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» мая 2020 г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Рабочая программа
для обучающихся по направлению подготовки
05.03.06 Экология и природопользование
Профиль Экология и техносферная безопасность
Форма обучения очная

Буслова Н.С. Информационная безопасность. Рабочая программа для обучающихся по направлению подготовки 05.03.06 Экология и природопользование, профиль Экология и техносферная безопасность, форма обучения очная. Тобольск, 2020.

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

1. Пояснительная записка

Цель освоения дисциплины - формирование системы знаний о современном состоянии проблемы обеспечения информационной безопасности, методах и средствах защиты информации, основах построения комплексных систем защиты.

Задачи:

- формирование представления о проблеме обеспечения информационной безопасности, ее важность и актуальность;
- изучение основных средств обеспечения информационной безопасности в сетях;
- изучение способов удостоверения и контроля аутентичности входящей и исходящей информации, методов ее проверки;
- овладение основными правового обеспечения информационной безопасности и защиты информации;
- формирование навыков эффективного использования доступных методов и средств обеспечения информационной безопасности современных компьютерных систем.

1.1. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к дисциплинам по выбору вариативной части блока Б1.

Для освоения дисциплины «Информационная безопасность» студенты используют знания и умения, сформированные в ходе изучения дисциплины «Информатика и современные информационные технологии в экологии и природопользовании», «Опасности социального характера и антитеррористическое просвещение работников предприятий».

Освоение данной дисциплины является необходимой основой для последующего изучения дисциплин направления, дисциплин по выбору студента и подготовки к итоговой государственной аттестации.

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины

Процесс изучения данной дисциплины направлен на формирование элементов следующих компетенций по данному направлению подготовки:

ПК-4 - способностью прогнозировать техногенные катастрофы и их последствия, планировать мероприятия по профилактике и ликвидации последствий экологических катастроф, принимать профилактические меры для снижения уровня опасностей различного вида и их последствий;

ПК-12 - владением навыками работы в административных органах управления предприятий, фирм и других организаций; проведения экологической политики на предприятиях;

ПК-13 - владением навыками планирования и организации полевых и камеральных работ, а также участия в работе органов управления.

Код и наименование компетенции	Компонент (знаниевый/функциональный)
ПК-4 - способностью прогнозировать техногенные катастрофы и их последствия, планировать мероприятия по профилактике и ликвидации последствий экологических катастроф, принимать профилактические меры для снижения уровня опасностей различного вида и их последствий;	Знает методы и средства обеспечения информационной безопасности; критерии защищенности компьютерных систем и принципы построения комплексной системы защиты информации Умеет находить эффективные способы защиты информации и использовать их для обеспечения информационной безопасности современных компьютерных систем

ПК-12 - владением навыками работы в административных органах управления предприятий, фирм и других организаций; проведения экологической политики на предприятиях;	Знает сущность проблемы обеспечения информационной безопасности, ее важность и актуальность; методы и средства обеспечения информационной безопасности и защиты информации Умеет реализовывать общие правила и меры обеспечения информационной безопасности
ПК-13 - владением навыками планирования и организации полевых и камеральных работ, а также участия в работе органов управления.	Знает особенности информации и информационных систем как объекта защиты информации, основные угрозы для информационных ресурсов, возможные последствия воздействия угроз и способы их реализации в осуществлении профессиональной деятельности Умеет использовать доступные методы и средства обеспечения информационной безопасности в профессиональной деятельности

2. Структура и объем дисциплины

Семестр 8. Форма промежуточной аттестации (зачет, экзамен): экзамен.

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 академических часа, из них 48 часов, выделенных на контактную работу с преподавателем, 96 часов, выделенный на самостоятельную работу.

Вид учебной работы	**Всего часов**	**Часов в семестре**
		8
Общая трудоемкость **зач. ед.**	4	4
час	144	144
Из них:		
Часы аудиторной работы (всего):	48	48
Лекции	24	24
Практические занятия	24	24
Лабораторные / практические занятия по подгруппам	-	-
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	96	96
Вид промежуточной аттестации		экзамен

3. Система оценивания

Экзамен проводится в форме собеседования по вопросам теоретического и практического характера. Успешная работа на занятиях, составление опорных конспектов, выполнение практических заданий может быть засчитана как практическая часть экзамена.

4. Содержание дисциплины

4.1. Тематический план дисциплины

№	Наименование тем и/или разделов	Объем дисциплины, час.			
		Всего	Виды аудиторной работы (акад. час.)		Иные виды контактной работы
			Лекции	Практические занятия	
1	2	3	4	5	6
1	Информационная безопасность - основные понятия	2	2	-	
2	Основные угрозы информационной безопасности в информационной среде	4	2	2	
3	Основные меры защиты информации в распределенных компьютерных системах	8	4	4	
4	Взаимодействие в условиях недоверенной распределенной среде	8	4	4	
5	Стандарты в области информационной безопасности в ИОС	6	2	4	
6	Правовое обеспечение информационной безопасности	8	4	4	
7	Организационное обеспечение информационной безопасности в ИОС	4	2	2	
8	Лицензирование и сертификация в информационной среде	4	2	2	
9	Международное законодательство в области защиты информации. Компьютерные правонарушения	4	2	2	
	Итого (часов):	48	24	24	

4.2. Содержание дисциплины по темам

4.2.1. Темы лекций

Информационная безопасность - основные понятия

Понятие информационной безопасности (ИБ). Аспекты безопасности, понятия уязвимости, угрозы, атаки. Основные стратегии предупреждения нарушений. Иллюстрирующие инциденты. Анализ возможностей и объектов защиты с помощью уровневых сетевых моделей. Актуальность проблемы обеспечения ИБ в ИОС. Проблема ИБ с точки зрения правового обеспечения.

Основные угрозы информационной безопасности в информационной среде

Типовые угрозы ИБ. Виды возможных нарушений. Правовая классификация и оценка нарушений ИБ. Классификация уязвимостей различных уровней в модели DOD. Реализация типовых угроз. Средства защиты от типовых угроз на уровне доступа к среде, сетевом и транспортном уровнях.

Основные меры защиты информации в распределенных компьютерных системах

Организационно-технические меры обеспечения ИБ. Понятие политики безопасности. Управление доступа к данным. Реализация типовых угроз на прикладном уровне, средства и методы защиты.

Взаимодействие в условиях недоверенной распределенной среде

Защита информации в компьютерных системах от несанкционированного доступа. Методы и средства защиты от несанкционированного изменения. Криптографические методы защиты информации. Системы шифрования с открытым ключом (асимметричные). Симметричное

шифрование. Сертификаты, обмен сертификатами, доверие. Шифрование информации на прикладном уровне - протоколы HTTPS, система PGP. Система электронно-цифровой подписи. Примеры использования. Социальная инженерия.

Стандарты в области информационной безопасности в ИОС

Международный стандарт ИБ. Госстандарты. Основные вопросы стандартов ИБ в ИОС. Проблемы стандартизации ИБ.

Правовое обеспечение информационной безопасности

Понятие правового обеспечения ИБ. Особенности информации как объекта права. Госполитика РФ в области правового обеспечения.

Организационное обеспечение информационной безопасности в ИОС

Понятие организационного обеспечения ИБ в ИОС. Характеристика организационных методов обеспечения ИБ. Организационно-распорядительные документы, связанные с защитой сведений конфиденциального характера.

Лицензирование и сертификация в информационной среде

Правовая основа системы лицензирования и сертификации в РФ. Лицензирование деятельности по защите информации. Объекты лицензирования в сфере защиты информации. Понятие сертификации по российскому законодательству.

Международное законодательство в области защиты информации. Компьютерные правонарушения

Международные договоры и конвенции в области защиты информации. Законодательство в области международного информационного объекта и компьютерных преступлений.

4.2.2. Темы практических занятий

Тема 1. Информационная безопасность - основные понятия

Подготовка терминологического словаря основных понятий темы

Тема 2. Основные угрозы информационной безопасности в информационной среде

Ознакомление с наиболее частыми уязвимостями, методами их обнаружения и устранения.

Прочитать задачу, найти правовое обоснование и разрешить противоречивую правовую ситуацию. Обсудить найденное решение, обосновать свою позицию аргументами и положениям правовых актов.

"Задача: Гражданин Иванов, служил в качестве члена научно-исследовательской группы института "Прогресс".

Иванов дал интервью для журнала «Метрополитен», в котором оценил радиационную обстановку в регионе с целью продемонстрировать суть его технической разработки по определению интенсивности излучения. Интервью с Ивановым была опубликована и стала общедоступной, и научным руководством Института "Прогресс". Администрация института подала заявление на Иванова о возбуждении уголовного дела по признакам преступлений, предусмотренных ст. 147 и ст. 183 Уголовного кодекса. Защитнику Иванова стало известно, что Иванов воспользовался для разработки своего технического устройства сведениями, составляющими коммерческую тайну.

Будет ли Иванов привлечен к уголовной ответственности? Как ему избежать уголовной ответственности?"

Тема 3. Основные меры защиты информации в распределенных компьютерных системах

Изучение основных способов регламентации доступа

Прочитать задачу, найти правовое обоснование и разрешить противоречивую правовую ситуацию. Обсудить найденное решение, обосновать свою позицию аргументами и положениям правовых актов.

"Задача: Общественная организация «За здоровье нации» обратилась к администрации Аргаяшской птицефабрики с заявлением о предоставлении информации о технике безопасности на предприятии: уровне ПДК в воздухе производственных помещений, уровне травматизма на производстве и выплате компенсаций по здоровьесбережению. Руководство предприятия отказалось удовлетворить просьбу общественной организации, мотивируя свое отказное решение тем, что указанные данные являются конфиденциальной информацией.

Дайте разъяснения по существу сложившейся ситуации, приведите правовые нормы в обоснование своих доводов."

Тема 4. Взаимодействие в условиях недоверенной распределенной среде

Сопоставить предложенный перечень понятий с определениями, приведенными ниже. Результат сопоставления оформить в виде пар чисел, где арабская цифра – ключевое понятие, а римская цифра – его определение:

Часть 1

Вирус (компьютерный, программный)
Информационная система общего пользования
Документированная информация
Аутентификация отправителя данных
Государственная тайна
Информационная система
Автоматизированная обработка персональных данных
Блокирование персональных данных
Автоматизированная система
Информация
Гриф секретности
Вредоносная программа
Доступ к информации
Информационно-телекоммуникационная сеть
Вспомогательные технические средства и системы
Защищаемая информация.
Безопасность персональных данных

Часть 2

I. программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных

II. возможность получения информации и ее использования

III. технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

IV. информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации

V. реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него

VI. сведения (сообщения, данные) независимо от формы их представления

VII. временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)

VIII. зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель

IX. подтверждение того, что отправитель полученных данных соответствует заявленному

X. состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных

XI. технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных

XII. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации
XIII. совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
XIV. обработка персональных данных с помощью средств вычислительной техники
XV. система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций
XVI. исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения
XVII. информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.
Освоение криптографических средств защиты информации (симметричные и асиммитричные системы шифрования)

Тема 5. Стандарты в области информационной безопасности в ИОС

Прочитать задачу, найти правовое обоснование и разрешить противоречивую правовую ситуацию. Обсудить найденное решение, обосновать свою позицию аргументами и положениям правовых актов.

"Задача: Лех Я.В. обратился в суд с иском к ООО «Гранада» о взыскании компенсации за нарушение исключительного права на произведение, компенсации морального вреда, возложении обязанности по удалению произведения с сайта. В обоснование иска указал, что общество разместило на своем сайте литературно-художественный публицистический очерк (документальный рассказ), посвященный дню защиты Земли, автором которого он является Лех. Разрешение на публикацию очерка на сайте ответчика он не давал. Путем размещения на сайте указанного очерка было нарушено его авторское неимущественное право. Представитель ответчика факт размещения произведения истца на сайте не отрицала, исковые требования признала в части компенсации за нарушение ответчиком авторского права истца, при этом ссылалась на завышенный размер компенсации, заявленный истцом. В части компенсации морального вреда иск не признала, ссылаясь на то, что неимущественные права истца ответчиком не нарушены. Отмечает, что «незаконно использованный» ответчиком очерк по количеству строк более чем в два раза превышает написанный им рассказ, авторские права на который были приобретены московским продюсером за 1000 долларов. При этом над очерком он работал около 4 месяцев, а рассказ написан за 1 день. Как разрешитъ этот спор с позиции норм информационного права?"

Тема 6. Правовое обеспечение информационной безопасности

Составить электронный конспект по основным правовым актам в области информационной безопасности:

- ст. ст. 23, 24, 29, 42 Конституции РФ, ст. ст. 5,7,8,9 ФЗ "Об информации, информационных информации" от 27.07.2006 N 149-ФЗ (действующая редакция, 2016);
- ст.ст. 3, 4 Закона РФ от 27.12.1991 N 2124-1 (ред. от 03.07.2016) "О средствах массовой информации" (с изм. и доп., вступ. в силу с 15.07.2016),
- ст. ст. 7, 8, 9, 11 ФЗ "О персональных данных" от 27.07.2006 N 152-ФЗ (действующая редакция, 2016); сфера действия и принцип отнесения к гостайне ФЗ РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) "О государственной тайне";
- ст. 2 ФЗ "Об электронной подписи" от 06.04.2011 N 63-ФЗ (действующая редакция, 2016);
- ст.272, 273, 274 УК РФ.

Тема 7. Организационное обеспечение информационной безопасности в ИОС

Составить аналитическую записку - обзор по предложенному перечню. Аналитическая записка должна содержать иерархическую структуру исследованных правовых актов, сферу действия отдельных групп документов, соотношение и согласование групп правовых документов, принадлежность к государственному органу.

Тема 8. Лицензирование и сертификация в информационной среде
Найти сайт образовательного учреждения. Смоделировать политику безопасности образовательного учреждения и составить матрицу доступа для образовательного учреждения. Составить иерархию ролей для данного образовательного учреждения с описанием ролей сотрудников. При описании должен быть реализован принцип минимизации привилегий**.**
Тема 9. Международное законодательство в области защиты информации. Компьютерные правонарушения
1Найти определения АС в соответствии с классификацией, принятой в действующей системе правовых актов и нормативно-методических документов.
2 Вставить определения вместо пропусков.
3 Отметить нормативные документы, регламентирующие функционирование конкретной АС в предлагаемом перечне нормативных документов.
4 Проверить правильность выполнения заданий путем совместного обсуждения и проверки.

4.2.3. Образцы средств для проведения текущего контроля

Степень овладения знаниями и практическими навыками определяется в процессе текущего и итогового контроля. Работа на занятии, обсуждение рекомендованной литературы, составление опорных конспектов, выполнение практических заданий.

Вопросы для обсуждения
1. Какие методы защиты информации, использовавшиеся в древнее время и в Средние века Вам известны?
2. Покажите связь между уровнем развития общества и технологиями защиты информации.
3. В каких направлениях идет развитие теории информационной безопасности в настоящее время?
4. Каков вклад российских ученых в теорию информационной безопасности?
5. С чем связан возросший интерес к проблемам защиты информации?
6. Каковы отличия формального и неформального подходов к проблемам защиты информации?
7. В чем, на Ваш взгляд, заключаются основные трудности обеспечения информационной безопасности в настоящее время?
8. Что такое информационная система? Телекоммуникационная система? Автоматизированная система?
9. Каковы правовые понятия в области защиты информации?
10. Что такое защита информации? Информационная безопасность?

Практические задания
1. Подготовка терминологического словаря основных понятий темы
2. Прочитать задачу, найти правовое обоснование и разрешить противоречивую правовую ситуацию. Обсудить найденное решение, обосновать свою позицию аргументами и положениям правовых актов.
3. Сопоставить предложенный перечень понятий с определениями, приведенными ниже. Результат сопоставления оформить в виде пар чисел, где арабская цифра – ключевое понятие, а римская цифра – его определение
4. Составить электронный конспект по основным правовым актам в области информационной безопасности
5. Составить аналитическую записку - обзор по предложенному перечню. Аналитическая записка должна содержать иерархическую структуру исследованных правовых актов, сферу действия отдельных групп документов, соотношение и согласование групп правовых документов, принадлежность к государственному органу
6. Найти сайт образовательного учреждения. Смоделировать политику безопасности образовательного учреждения и составить матрицу доступа для образовательного учреждения.

Составить иерархию ролей для данного образовательного учреждения с описанием ролей сотрудников. При описании должен быть реализован принцип минимизации привилегий
7. Найти определения АС в соответствии с классификацией, принятой в действующей системе правовых актов и нормативно-методических документов. Вставить определения вместо пропусков. Отметить нормативные документы, регламентирующие функционирование конкретной АС в предлагаемом перечне нормативных документов. Проверить правильность выполнения заданий путем совместного обсуждения и проверки

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

№	Разделы	Формы СРС, включая требования к подготовке к занятиям
1	Информационная безопасность - основные понятия	Подготовка терминологического словаря основных понятий темы
2	Основные угрозы информационной безопасности в информационной среде	Ознакомление с наиболее частыми уязвимостями, методами их обнаружения и устранения. Компьютерные вирусы
3	Основные меры защиты информации в распределенных компьютерных системах	Изучение основных способов регламентации доступа в распределенных системах
4	Взаимодействие в условиях недоверенной распределенной среде	Освоение криптографических средств защиты информации (симметричные и асиммитричные системы шифрования)
5	Стандарты в области информационной безопасности в ИОС	Рассмотрение практических вопросов стандартизации ИБ ИОС
6	Правовое обеспечение информационной безопасности	Изучение правовых норм в области ИБ. Рассмотрение зарубежного законодательства в области ИБ, международного законодательства в области защиты информации. Рассмотрение законодательства в области защиты интеллектуальной собственности
7	Организационное обеспечение информационной безопасности в ИОС	Подготовка нормативной документации о проведении инструктажа сотрудников, организации контроля за соблюдением процедур, связанных с защитой информации
8	Лицензирование и сертификация в информационной среде	Рассмотрение видов деятельности в информационной сфере, подлежащих лицензированию. Изучение объектов сертификационной деятельности, органов сертификации.
9	Международное законодательство в области защиты информации. Компьютерные правонарушения	Изучение международного правого опыта обеспечения информационной безопасности

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

Промежуточная аттестация студентов по курсу предполагает экзамен. Экзамен проводится в форме собеседования по вопросам теоретического и практического характера.

Перечень примерных вопросов для промежуточного контроля

1. Понятие информационной безопасности
2. Аспекты безопасности

3. Определение «уязвимости», «угрозы», «атаки» и «эксплойта». Модели угроз и виды угроз (антропогенные, техногенные, стихийные источники угроз).

4. Модель нарушителя: определение хакерства. Цели и задачи хакера. «Белые», «серые» и «чѐрные» хакеры. Социальная инженерия: определение, задачи, примеры применения для нарушения конфиденциальности, целостности и доступности информации.

5. Основные механизмы обеспечения ИБ: идентификация, аутентификация, авторизация, аудит.

Задания практического характера аналогичны заданиям, рассматриваемым в ходе практических занятий.

6.1. Критерии оценивания компетенций:

Карта критериев оценивания компетенций

Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
ПК-4 - способностью прогнозировать техногенные катастрофы и их последствия, планировать мероприятия по профилактике и ликвидации последствий экологических катастроф, принимать профилактические меры для снижения уровня опасностей различного вида и их последствий;	Знает методы и средства обеспечения информационной безопасности; критерии защищенности компьютерных систем и принципы построения комплексной системы защиты информации Умеет находить эффективные способы защиты информации и использовать их для обеспечения информационной безопасности современных компьютерных систем	Устные ответы на вопросы, Выполнение практических заданий	*Пороговый уровень:* может выполнять работы под контролем преподавателя. *Базовый уровень:* может выполнять работы самостоятельно. *Повышенный уровень:* готов выполнять работы по обеспечению информационной безопасности для обеспечения информационной безопасности современных компьютерных систем
ПК-12 - владением навыками работы в административных органах управления предприятий, фирм и других организаций; проведения экологической политики на предприятиях;	Знает сущность проблемы обеспечения информационной безопасности, ее важность и актуальность; методы и средства обеспечения информационной безопасности и защиты информации Умеет реализовывать общие правила и меры обеспечения информационной безопасности	Устные ответы на вопросы, Выполнение практических заданий	*Пороговый уровень:* может выполнять работы под контролем преподавателя. *Базовый уровень:* может выполнять работы самостоятельно. *Повышенный уровень:* готов выполнять работы по обеспечению информационной безопасности
ПК-13 - владением навыками планирования и организации полевых и камеральных работ, а также участия в работе органов управления.	Знает особенности информации и информационных систем как объекта защиты информации, основные угрозы для информационных ресурсов, возможные последствия воздействия угроз и способы их реализации в осуществлении профессиональной деятельности Умеет использовать доступные методы и средства обеспечения информационной безопасности в профессиональной деятельности	Устные ответы на вопросы, Выполнение практических заданий	*Пороговый уровень:* может выполнять работы под контролем преподавателя. *Базовый уровень:* может выполнять работы самостоятельно. *Повышенный уровень:* готов выполнять работы по обеспечению информационной безопасности в профессиональной деятельности

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература:

Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. – Москва: ИНФРА-М, 2021. – 201 с.- URL: ***https://znanium.com/read?id=365029***. – Режим доступа: по подписке ТюмГУ.

7.2 Дополнительная литература

1. Информационная безопасность: практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2019. - 84 с. - URL: https://znanium.com/read?id=358668. – Режим доступа: по подписке. ТюмГУ.
2. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва: РИОР, 2013. - 222 с. - URL: https://znanium.com/read?id=213488. – Режим доступа: по подписке ТюмГУ.

7.3 Интернет-ресурсы

1. Единое окно доступа к образовательным ресурсам. – URL: http://window.edu.ru/ Режим доступа: свободный.
2. Российское образование. Федеральный портал. – URL: http://www.edu.ru Режим доступа: свободный.
3. Единая коллекция цифровых образовательных ресурсов – URL: http://school-collection.edu.ru/. Режим доступа: свободный.
4. Академия Педагогики. Центр дистанционной поддержки учителей. – URL: http://pedakademy.ru Режим доступа: свободный.

7.4. Современные профессиональные базы данных и информационные справочные системы:

1. Электронно-библиотечная система издательства «Лань» – URL: https://e.lanbook.com/ Режим доступа: по подписке ТюмГУ.
2. Электронно-библиотечная система Znanium.com – URL: https://znanium.com/ Режим доступа: по подписке ТюмГУ.
3. IPR BOOKS – URL: http://www.iprbookshop.ru/ Режим доступа: по подписке ТюмГУ.
4. Научная электронная библиотека eLIBRARY.RU – URL: https://www.elibrary.ru/defaultx.asp Режим доступа: по подписке ТюмГУ.
5. Межвузовская электронная библиотека (МЭБ) – URL: https://icdlib.nspu.ru/ Режим доступа: по подписке ТюмГУ.
6. Национальная электронная библиотека (НЭБ) – URL: https://rusneb.ru/ Режим доступа: по подписке ТюмГУ.
7. Ивис – URL: https://dlib.eastview.com/ Режим доступа: по подписке ТюмГУ.
8. Библиотека ТюмГУ – URL: https://library.utmn.ru/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- Интернет-браузер для работы с учебными порталами;

Лицензионное ПО для разработки учебно-методических материалов:

- Microsoft Office 2003, Microsoft Office 2007, Microsoft Office 2010, Windows, Dr. Web, Конструктор тестов 2.5 (Keepsoft), Adobe Design Premium CS4, Corel Draw Graphics Suite X5.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Мультимедийная учебная аудитория для проведения занятий лекционного и лабораторного типа, для самостоятельной работы № 201 на 24 рабочих места с компьютерным классом на 20 рабочих мест, оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, принтер, персональные компьютеры.

15+1 ПК (HP EliteDesk 800 G5: Intel Core i5 9500T 2,2 ГГц; AMD Radeon RX 560 4 ГБ; DDR4 16 ГБ; SSD 256 ГБ; HP ProDisplay P244: 1920x1080; 23 дюйма; MS Windows 10; MS Office 2010), 5 ноутбуков (HP 255 G7: AMD Ryzen 3 2200U 2,5 ГГц; AMD Radeon Vega 3; DDR4 8 ГБ; SSD 128 ГБ; 1920x1080; 15,6 дюйма; MS Windows 10; MS Office 2010), принтер лазерный цветной А3 (HP Color LaserJet Pro CP5225N), проектор (Epson EB-980W: 1280x800; 3800 лм), экран (16:10; 300x250 см). 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.

Мультимедийная учебная аудитория для проведения занятий лекционного и лабораторного типа, для самостоятельной работы № 303 на 24 рабочих места с **компьютерным классом** на 15 рабочих мест, оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, принтер, персональные компьютеры.

15+1 ПК (Dell 3060-7601: Intel Core i5 8500T 2,1 ГГц; DDR4 8 ГБ; SSD 256 ГБ; Dell SE2216H: 1920x1080; 21,5 дюйма; MS Windows 10; MS Office 2010), **проектор** (Epson EB-980W: 1280x800; 3800 лм), экран.

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.

Мультимедийная учебная аудитория для самостоятельной работы студентов №301 на 20 посадочных мест, с компьютерным классом на 15 рабочих мест оснащена следующими техническими средствами обучения и оборудованием:

15+1 ПК (Dell 3060-7601:Intel Core i5 8500T 2,1 ГГц; DDR4 8 ГБ; SSD 256 ГБ; Dell SE2216H: 1920x1080; 21,5 дюйма; MS Windows 10; MS Office 2010), **интерактивная доска** (SmartBoard SBX885: 16:10; 188x117 см; 87 дюймов), **проектор** (SMART V25: 1024x768; 2000 лм)

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.

Мультимедийная учебная аудитория для проведения занятий лекционного и лабораторного типа, для самостоятельной работы № 311 на 24 рабочих мест с компьютерным классом на 15 рабочих мест оснащена следующими техническими средствами обучения и оборудованием:

15+1 ПК (Dell 3060-7601:Intel Core i5 8500T 2,1 ГГц; DDR4 8 ГБ; SSD 256 ГБ; Dell SE2216H: 1920x1080; 21,5 дюйма; MS Windows 10; MS Office 2010), **проектор** (Epson EB-980W: 1280x800; 3800 лм), **экран** (16:10)

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.