

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования

«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Тобольский педагогический институт им. Д.И.Менделеева (филиал)

Тюменского государственного университета

УТВЕРЖДАЮ

Директор

Шилов С.П.

« 28 »

2020 г.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Рабочая программа для обучающихся направления

44.03.05 Педагогическое образование (с двумя профилями подготовки)

Профили история; обществознание

Форма обучения: очная

Яркова И.В. Информационная безопасность и защита информации. Рабочая программа для обучающихся по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), профили история; обществознание, форма обучения заочная. Тобольск, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Информационная безопасность и защита информации. [электронный ресурс] / Режим доступа: <https://tobolsk.utmn.ru/sveden/education/#>

1. Пояснительная записка

Целью освоения дисциплины является изучение проблем информационной безопасности различных типов организаций и предприятий, а также системы защиты ценной информации, являющейся составной частью информационных ресурсов их собственников.

Задачи дисциплины:

- познакомить студентов с определением, классификацией и характеристиками информационной безопасности;
- познакомить с организационными и экономическими аспектами работы с информационными ресурсами и методами оценки эффективности их безопасности;
- дать представление об особенностях информационной безопасности, сегментах и участниках информационного рынка, особенностях формирования безопасности информации.

1.1. Место дисциплины в структуре образовательной программы:

Дисциплина «Информационная безопасность и защита информации» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений учебного плана.

Для освоения дисциплины «Информационная безопасность и защита информации» обучающиеся используют знания, умения, навыки, сформированные в ходе изучения дисциплин «Правовые основы архивного дела и документоведения в РФ», «Документоведение и делопроизводство».

Освоение дисциплины «Информационная безопасность и защита информации» является основой для освоения дисциплин «Консалтинг и аудит в сфере документационного обеспечения управления и архивном деле», «Информационные технологии в архивном деле и документационном обеспечении управления. Электронный офис».

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины

Код и наименование компетенции (из ФГОС ВО)	Компонент (знаниевый/функциональный)
ПК – 1. Способен осуществлять обучение учебному предмету на основе использования предметных методик с учетом возрастных и индивидуальных особенностей обучающихся	Знать: теоретические основы обучения, развития обучающихся, в том числе с особыми образовательными потребностями; предметные методики; а также слабо знает возрастные, индивидуальные особенности обучающихся. Уметь: осуществлять учебный процесс с использованием предметных методик, а также с учётом возрастных и индивидуальных особенностей обучающихся; слабо знает различные теории обучения, тем самым сложно оперировать существующими знаниями.
ПК-2. Способен применять современные информационно-коммуникационные технологии в учебном процессе	Знает: о современных информационно-коммуникационных технологиях в учебном процессе, основах информационной безопасности и защиты информации. Умеет: использовать технологии мультимедиа, коммуникационные технологии для обеспечения учебного

	процесса, способы защиты информации.
--	--------------------------------------

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	Всего часов	Часов в семестре
		19
Общий объем зач.ед. час.	5	5
	180	180
Из них:		
Часы аудиторной работы всего:	16	16
Лекции	8	8
Практические занятия	8	8
Лабораторные/ практические занятия по подгруппам	-	-
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	116	116
Вид промежуточной аттестации		экзамен

3. Система оценивания

Оценивание осуществляется в рамках балльной системы, разработанной преподавателем и доведенной до сведения обучающихся на первом занятии.

№	Виды оцениваемой работы	Количество баллов	
		Текущий контроль	Промежуточный контроль
1.	Составление и рассказ тезауруса	0-30	-
2.	Устный ответ на практическом занятии	0- (5x4=20)	-
3.	Выполнение заданий по темам	0-10 (10x5=50)	-
4.	Экзамен	-	0-91

Промежуточная аттестация может быть выставлена с учетом совокупности баллов, полученных обучающимся в рамках текущего контроля.

Перевод баллов в оценки (экзамен)

№	Баллы	Оценки
1.	0-60	Неудовлетворительно
2.	61-74	Удовлетворительно
3.	75-90	Хорошо
4.	91-100	Отлично

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

Форма тематического плана для заочной формы обучения

№ п/п	Наименование тем и/или разделов	Объем дисциплины модуля, час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные/	

					практические занятия по подгруппам	
1	2	3	4	5	6	7
1	Информационные ресурсы и конфиденциальность информации	16	2			
2	Законодательство о безопасности и защите информации	16		2		
3	Источники конфиденциальной информации и каналы ее утраты	16	2			
4	Промышленный и экономический шпионаж	16				
5	Комплексная система защиты конфиденциальной информации	16		2		
6	Основные направления, этапы и методы информационно-аналитической работы	16				
7	Организация работы с персоналом, владеющим конфиденциальной информацией	16	1			
8	Конфиденциальное делопроизводство в системе защиты конфиденциальной информации	16		2		
9	Документирование конфиденциальной информации	16	1			
10	Организация конфиденциального документооборота и его сущность	16		2		
11	Формирование, оформление и хранение дел, содержащих конфиденциальные документы	20	2			
	Итого (часов)	180	8	8		

4.2. Содержание дисциплины (модуля) по темам

4.2.1. Темы лекционных занятий

Тема 1. Информационные ресурсы и конфиденциальность информации

Понятие информационных ресурсов и их классификация. Критерии ценности ИР. Правовые и экономические предпосылки выделения ценной информации. ИР открытые и ресурсы ограниченного доступа и использования.

Понятие тайны, секрета, конфиденциальности. Тайна государственная и негосударственная. Классификация видов негосударственной тайны. Коммерческая тайна как форма защиты ценной деловой и производственной информации. Сущность профессиональной, служебной, личной и семейной тайны.

Конфиденциальная информация и ее виды. Персональные данные. Правовые и технологические аспекты присвоения информации категории конфиденциальной. Ограничения на отнесение информации к категории конфиденциальной. Понятие конфиденциальности документа, его особенности. Общая классификация конфиденциальных документов. Конфиденциальная информация в вычислительных системах и сетях.

Тема 2. Источники конфиденциальной информации и каналы ее утраты

Классификация источников конфиденциальной информации, их характеристика. Уязвимость информации и интерес к ней как предпосылка возникновения угрозы информации, виды угроз.

Каналы утраты конфиденциальной информации, их характеристика. Несанкционированный доступ к информации и его последствия. Разглашение и утечка информации, их сущность и отличие. Особенности структуры каналов распространения информации в компьютерах, локальных сетях, оргтехнике и средствах связи.

Тема 4. Организация работы с персоналом, владеющим конфиденциальной информацией

Персонал как основная опасность утраты конфиденциальной информации. Особенности приема и перевода сотрудников на работу, связанную с конфиденциальной информацией. Принципы подбора персонала. Этапы, процедура и методы подбора. Особенности проведения собеседования, анкетирования, тестирования и опроса. Особенности документирования приема или перевода на должность.

Текущая работа с персоналом, владеющим конфиденциальной информацией. Процесс обучения и инструктирования сотрудников.

Методы и формы контроля соблюдения персоналом правил работы с конфиденциальной информацией. Особенности увольнения сотрудников, владеющих конфиденциальной информацией.

Порядок проведения совещаний и переговоров по конфиденциальным вопросам. Правила работы с посетителями в процессе публикационной, рекламной, выставочной деятельности.

Тема 5. Документирование конфиденциальной информации

Определение состава конфиденциальных сведений и документов. Правовые основы регламентации и критерии определения состава ценных сведений, подлежащих защите в конкретной организации. Перечень конфиденциальных сведений и перечень ценных и конфиденциальных документов в системе защиты информации. Цели и задачи перечней, их структура, особенности составления.

Основные этапы подготовки конфиденциальных документов. Определение уровня грифа конфиденциальности документа, порядок присвоения, изменения и снятие грифа конфиденциальности. Процедура предварительного учета носителей информации. Виды носителей информации, их маркировка и формы учета. Составление текста документа. Изготовление оригинала конфиденциального документа, его оформление. Процедура издания

подготовленных конфиденциальных документов, особенности подписания и утверждения. Порядок копирования и тиражирования документов.

Тема 6. Формирование, оформление и хранение дел, содержащих конфиденциальные документы
Угрозы документам в процессе формирования их в дела и хранения. Задачи защиты документов. Особенности процедур составления и ведения номенклатуры дел.

Формирование и оформление дел. Особенности оформления дела при его закрытии, выдачи законченных дел сотрудникам.

Подготовка конфиденциальных дел для архивного хранения и уничтожения. Особенности экспертизы ценности документов и процедуры составления описи дел, передаваемых в ведомственный архив.

Подготовка конфиденциальных дел и документов к уничтожению. Составление акта на уничтожение документов и дел. Состав документов, проектов документов, других материалов и носителей информации, уничтожаемых без акта. Процедура физического уничтожения документов и ее документирование.

Порядок хранения дел в службе конфиденциального делопроизводства и ведомственном архиве. Требования предъявляемые к режиму хранения. Организация использования документов и дел.

Проверка наличия документов, дел и носителей информации. Назначение, задачи и типы проверок. Состав проверяемых документов и процедуры проверки правильности работы исполнителей с конфиденциальными документами. Особенности и порядок проведения нерегламентированной проверки наличия документов, дел и носителей информации.

4.2.2. Планы практических занятий

Тема: Законодательство о безопасности и защите информации

План:

1. Понятие тайны.
2. Виды тайн и их содержание.
3. Конфиденциальная информация и ее сущность.
4. Законодательство о безопасности и защите информации, его структура и содержание.

Тема. Комплексная система защиты конфиденциальной информации

План:

1. Цели и задачи системы защиты конфиденциальной информации.
2. Комплексность системы защиты и принципы ее построения.
3. Методика разработки системы защиты информации предприятия.
4. Правовая, организационная, инженерно-техническая система защиты конфиденциальной информации.
5. Криптографическая система защиты информации.
6. Компьютерные вирусы и способы воздействия на информацию.
7. Методы и средства обеспечения компьютерной безопасности.

Тема: Конфиденциальное делопроизводство в системе защиты конфиденциальной информации

План:

1. Определение понятия «конфиденциальное делопроизводство».
2. Сущность и задачи конфиденциального делопроизводства, его организационно-технические особенности.
3. Организация конфиденциального делопроизводства.
4. Нормативно-правовая регламентация деятельности подразделения по работе с конфиденциальными документами.

Тема: Организация конфиденциального документооборота и его сущность

План:

1. Определение понятия «конфиденциальный документооборот», «защищенный документооборот». Принципы, цели и задачи организации конфиденциального документооборота.

2. Учет конфиденциальных документов как способ защиты конфиденциальной информации. Цели и задачи учета, его особенности. Виды учета, их место в технологической системе обработки и хранения конфиденциальных документов. Формирование справочно-информационного банка данных.

3. Порядок работы персонала с конфиденциальными документами и материалами. Персональная ответственность за сохранность информации, носителя информации и документа.

4.2.3. Образцы средств для проведения текущего контроля

1. Работа на семинаре, устный ответ, обсуждение рекомендованной литературы.

2. Составление и рассказ тезауруса

Студент формирует тезаурус в процессе лекционных и практических занятий, а также чтения рекомендованной литературы, работы со словарями и энциклопедиями в форме таблицы:

Образец

№ п/п	Термин	Определение (дефиниция)	Полное библиографич. описание источника (автор, заглавие, место, изд-во, год, страница)

3. Задания по темам

Тема: Информационные ресурсы и конфиденциальность информации

Задание: подготовить конспект статьи: Бундин М.В. Система информации ограниченного доступа и конфиденциальность. <https://cyberleninka.ru/article/n/sistema-informatsii-ogranichennogodostupa-i-konfidentsialnost>

Тема: Законодательство в области информационной безопасности и защиты информации

Задание 1. В виде схемы представить структуру законодательства, регулирующего правовые основы информационной безопасности и защиты информации (Конституция, кодексы, ФКЗ, ФЗ, указы Президента, постановления Правительства, ГОСТ).

Задание 2. Из текстов законодательных актов основные понятия, относящиеся к сфере информационной безопасности и защите информации. Перечень понятий оформить в виде таблицы.

Наименование закона	Перечень понятий	Определение понятий

Тема: Промышленный и экономический шпионаж

Задание: подготовить конспект статьи: Воробьева В.А. Промышленный шпионаж как угроза экономической безопасности информации. URL: <https://moluch.ru/archive/286/64528/>

Тема: Конфиденциальное делопроизводство в системе защиты конфиденциальной информации

Задание: Проанализировать структуру (основные разделы) документов и состав включаемой в них информации. Заполнить сравнительную таблицу.

Параметры	Инструкция по	Договор о	Руководство	Методические
-----------	---------------	-----------	-------------	--------------

анализа	информационной безопасности	конфиденциальности	пользователю локальной защищенной компьютерной сети	рекомендации по организации работы
1. Реквизиты документа				
2. Структура документа				
3. Краткое содержание структурных частей				
4. Вывод об особенностях применения документа и его роли в системе информационной безопасности учреждения				

Тема: Организация конфиденциального документооборота и его сущность

Задание 1: Разработать схему обработки конфиденциальных документов внутреннего и выходного потоков. Отразить материал об особенностях процедур:

- а) оформления и учета носителей конфиденциальной информации;
- б) обработки изданных документов.

Задание 2: Разработать схему обработки конфиденциальных документов входного потока.

Отразить процедуры:

- а) приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов;
- б) традиционного учета поступивших документов и формирования справочно-информационного банка данных по документам;
- в) автоматизированного учета поступивших документов и формирования справочно-информационного банка данных по документам.

Задание 3: Сформулировать выводы об особенностях и различиях технологических операций по обработке потоков входящих, исходящих и внутренних конфиденциальных документов. Отметить преимущества и недостатки традиционных и автоматизированных технологий обработки этих документов.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Информационные ресурсы и конфиденциальность информации	1. Составление тезауруса. Тезаурус формируется в процессе лекционных и практических занятий, а также чтения рекомендованной литературы, работы со словарями и энциклопедиями. Критерием оценивания является полнота раскрытия понятий во время ответа. 2. Выполнение задания по теме.

2	Законодательство о безопасности и защите информации	<p>1. Подготовка к практическому занятию. Подготовка к практическому занятию предполагает самостоятельное прочтение указанных работ для подготовки к учебному занятию, а также путем конспектирования отдельных фрагментов подготовку ответов на поставленные в плане вопросы. К критериям оценивания относятся логичность, полнота, лаконичность ответа.</p> <p>2. Составление тезауруса. Тезаурус формируется в процессе лекционных и практических занятий, а также чтения рекомендованной литературы, работы со словарями и энциклопедиями. Критерием оценивания является полнота раскрытия понятий во время ответа.</p> <p>3. Выполнение заданий по теме. Выполнение заданий по теме предполагает изучение материалов лекций, рекомендованной литературы. Задания выполняются в письменном виде. При оценивании учитывается правильность ответа</p>
3	Источники конфиденциальной информации и каналы ее утраты	<p>1. Подготовка к практическому занятию. Подготовка к практическому занятию предполагает самостоятельное прочтение указанных работ для подготовки к учебному занятию, а также путем конспектирования отдельных фрагментов подготовку ответов на поставленные в плане вопросы. К критериям оценивания относятся логичность, полнота, лаконичность ответа.</p> <p>2. Составление тезауруса. Тезаурус формируется в процессе лекционных и практических занятий, а также чтения рекомендованной литературы, работы со словарями и энциклопедиями. Критерием оценивания является полнота раскрытия понятий во время ответа.</p>
4	Промышленный и экономический шпионаж	<p>1. Тезаурус формируется в процессе лекционных и практических занятий, а также чтения рекомендованной литературы, работы со словарями и энциклопедиями. Критерием оценивания является полнота раскрытия понятий во время ответа.</p> <p>2. Выполнение задания по теме.</p>
5	Комплексная система защиты конфиденциальной информации	<p>1. Подготовка к практическому занятию. Подготовка к практическому занятию предполагает самостоятельное прочтение указанных работ для подготовки к учебному занятию, а также путем конспектирования отдельных фрагментов подготовку ответов на поставленные в плане вопросы. К критериям оценивания относятся логичность, полнота, лаконичность ответа.</p> <p>2. Составление тезауруса. Тезаурус формируется в процессе лекционных и практических занятий, а также чтения рекомендованной литературы, работы со словарями и энциклопедиями. Критерием оценивания является полнота раскрытия понятий во время ответа.</p>

6	Основные направления, этапы и методы информационно-аналитической работы	Составление тезауруса. Тезаурус формируется в процессе лекционных и практических занятий, а также чтения рекомендованной литературы, работы со словарями и энциклопедиями. Критерием оценивания является полнота раскрытия понятий во время ответа.
7	Организация работы с персоналом, владеющим конфиденциальной информацией	Составление тезауруса. Тезаурус формируется в процессе лекционных и практических занятий, а также чтения рекомендованной литературы, работы со словарями и энциклопедиями. Критерием оценивания является полнота раскрытия понятий во время ответа.
8	Конфиденциальное делопроизводство в системе защиты конфиденциальной информации	1. Подготовка к практическому занятию. Подготовка к практическому занятию предполагает самостоятельное прочтение указанных работ для подготовки к учебному занятию, а также путем конспектирования отдельных фрагментов подготовку ответов на поставленные в плане вопросы. К критериям оценивания относятся логичность, полнота, лаконичность ответа. 2. Составление тезауруса. Тезаурус формируется в процессе лекционных и практических занятий, а также чтения рекомендованной литературы, работы со словарями и энциклопедиями. Критерием оценивания является полнота раскрытия понятий во время ответа. 3. Выполнение задания по теме. Выполнение заданий по теме предполагает изучение материалов лекций, рекомендованной литературы. Задания выполняются в письменном виде. При оценивании учитывается правильность ответа
9	Документирование конфиденциальной информации	Составление тезауруса. Тезаурус формируется в процессе лекционных и практических занятий, а также чтения рекомендованной литературы, работы со словарями и энциклопедиями. Критерием оценивания является полнота раскрытия понятий во время ответа.
10	Организация конфиденциального документооборота и его сущность	1. Подготовка к практическому занятию. Подготовка к практическому занятию предполагает самостоятельное прочтение указанных работ для подготовки к учебному занятию, а также путем конспектирования отдельных фрагментов подготовку ответов на поставленные в плане вопросы. К критериям оценивания относятся логичность, полнота, лаконичность ответа. 2. Составление тезауруса. Тезаурус формируется в процессе лекционных и практических занятий, а также чтения рекомендованной литературы, работы со словарями и энциклопедиями. Критерием оценивания является полнота раскрытия понятий во время ответа. 3. Выполнение заданий по теме. Выполнение заданий по теме предполагает изучение

		материалов лекций, рекомендованной литературы. Задания выполняются в письменном виде. При оценивании учитывается правильность ответа
11	Формирование, оформление и хранение дел, содержащих конфиденциальные документы	Составление тезауруса. Тезаурус формируется в процессе лекционных и практических занятий, а также чтения рекомендованной литературы, работы со словарями и энциклопедиями. Критерием оценивания является полнота раскрытия понятий во время ответа.
12	По всему курсу	Подготовка к экзамену

6. Промежуточная аттестация по дисциплине

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

Форма промежуточной аттестации - экзамен. Процедура оценивания производится в форме устного ответа на вопросы по дисциплине и по результатам выполнения заданий текущего контроля.

Вопросы к экзамену.

1. Понятие «безопасность» и «информационная безопасность». Законодательство о безопасности и защите информации, его структура и содержание.

2. Законодательство об интеллектуальной и промышленной собственности и проблемы обеспечения информационной безопасности.

3. Законодательство о защите государственной и коммерческой тайны, персональных данных, его структура и содержание.

4. Отражение вопросов защиты информации в гражданском, уголовном и административном праве.

5. Понятие «тайна», «секрет». Виды тайн и их содержание.

6. Сущность понятий «ценность» и «конфиденциальность» информации. Определение состава конфиденциальной информации.

7. Источники конфиденциальной информации и каналы ее распространения.

8. Персонал организации как источник утраты конфиденциальной информации.

9. Особенности проведения конфиденциальных совещаний и переговоров.

10. Защита конфиденциальной информации в работе отдела кадров.

11. Конфиденциальный документ как источник конфиденциальной информации.

Основные группы конфиденциальных документов.

12. Основные угрозы конфиденциальной информации.

13. Состав угроз конфиденциальным документам (традиционным и электронным).

14. Система защиты информации, ее место в информационной безопасности организации.

15. Правовые основы организации работы с конфиденциальными сведениями.

16. Состав нормативно-методических материалов по регламентации системы защиты информации.

17. Организационные основы защиты конфиденциальной информации.

18. Инженерно-техническая защита конфиденциальной информации.

19. Программно-аппаратная и криптографическая защита конфиденциальной информации.

20. Направления и методы защиты профессиональной и служебной тайны.

21. Опыт зарубежных стран по защите информации.

22. Аналитическая работа в сфере защиты информации.

23. Особенности работы с персоналом, владеющим конфиденциальной информацией.

24. Текущая работа с персоналом, владеющим конфиденциальной информацией.

25. Конфиденциальное делопроизводство, его сущность и особенности.

26. Особенности организации конфиденциального делопроизводства.

27. Регламентация состава конфиденциальных сведений и документов. Особенности и этапы составления перечня конфиденциальных документов.
28. Учет и оформление носителей информации.
29. Технология подготовки и издания конфиденциальных документов.
30. Особенности оформления конфиденциальных документов.
31. Организация и технология размножения конфиденциальных документов.
32. Общие требования к учету конфиденциальных документов. Особенности учета изданных, поступивших КД и документов выделенного хранения.
33. Особенности организации конфиденциального документооборота.
34. Разрешительная система доступа к конфиденциальным документам.
35. Организация исполнения конфиденциальных документов.
36. Отправление конфиденциальных документов. Особенности пакетирования отправляемых документов и передачи их адресатам по незащищенным линиям связи.
37. Составление номенклатуры конфиденциальных дел.
38. Формирование конфиденциальных документов в дела и работа с ними.
39. Оформление конфиденциальных дел.
40. Экспертиза ценности конфиденциальных документов.
41. Подготовка конфиденциальных дел и документов для архивного хранения.
42. Подготовка конфиденциальных дел и документов для уничтожения.
43. Режим хранения конфиденциальных документов.
44. Проверка наличия конфиденциальных документов.
45. Работа персонала с конфиденциальными документами.

6.2 Критерии оценивания компетенций:

Таблица 4

Карта критериев оценивания компетенций

№ п/п	Код наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1	ПК – 1. Способен осуществлять обучение учебному предмету на основе использования предметных методик с учетом возрастных и индивидуальных особенностей обучающихся	Знает: теоретические основы обучения, развития обучающихся, в том числе с особыми образовательными потребностями; предметные методики; а также слабо знает возрастные, индивидуальные особенности обучающихся	Устный ответ на практическом занятии, составление и рассказ тезауруса, выполненные задания по темам	Знаком с теоретическими основами обучения, развития обучающихся, в том числе с особыми образовательными потребностями; предметные методики; а также знает возрастные, индивидуальные особенности

		я. Умеет: осуществлять учебный процесс с использованием предметных методик, а также с учётом возрастных и индивидуальных особенностей обучающихся; слабо знает различные теории обучения, тем самым сложно оперировать существующими знаниями.		обучающихся. Может свободно осуществлять учебный процесс с использованием предметных методик, а также с учётом возрастных и индивидуальных особенностей обучающихся; слабо знает различные теории обучения, тем самым сложно оперировать существующими знаниями.
2	ПК-2. Способен применять современные информационно-коммуникационные технологии в учебном процессе	Знает: о современных информационно-коммуникационных технологиях в учебном процессе, основах информационной безопасности и защиты информации. Умеет: использовать технологии мультимедиа, коммуникационные технологии для обеспечения учебного процесса, способы защиты информации.	Устный ответ на практическом занятии, составление и рассказ тезауруса, выполненные задания по темам	Знаком с современными информационно-коммуникационными технологиями в учебном процессе, основами информационной безопасности и защиты информации. Может использовать технологии мультимедиа, коммуникационные технологии для обеспечения учебного процесса, способы защиты информации.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература:

1. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - Москва: РИОР: ИНФРА-М, 2020. - 336 с. - URL: <https://znanium.com/read?id=359537>

7.2. Дополнительная литература:

1. Введение в информационную безопасность: Учебное пособие для вузов / А.А. Малюк, В.И. Королёв, В.М. Фомичев; Под ред. В.С. Горбатов. - Москва: Гор. линия-Телеком, 2011. - 288 с.: ил.; . - (Специальность). ISBN 978-5-9912-0160-5, 1000 экз. - Текст: электронный. - URL: <https://znanium.com/read?id=42509>

2. Бахаров, Л. Е. Информационная безопасность и защита информации: разделы криптография и стеганография: практикум / Л. Е. Бахаров. - Москва: Изд. Дом НИТУ «МИСиС», 2019. - 59 с. - ISBN 978-5-906953-94-0. - Текст: электронный. - URL: <https://znanium.com/read?id=371197>

7.3. **Интернет-ресурсы:** Не предусмотрены.

7.4. **Современные профессиональные базы данных и информационные справочные системы:**

1. Лань - <https://e.lanbook.com/>
2. Знаниум - <https://znanium.com/>
3. IPR BOOKS - <http://www.iprbookshop.ru/>
4. eLIBRARY.RU - <https://www.elibrary.ru/>
5. Межвузовская электронная библиотека (МЭБ) - <https://icdlib.nspu.ru/> (только в филиале)
6. Национальная электронная библиотека (НЭБ) - <https://rusneb.ru/> (полное использование только в филиале)
7. Ивис - <https://dlib.eastview.com/>
7. Библиотека ТюмГУ - <https://library.utmn.ru/>

8. **Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)**

Платформа для электронного обучения Microsoft Teams.

Бесплатное программное обеспечение, установленное в аудиториях: 7-Zip, Adobe Acrobat Reader, Mozilla Firefox, OpenOffice.org.

Лицензионное программное обеспечение, установленное в аудиториях: Microsoft Office 2003, Microsoft Office 2007, Microsoft Office 2010, Windows, Конструктор тестов 2.5 (Keepsoft).

9. **Технические средства и материально-техническое обеспечение дисциплины**

– Учебные аудитории для проведения лекций и практических занятий укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: мультимедийные аудитории, укомплектованные таким оборудованием, как проектор, документ камера, проекционный экран.

– Помещения для самостоятельной работы обучающихся (компьютерные классы) оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечены доступом к электронной информационно-образовательной среде вуза.

– Лаборатории, оснащенные лабораторным оборудованием, для реализации данной дисциплины не предусмотрены.

На ПК установлено следующее программное обеспечение:

— Офисное ПО: операционная система MS Windows, офисный пакет MS Office, платформа MS Teams, офисный пакет LibreOffice, антивирусное ПО Dr. Web.

Обеспечено проводное подключение ПК к локальной сети и сети Интернет.