Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Амурский государственный университет»

УТВЕРЖДАЮ
Проректор по УиНР
_____ А.В.Лейфа
«__» 09 2021 г.

РАБОЧАЯ ПРОГРАММА

Инженерно-техническая защита информации

Направление подготовки 09.03.02 «Информационные системы и технологии»

Направленность (профиль) образовательной программы «Информационные системы и технологии»

Квалификация выпускника бакалавр

Год набора 2021

Форма обучения очная

Курс 3-4 Семестр 6, 7

Экзамен 6 (семестр) Зачет 7 (семестр)

Общая трудоемкость дисциплины 324 (акад. час.), 9 (з.е.)

Составитель А.В. Бушманов, к.т.н., доцент

Факультет математики и информатики

Кафедра информационных и управляющих систем

2021 г.

Рабочая программа составлена на основании Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 «Информационные системы и технологии», утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017г. № 926.

Рабочая программа обсуждена на заседании кафедры Информационных и управляющих систем

«01» 09 2021 г., протокол № 1

Заведующий кафедрой _____ А.В. Бушманов

СОГЛАСОВАНО
Начальник учебно-методического управления
_____ Н.А.Чалкина
«01» 09 2021 г.

СОГЛАСОВАНО
Заведующий выпускающей кафедры
_____ А.В. Бушманов
«01» 09 2021 г.

СОГЛАСОВАНО
Директор научной библиотеки
_____ О.В.Петрович
«01» 09 2021 г.

СОГЛАСОВАНО
Центр информационных и образовательных технологий
_____ А.А.Тодосейчук
«01» 09 2021 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Цель дисциплины: Целью изучения дисциплины является теоретическая и практическая подготовка студентов по вопросам защиты информации от утечки по инженерно-техническим каналам (техническая защита информации) на объектах информации и в выделенных помещениях.

Задачи дисциплины (модуля):

Изучение технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;

Изучение технических каналов утечки акустической (речевой) информации;

Изучение способов и средств защиты информации, обрабатываемой техническими средствами;

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

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

Освоение основ организации технической защиты информации на объектах информатизации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина относится к федеральному компоненту базового цикла вариативной части Учебного плана, разработанного согласно Федеральному государственному образовательному стандарту высшего образования по направлению подготовки 09.03.02 «Информационные системы и технологии».

Для успешного освоения данной дисциплины необходимы знания, умения и навыки, приобретенные в результате освоения дисциплин по направлению подготовки 09.03.02 «Информационные системы и технологии»: Базы данных; Сети и телекоммуникации; Информационные технологии.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

3.1. Профессиональные компетенции и индикаторы их достижений

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
ПК-9, способен обеспечивать информационную безопасность уровня баз данных.	ИД-1, знать особенности реализации структуры данных и управления данными в установленной БД, принципы и методы взаимодействия БД с устройствами ввода/вывода, типы сбоев и способы их устранения или обхода, полученные из различных источников ИД-2, уметь профессионально работать с устройствами хранения и обработки информации ИД-3, иметь навык быстро находить причины сбоя, анализируя симптомы и просматривая материалы из различных источников и/или руководствуясь собственным опытом

4. СТРУКТУРА ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 акад. часа.

№ п/п	Тема (раздел) дисциплины, курсовая работа (проект), промежуточная аттестация	Семестр	Виды контактной работы и трудоемкость (в академических часах)						Контроль (в академических часах)	Самостоятельная работа (в академических часах)	Формы текущего контроля успеваемости
			Л	ПЗ	ЛР	ИКР	КТО	КЭ			
1	Технические каналы утечки информации.	6	10	-	10					8	
2	Способы и средства защиты информации от утечки по техническим каналам.	6	12	-	12					8	
3	Методы и средства контроля эффективности технической защиты информации.	6	12	-	12					10	
4	Организация технической защиты информации.	7	34	-	34					8	
	Экзамен							0.3	35,7		
	Зачет						0,2				
	Всего:		68	-	68		0,2	0.3	35,7	79,8	

Л – лекция, ПЗ – практическое занятие, ЛР – лабораторная работа, ИКР – иная контактная работа, КТО – контроль теоретического обучения, КЭ – контроль на экзамене.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	Технические каналы утечки информации.	Системный подход к защите информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Распространение сигналов в технических каналах утечки информации. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в светопроводах.

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
		Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.
2	Способы и средства защиты информации от утечки по техническим каналам.	Основные концептуальные положения технической защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Моделирование случайных величин. Законы распределения случайных величин. Статистические оценки и их точность. Аппроксимация результатов статистического моделирования. Основные понятия теории случайных процессов, их классификация и основные характеристики. Марковские процессы с дискретными состояниями. Марковские процессы с дискретными состояниями и непрерывным временем. Стационарные случайные процессы. Моделирование инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Задачи защиты информации ТКС в условиях конфликта. Понятие конфликта. Способы разрешения конфликта в ТКС. Информационный конфликт (виды, варианты реализации). Стратегии противоборствующих сторон в динамике развития информационного конфликта ТКС с системами воздействия. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия.
3	Методы и средства контроля эффективности технической защиты информации.	Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля. Требования по защите информации от утечки по техническим каналам. Виды технического контроля. Показатели эффективности функционирования средств защиты информации в ТКС. Методические рекомендации, по оценке эффективности

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
		защиты информации. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых признаков объектов наблюдения. Способы оценки безопасности речевой информации в помещении. Способы определения уровней опасных сигналов на выходах основных и вспомогательных технических средств. Способы оценки размеров зон I и II.
4	Организация технической защиты информации.	Государственная система защиты информации. Основные задачи, структура и характеристика государственной системы противодействия технической защите. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Физические основы защиты информации от технических разведок. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок. Принципы действия аппаратуры технических разведок. Классификация методов и средств защиты информации от технических разведок. Методы инженерно-технической защиты информации. Классификация методов инженерно-технической защиты информации. Инженерная защита и техническая охрана объектов. Пространственное, энергетическое и структурное скрытие информации и ее носителей. Дезинформирование, как метод скрытия. Математическая модель канала утечки информации применительно к техническим разведкам. Методы скрытия информации и ее носителей Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио и электрических сигналов. Классификация методов инженерной защиты и технической охраны объектов защиты. Инженерные конструкции. Автономные и централизованные системы охраны. Модели злоумышленника. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара. Комплекс технических средств охраны.

5.2. Лабораторные работы

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	Ознакомление с лабораторным стендом.	Понятие о безопасности информации. Показатели оценивания безопасности информации. Аппаратура акустической защиты речевой информации. Проблемы применения. Принципы построения генераторов акустического и вибрационного шумов. Пассивные методы защиты акустической информации. Активные методы защиты акустической информации.
2	Изучение анализатора спектра цифрового интегрирующего «Тритон», подготовка программного изделия к работе.	Запуск программы «Тритон-Интерфейс». Описание интерфейса программы «Тритон-Интерфейс». Подготовка изделия «Тритон» к работе. Сборка базового комплекта изделия. Калибровка изделия. Порядок проведения измерений. Запись входного сигнала в файл. Запись выходного сигнала в файл.
3	Экспериментально-расчетная оценка коэффициентов звуко- и виброизоляции.	Основные характеристики человеческой речи. Основные характеристики звуковых волн. Структурные акустические волны. Опишите экспериментально-расчетную методику оценки звуковой виброизоляции помещений. Поясните принцип выбора контрольных точек для проведения измерений по вибрационному и акустическому каналам.
4	Экспериментально-расчетная оценка разборчивости речи.	Основные характеристики звуковых волн. Структурные акустические волны. Опишите экспериментально-расчетную методику оценки речевой разборчивости. Поясните принцип выбора контрольных точек для проведения виброакустических измерений. Укажите характеристики виброакустического технического канала утечки речевой информации.
5	Экспериментально-расчетная оценка разборчивости речи с использованием автоматизированного программно-аппаратного комплекса.	Виды разборчивости речи. Понятие форманты. Формантное распределение. Опишите экспериментально-расчетную методику оценки речевой разборчивости. Принципы построения генераторов акустического шума. Основные разновидности. Укажите характеристики виброакустического технического канала утечки речевой информации.
6	Исследование акустического и виброакустического каналов утечки информации.	Физические основы акустического канала утечки. Способы пассивной защита акустического ТКУ КИ. Способы активной защиты акустического ТКУ КИ. Как выбираются частоты сигнала при оценке защищенности акустического ТКУ КИ? Что такое октавная полоса звуковых частот? Как образуется виброакустический ТКУ КИ? В чем состоят различия акустического и виброакустического сигналов утечки КИ?

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
		Метод оценки утечки КИ по виброакустическому ТКУ. Достоинства и недостатки пассивных средств защиты КИ. Достоинства и недостатки активных средств защиты речевой КИ.

6. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	Наименование темы (раздела)	Форма (вид) самостоятельной работы	Трудоемкость в академических часах
1	Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.	Проверка домашнего задания.	10
2	Показатели эффективности инженерно-технической защиты информации.	Подготовка к лекциям и лабораторным занятиям.	10
3	Способы оптимизации мер инженерно-технической защиты информации.	Проверка домашнего задания.	10
4	Разрешение конфликта в условиях рефлексивных игр. Разработка матрицы конфликтного взаимодействия для типовых ТКС.	Проверка домашнего задания, допуск к выполнению лабораторной работы.	10
5	Особенности инструментального контроля эффективности инженерно-технической защиты информации.	Работа с учебно-методической литературой.	10
6	Оценка дальности перехвата сигналов.	Проверка домашнего задания.	10
7	Методический подход к оценке эффективности защиты информации от технических разведок.	Проверка домашнего задания.	10
8	Математическая модель канала акустической утечки информации.	Проверка домашнего задания.	9,8
Итого:			79,8

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательный процесс по дисциплине строится на основе комбинации следующих образовательных технологий.

Интегральную модель образовательного процесса по дисциплине формируют технологии методологического уровня: модульно-рейтинговое обучение, технология поэтапно-

го формирования умственных действий, технология развивающего обучения, элементы технологии развития критического мышления.

Реализация данной модели предполагает использование следующих технологий стратегического уровня (задающих организационные формы взаимодействия субъектов образовательного процесса), осуществляемых с использованием определенных тактических процедур:

– лекционные (вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция);

– лабораторные (углубление знаний, полученных на теоретических занятиях, решение задач, практическое применение некоторых теоретических знаний);

– тренинговые (формирование определенных умений и навыков, формирование алгоритмического мышления);

–активизации познавательной деятельности (приемы технологии развития критического мышления через чтение и письмо, работа с литературой, подготовка презентаций по темам домашних работ);

– самоуправления (самостоятельная работа студентов, самостоятельное изучение материала).

Информационные технологии используются при организации коммуникации со студентами для представления информации, выдачи рекомендаций и консультирования по оперативным вопросам (электронная почта), использование мультимедиа-средств при проведении лекционных и практических занятий.

В качестве образовательных технологий при изучении дисциплины используются мультимедийные лекции, на лабораторных занятиях используются современные пакеты программных продуктов, лабораторные стенды. С целью текущего контроля знаний студентов на лабораторных работах проводится контроль выполнения работы. Студентам предлагается обсудить полученные результаты и высказать свое мнение по применению возможных приемов для улучшения показателей либо результатов работы.

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания, типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций, а также методические материалы, определяющие процедуры оценивания знаний, умений и навыков отражены в фонде оценочных средств по дисциплине «Инженерно-техническая защита информации».

Фонд оценочных средств позволяет оценить знания, умения и уровень приобретенных компетенций. Фонд оценочных средств по дисциплине «Инженерно-техническая защита информации» включает:

Вопросы к экзаменам:

1. Дайте общую характеристику способов несанкционированного получения конфиденциальной информации через технические каналы с указанием источников и носителей такой информации.

2. Дайте общую характеристику способов несанкционированного получения конфиденциальной информации через технические каналы с привлечением используемых средств и раскрытием принципов записи и съема информации с носителей.

3.Укажите кардинальные специфические особенности, присущие речевой (акустической) информации.

4. Охарактеризуйте главные аспекты информационной безопасности.

5. Раскройте сущность информационного объекта защиты и приведите перечень мероприятий, необходимых для выявления этого объекта.

6. Дайте определения видов угроз безопасности информации и раскройте сущность этих угроз.

7. Охарактеризуйте естественные и искусственные каналы утечки информации и приведите обоснование экономической эффективности системы защиты.

8. Обоснуйте построение модели угрозы информационной безопасности с представлением технических возможностей нарушителя по перехвату конфиденциальной информации.

9. Перечислите комплекс организационных мер и технических средств, положенных в основу системы защиты информации.

10. Дайте краткие характеристики основным видам средств защиты и приведите перечень типовых задач, которые необходимо решить в результате разработки системы защиты информации.

11. Назовите общие демаскирующие признаки объектов и вкратце охарактеризуйте их.

12.Раскройте сущность опознавательных признаков демаскировки объекта.

13. Охарактеризуйте признаки деятельности, демаскирующие объект, и раскройте сущность дополнительных признаков.

14. Дайте краткую характеристику прямым и косвенным признакам, а также качественным и количественным демаскирующим признакам объектов.

15. Сформулируйте определения акустической разведки, ее физического базиса и слухового анализатора человека.

16. Приведите основные физические характеристики акустических волн.

17. Охарактеризуйте звуковое поле, создаваемое открытой с обеих сторон трубой, как физический базис групповых трубчатых направленных микрофонов.

18. Дайте характеристику скорости звука в твердых телах, жидкостях и газообразных средах и приведите аналитические соотношения.

19. Раскройте понятия громкости звука и его высоты, укажите диапазоны слышимости людей и животных.

20. Приведите математическое описание продольных звуковых волн с раскрытием особенности представления звуковой волны через смещение и давление.

21. Дайте определение интенсивности (силы) звука, получите закон обратных квадратов и выявите связь интенсивности и звукового давления.

22. Обоснуйте применение шкалы децибел при определении уровня громкости звука и объясните необходимость измерения громкости в фонах.

23. Раскройте сущность реверберации как средства акустической маскировки.

24. Укажите особенности распространения структурного звука в зданиях, сооружениях и пассивные способы защиты акустической (речевой) информации от ее утечки через строительные конструкции.

25. Раскройте понятие интерференции звуковых волн и определите условия гашения и усиления звука.

26. Раскройте сущность звуковых биений и приведите необходимые соотношения.

27. Опишите эффект Допплера в акустике и дайте вывод основных формул.

28. Приведите пример использования эффекта Допплера в системе охранной сигнализации.

29. Дайте краткие характеристики современным средствам перехвата конфиденциальной акустической информации: электронным стетоскопам, пьезоакселерометрам, пьезоэлектрическим геофонам и др.

30. Перечислите важные особенности ведения аудиоразведки в помещениях при наличии диффузного звукового поля.

31. Опишите факторы, влияющие на дальность ведения аудиоразведки на открытой местности.

32. Приведите главные технические характеристики направленных микрофонов.

33. Сформулируйте принцип действия направленных микрофонов с параболическим отражателем.

34. Раскройте особенности функционирования трубчатых микрофонов органного типа при двух температурных режимах.

35. Поясните работу микрофонной решетки.

36. Приведите спектральные характеристики акустических речевых сигналов и укажите особенности их восприятия.

37. Рассмотрите функциональные особенности дистанционно управляемых микрофонов, мобильных телефонов и радиозакладок в качестве подслушивающих устройств.

38. Перечислите основные защитные мероприятия от подслушивания и записи конфиденциальной информации и раскройте их сущность.

39. Сформулируйте принципы действия систем поиска и обнаружения закладных устройств – нелинейных радиолокаторов, металлодетекторов, тепловизионных и рентгено-телевизионных систем, подповерхностных локаторов и ультразвуковых систем, – позволяющих выявлять временно отключенные радиозакладки и устройства радиоподслушивания с программным и дистанционным управлением.

40. Охарактеризуйте распространенные способы и устройства подслушивания в телефонных каналах связи.

Вопросы к зачету:

1. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации.

2. Представление сил и средств защиты информации в виде системы.

3. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации.

4. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях.

5. Распространение оптических сигналов в атмосфере и в светопроводах.

6. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.

7. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации.

8. Принципы защиты информации техническими средствами.

9. Основные направления инженерно-технической защиты информации.

10. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации.

11. Демаскирующие признаки объектов наблюдения, сигналов и веществ.

12. Основные теоремы теории вероятностей.

13. Моделирование случайных величин и их законы распределения.

14. Статистические оценки и их точность.

15. Аппроксимация результатов статистического моделирования.

16. Основные понятия теории случайных процессов, их классификация и основные характеристики.

17. Марковские процессы с дискретными состояниями.

18. Марковские процессы с дискретными состояниями и непрерывным временем.

19. Стационарные случайные процессы.

20. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации.

21. Принципы моделирования объектов защиты.

22. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты.

23. Задачи защиты информации ТКС в условиях конфликта.

24. Понятие конфликта. Способы разрешения конфликта в ТКС.

25. Стратегии противоборствующих сторон в динамике развития информационного конфликта ТКС с системами воздействия.

26. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС.

27. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия.

28. Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля.

29. Требования по защите информации от утечки по техническим каналам. Виды технического контроля.

30. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых признаков объектов наблюдения.

31. Способы оценки безопасности речевой информации в помещении.

32. Способы определения уровней опасных сигналов на выходах основных и вспомогательных технических средств.

33. Способы оценки размеров зон I и II.

34. Основные задачи, структура и характеристика государственной системы противодействия технической защите.

35. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации.

36. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок.

37. Принципы действия аппаратуры технических разведок.

38. Классификация методов и средств защиты информации от технических разведок.

39. Классификация методов инженерно-технической защиты информации.

40. Инженерная защита и техническая охрана объектов.

41. Пространственное, энергетическое и структурное скрытие информации и ее носителей.

42. Дезинформирование, как метод скрытия.

43. Математическая модель канала утечки информации применительно к техническим разведкам.

44. Пространственное скрытие объектов наблюдения и сигналов.

45. Структурное и энергетическое скрытие объектов наблюдения.

46. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение.

47. Энергетическое скрытие радио и электрических сигналов.

48. Классификация методов инженерной защиты и технической охраны объектов защиты.

49. Инженерные конструкции. Автономные и централизованные системы охраны

50. Модели злоумышленника.

51. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления.

52. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара.

53. Комплекс технических средств охраны.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) литература:

Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник / О.В. Прохорова. — Электрон. текстовые данные. — Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. — 978-5-9585-0603-3. — Режим доступа: http://www.iprbookshop.ru/43183.html

Внуков, А. А. Защита информации: учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772

Иванов, А. В. Защита речевой информации от утечки по акустоэлектрическим каналам: учебное пособие / А. В. Иванов, В. А. Трушин. — Новосибирск: Новосибирский государственный технический университет, 2012. — 43 с. — ISBN 978-5-7782-1888-8

Сагдеев К.М. Физические основы защиты информации [Электронный ресурс] : учебное пособие / К.М. Сагдеев, В.И. Петренко, А.Ф. Чипига. — Электрон. текстовые данные. — Ставрополь: Северокавказский федеральный университет, 2015. — 394 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63152.html

Петренко, В. И. Теоретические основы защиты информации: учебное пособие / В. И. Петренко. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 222 с. — ISBN 2227-8397.

б) программное обеспечение и Интернет-ресурсы:

Перечень программного обеспечения:

№	Перечень программного обеспечения (обеспеченного лицензией)	Реквизиты подтверждающих документов
1	Операционная система MS Windows 7 Pro, Операционная система MS Windows XP SP3	DreamSpark Premium Electronic Software Delivery (3 years) договору – Сублицензионный договор №Tr000074357/KHB 17 от 01 марта 2016 года
2	Операционная система MS Windows 10 Education, Pro	DreamSpark Premium Electronic Software Delivery (3 years) договору – Сублицензионный договор №Tr000074357/KHB 17 от 01 марта 2016 года
3	MS office 2010 standard	Лицензия Microsoft office 2010 Standard RUS OLM ML Academic 50,договор №492 от 28 июня 2012 года
4	MS Office 2013/2016 PRO PLUS Academic	Сублицензионный договор № Tr000027462 от 10.12.2015
5	MS Access 2007, 2010, 2013, 2016 MS Visio 2007, 2010, 2013, 2016 MS InfoPath 2007, 2010, 2013, 2016 MS OneNote 2007, 2010, 2013, 2016 MS Project 2007, 2010, 2013, 2016	DreamSpark Premium Electronic Software Delivery Renewal по договору - Сублицензионный договор № Tr000074357/KHB 17 от 01 марта 2016 года
6	Kaspersky Endpoint Security 2010	Лицензия (Стандартный Russian Edition. 250-499 Node 1 year Educational Renewal License) 26FE19040405012644464 до 04.06.2020
7	Автоматизированная информацион-	лицензия коммерческая по договору №945

№	Перечень программного обеспечения (обеспеченного лицензией)	Реквизиты подтверждающих документов
	ная библиотечная система «ИРБИС 64»	от 28 ноября 2011 года
8	Учебный комплект программного обеспечения КОМПАС-3D V16 на 50 рабочих мест. Проектирование и конструирование в машиностроении	Сублицензионный договор № Ец-15-000059 от 08.12.2015
9	MATLAB+SIMULINK	Academic classroom 25 по договору №2013.199430/949 от 20.11.2013

Перечень Интернет-ресурсов:

№	Наименование ресурса	Краткая характеристика
1	amursu.ru	Сайт ФГБОУ ВПО АмГУ
2	http://www.iprbookshop.ru/	Электронно-библиотечная система IPRbooks - научно-образовательный ресурс для решения задач обучения в России и за рубежом. Уникальная платформа ЭБС IPRbooks объединяет новейшие информационные технологии и учебную лицензионную литературу. ЭБС IPRbooks в полном объеме соответствует требованиям законодательства РФ в сфере образования
3	http://www.intuit.ru/	Интернет университет информационных технологи, содержит бесплатные учебные курсы, учебники и методические пособия по всем направлениям подготовки
4	https://e.lanbook.com	Электронно-библиотечная система Лань – ресурс, включающий в себя как электронные версии книг ведущих издательств учебной и научной литературы (в том числе университетских издательств), так и электронные версии периодических изданий по различным областям знаний.
5	https://www. https://urait.ru/	Электронная библиотечная система «ЮРАЙТ», тематические пакеты: математика, физика, инженерно-технические науки, химия. Фонд электронной библиотеки составляет более 4000 наименований и постоянно пополняется новинками, в большинстве своем это учебники и учебные пособия для всех уровней профессионального образования от ведущих научных школ с соблюдением требований новых ФГОСов.

Профессиональные базы данных и информационные справочные системы:

№	Наименование ресурса	Краткая характеристика
1	http://www.learner.org/	Профессиональная база данных на английском языке свободного доступа с обучающими текстовыми, аудио, видеоматериалами, тестами.
2	http://www.ict.edu.ru/about	Портал «информационно-коммуникационные технологии в образовании» входит в систему федеральных образовательных порталов и нацелен на обеспечение комплексной информационной поддержки образования в области современных информационных и телекоммуникационных технологий, а также деятельности по применению икт в сфере образования.
3	https://fstec.ru	Профессиональная база данных нормативных правовых актов, организационно-распорядительных документов, нормативных и методических документов по технической защите информации. Содержит банк данных угроз безопасности информации
4	https://reestr.minsvyaz.ru	Единый реестр российских программ для электронных вычислительных машин и баз данных. Реестр создан в соответствии со статьей 12.1 федерального закона «об информации, информационных технологиях и о защите информации» в целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из российской федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки
5	https://www.gost.ru/portal/gost/home/standarts	Каталог международных, межгосударственных и национальных стандартов, действующих технических регламентов
6	http://www.informika.ru	Сайт ФГАУ, ГНИИиТТ, «ИНФОРМИКА». Институт является государственным научным предприятием, созданным для обеспечения всестороннего развития и продвижения новых информационных технологий в сферах образования и науки России. Институт создан для осуществления комплексной поддержки развития и использования новых информационных технологий и телекоммуникаций в сфере образования и науки России
7	www.elibrary.ru	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.
8	www.iop.org	В свободном доступе представлены все оглавления и все рефераты. Полные тексты всех статей во всех журналах находятся в свободном доступе в течение 30 дней после даты их онлайновой публикации.

№	Наименование ресурса	Краткая характеристика
9	www.nature.com archive.neicon.ru	Один из самых старых и авторитетных общенаучных журналов. Публикует исследования, посвящённые широкому кругу вопросов, в основном естественнонаучной тематики. С 2005 года журнал публикует подкасты, где вкратце обсуждаются достижения науки и публикации за последнюю неделю – две.
10	https://www.scopus.com	Международная реферативная база данных научных изданий scopus
11	https://login.webofknowledge.com	Международная реферативная база данных научных изданий webofscience

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

При обучении используются:

12.1 Лекционная аудитория, оборудованная мультимедийными средствами.

12.2 Лаборатории, оборудованные рабочими местами пользователей ЭВМ.

12.3 Программное обеспечение.

Самостоятельная работа обучающихся осуществляется в помещениях, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.