УТВЕРЖДЕНО
решением Ученого совета факультета математики, информационных и авиационных технологий
от «21» 06 2019 г., протокол №5/19
Председатель _____ М.А. Волков
(подпись, расшифровка подписи)
«21» 06 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Техническая защита информации
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 2018 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	СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину	Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
_____ / Андреев А.С. / *(подпись) (Ф.И.О.)* «19» 06 2019 г.	_____ / Андреев А.С. / *(подпись) (Ф.И.О.)* «19» 06 2019 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Учебная дисциплина «Техническая защита информации» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Основной целью освоения дисциплины «Техническая защита информации» 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 «Техническая защита информации» изучается в 6 семестре и относится к базовой части дисциплин блока Б1.Б специальности 10.05.01 – «Компьютерная безопасность».

Курс учебной дисциплины тесно связан с другими учебными дисциплинами, в первую очередь с курсами «Физика», «Электроника и схемотехника», «Аппаратные средства вычислительной техники», «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-1- Способность анализировать физические явления и процессы при решении профессиональных задач	**Знать:** Основные физические явления и процессы при решении профессиональных задач **Уметь:** анализировать физические явления и процессы при решении профессиональных задач **Владеть:** навыками анализа физических явлений и процессов при решении профессиональных задач
ПК-11 - способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты инфор-мации в компьютерных системах по требованиям безопасности информации	**Знать:** организацию защиты информации от утечки по техническим каналам на объектах информатизации; технические каналы утечки информации **Уметь:** пользоваться нормативными документами по противодействию технической разведке **Владеть:** методами технической защиты информации; методами расчета и инструментального контроля основных показателей технической защиты информации
ПК-19 - способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации	**Знать:** возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации **Уметь:** использовать типовые приборы для выявления и защиты основных каналов утечки информации **Владеть:** средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации

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 ___*дневная*_____)**			
	Всего по плану	**В т.ч. по семестрам**		
		6 семестр		
1	2	3	4	5
Контактная работа обучающихся с преподавателем	54	54/54		

1	2	3	4	5
Аудиторные занятия:	54	54/54		
Лекции	18	18/18		
Практические и семинарские занятия	18	18/18		
Лабораторные работы (лабораторный практикум)	18	18/18		
Самостоятельная работа	90	90		
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 (курсовых) 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 дневная

Название разделов и тем	Все-го	Виды учебных занятий					
		Аудиторные занятия			Занятия в ин-терактивной форме	Са-мостоя-тельная работа	Форма текущего контроля знаний
		Лекции	Практ. занятия, семинары	Лабораторные работы			
1	2	3	4	5	6	7	8
Раздел 1. Основы технической защиты информации							
1. Концепция технической защиты информации	10	2	2			6	Тесты Т1, реферат № 1)
2. Физические основы утечки информации за счет побочных излучений и наводок	16	2	4			10	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	12	2	2			8	Тесты Т4, реферат (№ 7,9)
5. Акустические, виброакустические и оптические каналы утечки информации	12	2	2			8	Тесты Т5, реферат (№ 3,7)
6. Электромагнитные каналы утечки информации	12	2	2			8	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	24	2	2	6	6	14	Тесты Т7, реферат (№ 1,2), лаб. Раб № 1,2
8. Методы и средства защиты информации от утечки в акустическом (виброакустическом) канале	20	2	2	4	4	12	Тесты Т8, реферат (№ 3), лаб. Раб № 3

1	2	3	4	5	6	7	8
9. Мероприятия по выявлению средств технической разведки. Методика поиска специальных технических средств	32	2	2	8	8	20	Тесты Т9, реферат (№ 4,8), лаб. Раб № 4,5,6
Итого:	144	18	18	18	18	90	

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 (4 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. (2 часа). «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 (4часа). «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 (2 часа). «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 (4 часа). «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
1	2	3	4
Раздел 1. Основы технической защиты информации (ЗИ) Тема 1. Концепция технической ЗИ	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	6	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	10	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 каналов утечки информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	8	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	8	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	8	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	14	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	12	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 3. Тема 9. Мероприятия по выявлению средств технической разведки. Методика поиска специальных технических средств	Подготовка к занятию, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	20	Тесты перед 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 [Электронный ресурс]: 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 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html.

2. Бузов Г.А., Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс] / Г.А. Бузов - М.: Горячая линия - Телеком, 2015. – 586 с. - ISBN 978-5-9912-0424-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204248.html

3. Свинарев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: учеб. пособие / Свинарев Н.А., Ланкин О.В., Данилкин А.П, Потехецкий С.В., Перетокин О.И. - Воронеж: ВГУИТ, 2013. - 192 с. - ISBN 978-5-00032-018-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785000320181.html

дополнительная

1. Бузов Г.А., Практическое руководство по выявлению специальных технических средств несанкционированного получения информации [Электронный ресурс] / Бузов Г.А. - М.: Горячая линия - Телеком, 2010. - 240 с. - ISBN 978-5-9912-0121-6 - Режим доступа: 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». Режим доступа: 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»
Режим доступа: 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")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

2.4 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/

учебно-методическая

1. 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: http://lib.ulsu.ru/MegaPro/Download/MObject/297

2. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", «Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", «Системный анализ и управление» / А.С. Андреев, С.М. Бородин, А.М. Иванцов. - Ульяновск: УлГУ, 2015. 54 с.

3. Иванцов А. М.
Методические указания для самостоятельной работы студентов по дисциплине «Техническая защита информации» для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск: УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 327 КБ). - Текст : электронный.
http://lib.ulsu.ru/MegaPro/Download/MObject/4971

Согласовано:
Гл. библ-рь НБ Ул / Попова И.Ю / / 14.06.2019
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. **IPRbooks** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов, [2019]. - Режим доступа: http://www.iprbookshop.ru.
1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://www.biblio-online.ru.
1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://www.studentlibrary.ru/pages/catalogue.html.
1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: https://e.lanbook.com.
1.5. **Znanium.com** [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://znanium.com.
2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва: КонсультантПлюс, [2019].
3. **База данных периодических изданий** [Электронный ресурс]: электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: https://dlib.eastview.com/browse/udb/12.
4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://нэб.рф.
5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://dvs.rsl.ru.
6. Федеральные информационно-образовательные порталы:
6.1. Информационная система Единое окно доступа к образовательным ресурсам.

Режим доступа: http://window.edu.ru

6.2. Федеральный портал Российское образование. Режим доступа: http://www.edu.ru

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : http://lib.ulsu.ru/MegaPro/Web

7.2. Образовательный портал УлГУ. Режим доступа : http://edu.ulsu.ru

8. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

Согласовано:

Зам. нач. УИиТ /Клочкова А.В. 14.06.2019

Должность сотрудника УИиТ 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: подпись доцент кафедры должность Иванцов Андрей Михайлович ФИО

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/выпускающей кафедрой	Подпись	Дата
1	Внесение изменений в п.п. 4.2 Объем дисциплины по видам учебной работы п. «Общая трудоемкость дисциплины» с оформлением приложения 1	Андреев А.С.		08.04.2020 Протокол заседания кафедры № 12
2	Внесение изменений в п. 13 «Специальные условия для обучающихся с ограниченными возможностями здоровья» с оформлением приложения 2	Андреев А.С.		08.04.2020 Протокол заседания кафедры № 12
3	Внесение изменений в п/п а) Список рекомендуемой литературы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 3	Андреев А.С.		27.05.2020 Протокол заседания кафедры № 14
4	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 4	Андреев А.С.		27.05.2020 Протокол заседания кафедры № 14

Приложение 1

4.2 Объем дисциплины по видам учебной работы (в часах)

Вид учебной работы	**Количество часов (форма обучения ___*дневная*_____)**			
	Всего по плану	**В т.ч. по семестрам**		
		6 семестр		
1	2	3	4	5
Контактная работа обучающихся с преподавателем	54	54/54*		
Аудиторные занятия:	54	54/54*		
Лекции	18	18/18*		
Практические и семинарские занятия	18	18/18*		
Лабораторные работы (лабораторный практикум)	18	18/18*		
Самостоятельная работа	90	90		
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 (курсовых) 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		

*Количество часов работы ППС с обучающимися в дистанционном формате с применением электронного обучения.

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.

Приложение 2

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

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

Приложение 3

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: 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 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html.

2. Бузов Г.А., Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс] / Г.А. Бузов - М.: Горячая линия - Телеком, 2015. – 586 с. - ISBN 978-5-9912-0424-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204248.html

3. Свинарев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: учеб. пособие / Свинарев Н.А., Ланкин О.В., Данилкин А.П, Потехецкий С.В., Перетокин О.И. - Воронеж: ВГУИТ, 2013. - 192 с. - ISBN 978-5-00032-018-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785000320181.html

дополнительная

1. Бузов Г.А., Практическое руководство по выявлению специальных технических средств несанкционированного получения информации [Электронный ресурс] / Бузов Г.А. - М.: Горячая линия - Телеком, 2010. - 240 с. - ISBN 978-5-9912-0121-6 - Режим доступа: 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». Режим доступа: 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»

Режим доступа: 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")

Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

2.4 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации")

Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/

учебно-методическая

1. 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: http://lib.ulsu.ru/MegaPro/Download/MObject/297

2. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", «Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", «Системный анализ и управление» / А.С. Андреев, С.М. Бородин, А.М. Иванцов. - Ульяновск: УлГУ, 2015. 54 с. http://lib.ulsu.ru/MegaPro/Download/MObject/297/Andreev2015.pdf

3. **Иванцов А. М.**

Методические указания для самостоятельной работы студентов по дисциплине «Техническая защита информации» для студентов специалитета по специальностям

10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск: УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 327 КБ). - Текст : электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/4971

Согласовано:

Гл. библ-рь ИБ УлГУ	Попова И. Ю.		14.06.2019
Должность сотрудника научной библиотеки	ФИО	подпись	дата

Приложение 4

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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. **IPRbooks** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов, [2019]. - Режим доступа: http://www.iprbookshop.ru.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО

1.1. **IPRbooks** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов, [2019]. - Режим доступа: http://www.iprbookshop.ru.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://www.biblio-online.ru.

1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://www.studentlibrary.ru/pages/catalogue.html.

1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: https://e.lanbook.com.

1.5. **Znanium.com** [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://znanium.com.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва: КонсультантПлюс, [2019].

3. **База данных периодических изданий** [Электронный ресурс]: электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: https://dlib.eastview.com/browse/udb/12.

4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://нэб.рф.

5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://dvs.rsl.ru.

6. Федеральные информационно-образовательные порталы:

6.1. Информационная система Единое окно доступа к образовательным ресурсам. Режим доступа: http://window.edu.ru

6.2. Федеральный портал Российское образование. Режим доступа: http://www.edu.ru

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : http://lib.ulsu.ru/MegaPro/Web

7.2. Образовательный портал УлГУ. Режим доступа : http://edu.ulsu.ru

8. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

Согласовано:

Зам. нач. УИиТ / Клочкова А.В. / 14.06.2019

Должность сотрудника УИиТ / ФИО / подпись / дата