средствам добывания и защиты информации;
- по методическому обеспечению технической защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Защита информации от утечки по техническим каналам» изучается в 6 семестре и относится к обязательным дисциплинам блока Б1 специальности 10.05.01 – «Компьютерная безопасность».

Курс учебной дисциплины тесно связан с другими учебными дисциплинами, в первую очередь с курсами «Физика», «Электроника и схемотехника», «Безопасность операционных систем», «Основы информационной безопасности», позволяющими понять физическую сущность возникновения технических каналов утечки информации, возможности современных средств технической разведки, методы и способы защиты от утечки по техническим каналам.

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

знание базовых понятий в области физики, вычислительной техники, электроники и схемотехники;

способность использовать нормативные правовые документы;

способность анализировать 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: «Системы и сети передачи информации»; «Модели безопасности компьютерных систем»; «Защита в операционных системах».

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**
ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	**Знать:** основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации **Уметь:** применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации **Владеть:** навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации
ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знать:** порядок организации защиты 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 **Уметь:** организовывать 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 **Владеть:** навыками организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами
ОПК-9 - Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств	**Знать:** основные задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации **Уметь:** решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации **Владеть:**

защиты информации от утечки по техническим каналам, сетей и систем передачи информации	навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий

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**		
		6 семестр		
Контактная работа обучающихся с преподавателем	72/72*	72/72*		
Аудиторные занятия:	72/72*	72/72*		
Лекции	18/18*	18/18*		
Практические и семинарские занятия	18/18*	18/18*		
Лабораторные работы (лабораторный практикум)	36/36*	36/36*		
Самостоятельная работа	72	72		
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 - рефераты на заданные темы		
Курсовая работа	Дифференцированный зачёт	Дифференцированный зачёт		
Виды промежуточной аттестации (экзамен, зачет)	экзамен 36	экзамен 36		
Всего часов по дисциплине:	180 с экзаменом	180 с экзаменом		

* 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	Практ. занятия, семинары	Лабораторные работы			
Раздел 1. Основы технической защиты информации							
1. Концепция технической защиты информации	8	2	2			4	Тесты Т1, реферат № 1)
2. Физические основы утечки информации за счет побочных излучений и наводок	10	2	4			4	Тесты Т2, реферат (№ 2,3)
3. Основные направления технической защиты информации в организации	6	2				4	Тесты Т3, реферат (№ 5,10)
Раздел 2. Технические каналы утечки информации							
4. Типовая структура и виды технических каналов утечки информации	8	2	2			4	Тесты Т4, реферат (№ 7,9)
5. Акустические, виброакустические и оптические каналы утечки информации	8	2	2			4	Тесты Т5, реферат (№ 3,7)
6. Электромагнитные каналы утечки информации	8	2	2			4	Тесты Т6, реферат (№ 2,6)
Раздел 3. Методы и средства защиты информации от утечки по техническим каналам							
7. Методы и средства защиты информации от утечки в электромагнитном канале	32	2	2	12		16	Тесты Т7, реферат (№ 1,2), лаб. Раб № 1,2
8. Методы и средства защиты информации от утечки в акустическом (виброакустическом) канале	18	2	2	6		8	Тесты Т8, реферат (№ 3), лаб. Раб № 3

9. Мероприятия по выявлению средств технической разведки. Методика поиска специальных технических средств	46	2	2	18	18	24	Тесты Т9, реферат (№ 4,8), лаб. Раб № 4,5,6
Итого:	144	18	18	36	18	72	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Основы технической защиты информации

Тема 1. Концепция технической защиты информации

Обобщённая структура государственной системы защиты информации. Основные документы по противодействию иностранным техническим разведкам. Концепция технической защиты информации. Основные положения системного подхода к технической защите информации. Модель системы защиты информации (СЗИ).

Тема 2. Физические основы утечки информации за счет побочных излучений и наводок

Функциональные и случайные опасные сигналы. Источники опасных сигналов. Побочные электромагнитные излучения и наводки (ПЭМИН) как физическая основа возникновения случайных опасных сигналов. Побочные преобразования акустических сигналов в электрические. Паразитные связи и наводки. Низкочастотные и высокочастотные излучения технических средств. Электромагнитные излучения сосредоточенных и распределённых источников**.** Утечка информации по цепям электропитания. Утечка информации по цепям заземлений.

Тема 3. Основные направления технической защиты информации в организации

Основные факторы обеспечения защиты информации от угроз утечки информации. Этапы процесса утечки информации. Основные направления защиты: физическая защита; скрытие информации; нейтрализация источников опасных сигналов. Основные методы технической защиты информации: инженерная защита; техническая охрана объектов; пространственное (структурное, временное и энергетическое) скрытие.

Раздел 2. Технические каналы утечки информации

Тема 4. Типовая структура и виды технических каналов утечки информации

Типовая структура и виды технических каналов утечки информации (ТКУИ). Классификация ТКУИ. Основные показатели ТКУИ.

Тема 5. Акустические, виброакустические и оптические каналы утечки информации.

Понятие и основные характеристики акустического, виброакустического и оптического каналов утечки информации. Пассивные и активные способы защиты информации в выделенных помещениях от несанкционированного прослушивания. Рекомендации по выбору систем акустической и виброакустической защиты. Характеристика и противодействие оптическим каналам утечки информации. Средства противодействия наблюдению в оптическом диапазоне.

Тема 6. Электромагнитные каналы утечки информации, образуемые средствами вычислительной техники.

Характеристика режимов обработки информации в ПЭВМ с точки зрения утечки информации. Режим вывода информации на экран монитора. Потенциально информативные и неинформативные излучения. Условия возникновения электромагнитного канала утечки информации. Электрические каналы утечки информации. Сосредоточенные и распределённые случайные антенны. Специально создаваемые

технические каналы утечки информации. Аппаратные закладки для перехвата изображений, выводимых на экран монитора. Аппаратные закладки для перехвата информации, записываемой на жёсткий диск. Программные закладки.

Раздел 3. Методы и средства защиты информации от утечки по техническим каналам

Тема 7. Методы и средства защиты информации от утечки в электромагнитном канале

Методы пассивной и активной защиты. Экранирование, зашумление и фильтрация опасных сигналов. Методы и средства измерения уровня защищённости от утечки по электромагнитному каналу.

Тема 8. Методы и средства защиты информации от утечки в акустическом (виброакустическом) канале.

Методы пассивной и активной защиты. Технические средства обнаружения утечки информации по акустическому (виброакустическому) каналу. Средства противодействия перехвату «информации по акустовибрационному каналу.

Тема 9. Мероприятия по выявлению средств технической разведки. Методика поиска специальных технических средств.

Средства технической разведки. Мероприятия по выявлению средств технической разведки. Специальные технические средства (СТС). Методика поиска СТС. Радиомониторинг. Локализация радиоизлучающих СТС. Проверка наличия инфракрасных (ИК) излучений. Выявление низкочастотных (НЧ) магнитных полей. Проверка электросети и телефонных коммуникаций. Проверка помещения на наличие акустических каналов утечки. Физический поиск СТС.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Темы семинарских занятий:

Раздел 1. Основы технической защиты информации

Тема 1. Концепция технической защиты информации (семинар).

1. Обобщённая структура государственной системы защиты информации. Основные документы по противодействию иностранным техническим разведкам.
2. Концепция технической защиты информации.
3. Основные положения системного подхода к технической защите информации.
4. Модель системы защиты информации (СЗИ).

Тема 2. Физические основы утечки информации за счет побочных излучений и наводок (семинар).

1. Опасные сигналы и их источники.
2. Побочные электромагнитные излучения и наводки.

Раздел 2. Технические каналы утечки информации

Тема 4. Типовая структура и виды технических каналов утечки информации (семинар).

1. Типовая структура и виды технических каналов утечки информации.
2. Классификация технических каналов утечки информации.
3. Основные показатели технических каналов утечки информации.

Тема 5. Акустические, виброакустические и оптические каналы утечки информации (семинар).

1. Характеристика и противодействие акустическим каналам утечки информации.
2. Характеристика и противодействие оптическим каналам утечки информации.

Тема 6. Электромагнитные каналы утечки информации, образуемые средствами

вычислительной техники (семинар).

1. Характеристика режимов обработки информации в ПЭВМ с точки зрения утечки информации.
2. Потенциально информативные и неинформативные излучения.
3. Электрические каналы утечки информации.
4. Специально создаваемые технические каналы утечки информации.

Раздел 3. Методы и средства защиты информации от утечки по техническим каналам

Тема 7. Методы и средства защиты информации от утечки в электромагнитном канале (семинар).

1. Методы и средства пассивной и активной защиты от утечки в электромагнитном канале.
2. Экранирование, зашумление и фильтрация опасных сигналов.
3. Методы и средства измерения уровня защищённости от утечки по электромагнитному каналу.

Тема 8. Методы и средства защиты информации от утечки в акустическом (виброакустическом) канале (семинар).

1. Методы пассивной и активной защиты.
2. Технические средства обнаружения утечки информации по акустическому (виброакустическому) каналу.
3. Средства противодействия перехвату «информации по акустовибрационному каналу.

Тема 9. Мероприятия по выявлению средств технической разведки. Методика поиска специальных технических средств (семинар).

1. Средства технической разведки. Мероприятия по выявлению средств технической разведки.
2. Специальные технические средства (СТС). Методика поиска СТС.
3. Технические средства для проведения радиомониторинга помещений.
4. Приборы для выявления акустических (виброакустических) каналов утечки.
5. Досмотровая техника для осуществления физического поиска СТС.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 3. Методы и средства защиты информации от утечки по техническим каналам

Тема 7. Методы и средства защиты информации от утечки в электромагнитном канале

Лабораторная работа № 1 (2 часа). «Защита каналов передачи информации генератором шума «Гром-ЗИ-4».

Цель работы: Ознакомление с техническими характеристиками генератора шума «Гром-ЗИ-4», изучение правил его эксплуатации и получение практических навыков работы с генератором шума Гром-ЗИ-4».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с генератором шума Гром-ЗИ-4».

Лабораторная работа № 2. (10 часов). «Ознакомление с техническими характеристиками селективного микровольтметра В6-9».

Цель работы: Получение практических навыков в работе с селективным микровольтметром в ходе измерения опасных сигналов.

Методические указания: основное внимание должно быть уделено практическим навыкам работы с селективным микровольтметром В6-9.

Тема 8. Методы и средства защиты информации от утечки в акустическом (виброакустическом) канале.

Лабораторная работа № 3 (6 часов). «Исследование акустического зашумления помещения».

Цель работы: Исследование возможностей генератора шума SI-3010, получение практических навыков в работе по акустическому зашумлению помещения.

Методические указания: основное внимание должно быть уделено практическим навыкам в работе по акустическому зашумлению помещения.

Тема 9. Мероприятия по выявлению средств технической разведки. Методика поиска специальных технических средств.

Лабораторная работа № 4 (2 часа). «Обнаружение и локализация передающих радиосредств с помощью детектора поля D 006».

Цель работы: Ознакомление с техническими характеристиками изделия D 006, изучение правил эксплуатации изделия D 006, получение практических навыков работы с изделием.

Методические указания: основное внимание должно быть уделено практической эксплуатации в ходе обнаружение и локализация передающих радиосредств с помощью детектора поля D 006.

Лабораторная работа № 5 (6 часов). «Обнаружение радиозлучающих устройств с использованием сканирующего радиоприемника AR-3000A».

Цель работы: Ознакомление с техническими характеристиками изделия AR-3000A, изучение правил эксплуатации изделия, получение практических навыков работы с изделием.

Лабораторная работа № 6 (10 часов). «Изучение методов поиска и локализации специальных технических средств с использованием прибора ST-032 Пиранья».

Цель работы: Изучить возможности прибора ST-032 «Пиранья» и научиться осуществлять поиск и локализацию специальных технических средств несанкционированного получения информации.

Методические указания: основное внимание должно быть уделено практической эксплуатации в ходе поиска и локализации специальных технических средств несанкционированного получения информации.

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 Контрольные работы не предусмотрены учебным планом дисциплины.

8.2 Примерная тематика рефератов:

1. Основные показатели эффективности добывания информации.
2. Способы и средства дезинформирования при противодействии радиолокационному наблюдению.
3. Основные характеристики средств визуальной разведки.
4. Условия и способы эффективного акустического зашумления речевой информации в помещении.
5. Сравнительный анализ характеристик средств обнаружения радиозакладок.

6. Скремблеры как техническое средство защиты информации.
7. Нелинейные локаторы и их применение.
8. Классификация способов нейтрализации закладных устройств.
9. Характеристики экранов, влияющие на эффективность электромагнитного экранирования.
10. Требования к цепям заземления и способы их реализации.

8.2.1 Правила оформления рефератов

1. Объём реферата 7-10 листов печатного текста. К оформлению рефератов предъявляются такие же требования, как и к курсовым работам для студентов 3 курса, описанные в учебно-методическом пособии: Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» / А.С. Андреев, А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

8.3 Примерная тематика курсовых работ:

1. Проблемы энергетического скрытия речевой информации в телефонных линиях связи и принципы их решения.
2. Анализ электромагнитных каналов утечки информации.
3. Анализ акустических каналов утечки информации.
4. Анализ эффективности использования физических средств защиты.
5. Принципы обнаружения и локализации радиозакладок.
6. Сравнительный анализ характеристик средств обнаружения радиозакладок.
7. Оптические каналы утечки информации и их локализация.
8. Реализация защиты информации от утечки через ПЭМИН.
9. Предотвращение утечки информации по цепям электропитания и заземления.
10. Способы увеличения дальности скрытного наблюдения в оптическом видимом и инфракрасном диапазонах.

8.3.1 Правила оформления курсовых работ

Требования к курсовым работам для студентов отражены в учебно-методическом пособии: Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» / А.С. Андреев, А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Обобщённая структура государственной системы защиты информации. Основные документы по противодействию иностранным техническим разведкам
2. Концепция технической защиты информации.
3. Основные положения системного подхода к технической защите информации.
4. Модель системы защиты информации.
5. Опасные сигналы (функциональные и случайные) и их источники.
6. Побочные электромагнитные излучения и наводки. Побочные преобразования акустических сигналов в электрические сигналы.
7. Побочные электромагнитные излучения и наводки. Паразитные связи и наводки.
8. Побочные электромагнитные излучения и наводки. Низкочастотные и высокочастотные излучения технических средств.

9. Побочные электромагнитные излучения и наводки. Электромагнитные излучения сосредоточенных и распределённых источников.

10. Побочные электромагнитные излучения и наводки. Утечка информации по цепям электропитания и заземления.

11. Основные факторы обеспечения защиты информации от угроз утечки информации.

12. Классификация направлений и методов инженерно-технической защиты информации.

13. Типовая структура и виды технических каналов утечки информации.

14. Классификация технических каналов утечки информации.

15. Основные показатели технических каналов утечки информации.

16. Характеристика и противодействие акустическим каналам утечки информации. Пассивные и активные способы защиты речи от несанкционированного прослушивания.

17. Характеристика и противодействие оптическим каналам утечки информации. Пассивные и активные способы защиты информации от несанкционированного наблюдения.

18. Характеристика режимов обработки информации в ПЭВМ с точки зрения утечки информации.

19. Потенциально информативные и неинформативные излучения.

20. Электрические каналы утечки информации.

21. Специально создаваемые технические каналы утечки информации.

22. Методы и средства пассивной и активной защиты от утечки в электромагнитном канале.

23. Экранирование, зашумление и фильтрация опасных сигналов.

24. Методы и средства измерения уровня защищённости от утечки по электромагнитному каналу.

25. Методы пассивной и активной защиты утечки информации по акустическому (виброакустическому) каналу.

26. Технические средства обнаружения утечки информации по акустическому (виброакустическому) каналу.

27. Средства противодействия перехвату «информации по акустовибрационному каналу.

28. Средства технической разведки. Мероприятия по выявлению средств технической разведки.

29. Специальные технические средства (СТС). Методика поиска СТС.

30. Технические средства для проведения радиомониторинга помещений.

31. Приборы для выявления акустических (виброакустических) каналов утечки.

32. Досмотровая техника для осуществления физического поиска специальных технических средств (СТС).

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Основы технической защиты информации Тема 1. Концепция технической защиты информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 1. Тема 2. Физические основы утечки информации за счет побочных излучений и наводок	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 1. Тема 3. Основные направления технической защиты информации в организации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Технические каналы утечки информации Тема 4. Типовая структура и виды технических ка-налов утечки информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Тема 5. Акустические, виброакустические и оптические каналы утечки информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Тема 6. Электромагнитные каналы утечки информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 3. Методы и средства защиты информации от утечки по техническим каналам Тема 7. Методы и средства защиты информации от утечки в электромагнитном канале	Подготовка к занятию, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	16	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 3. Тема 8. Методы и средства защиты информации от утечки в акустическом (виброакустическом) канале	Подготовка к занятию, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	8	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 3. Тема 9. Мero-	Подготовка к занятию,	24	Тесты перед

приятия по выявлению средств технической разведки. Методика поиска специальных технических средств	подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена		лекцией, тесты на семинаре, вопросы на лабораторной работе, 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. Бузов Г.А., Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов - М.: Горячая линия - Телеком, 2015. – 586 с. - ISBN 978-5-9912-0424-8 - URL: http://www.studentlibrary.ru/book/ISBN9785991204248.html

3. Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва: РУТ (МИИТ), 2019. — 144 с. — ISBN 978-5-7876-0326-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/188703

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/

3 Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268

учебно-методическая

1.Методические указания для самостоятельной работы студентов по дисциплине «Защита информации от утечки по техническим каналам» для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов; УлГУ, ФМИиАТ. - Ульяновск : УлГУ, 2021. - 21 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/10730

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