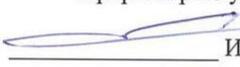


МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»
Проректор по учебной работе


И.Е. Поверинов

31 августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Организационное и правовое обеспечение информационной безопасности»

Направление подготовки (специальность) – 10.03.01 «Информационная безопасность»

Квалификация (степень) выпускника – бакалавр

Профиль «Информационно-аналитические системы финансового мониторинга»

Академический бакалавриат

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», утвержденного приказом Министерства образования и науки №1515 от 01.12.2016 г.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

старший преподаватель



С.О. Иванов

ОБСУЖДЕНО:

на заседании кафедры математического и аппаратного обеспечения информационных систем «30» августа 2017г., протокол №1

заведующий кафедрой
СОГЛАСОВАНО:



Д.В. Ильин

Методическая комиссия факультета информатики и вычислительной техники «30» августа 2017г., протокол №1

Декан факультета



А.В. Щипцова

Директор научной библиотеки



Н.Д. Никитина

Начальник управления информатизации



И.П. Пивоваров

Начальник учебно-методического управления



В.И. Маколов

Оглавление

1. Цель и задачи обучения по дисциплине	4
2. Место дисциплины в структуре основной образовательной программы (ООП)	4
3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП	4
4. Структура и содержание дисциплины	5
4.1. Содержание дисциплины	5
4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения.....	6
5. Содержание разделов дисциплины	6
5.1. Лекции и практические занятия.....	6
5.2. Вопросы для самостоятельной работы студента	9
6. Образовательные технологии	10
7. Формы аттестации и оценочные материалы	10
7.1. Вопросы к зачету.....	10
7.2. Оценивание результатов зачета.....	11
8. Учебно-методическое и информационное обеспечение дисциплины	11
8.1. Рекомендуемая основная литература	11
8.2. Рекомендуемая дополнительная литература.....	12
8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы. 12	
8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.....	12
9. Материально-техническое обеспечение дисциплины.....	13
10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями . 13	
11. Методические рекомендации по освоению дисциплины	14

1. Цель и задачи обучения по дисциплине

Дисциплина «Организационное и правовое обеспечение информационной безопасности» направлена на освоение обучаемыми нормативно-правовой базы в области обеспечения информационной безопасности.

Основными задачами дисциплины являются:

- участие в разработке технологической и эксплуатационной документации;
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к числу дисциплин базовой части. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Философия», «Информатика».

Дисциплина является предшествующей для дисциплин: «Основы управления информационной безопасностью», «Защита персональных данных», «Основы контрольно-надзорной деятельности», «Принципы построения, проектирования и эксплуатации информационных и аналитических систем», «Методология и организация и информационно-аналитического мониторинга», «Информационные технологии в финансах и банковской деятельности», прохождения производственных и преддипломной практик, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

- способность использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);
- способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);
- способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15).

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

- иерархию нормативно-правовых документов РФ (31);
- основные нормативные правовые акты в области информационной безопасности (32);
- систему нормативно-правовых актов в сфере информационной безопасности (33);
- нормативные правовые и методические документы регуляторов в сфере обеспечения информационной безопасности (34);

уметь:

- работать с правовыми информационно-справочными системами (У1);
- находить, классифицировать и интерпретировать нормативно-правовые акты в области информационной безопасности (У2);

- выполнять требования регуляторов и стандартов в области обеспечения информационной безопасности (У3);
 - организовывать технологический процесс защиты информации ограниченного доступа соответствующий требованиям регуляторов (У4)
- владеть:
- организационными мерами обеспечения информационной безопасности организации (Н1);
 - навыками выполнения требований нормативно-правовых актов (Н2);
 - навыками применения регламентов и стандартов для обеспечения информационной безопасности (Н3);
 - организационными мерами защиты информации ограниченного доступа (Н4).

4. Структура и содержание дисциплины

Образовательная деятельность по дисциплине проводится:

- в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);
- в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (практические занятия), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения:

Л – лекции, л/р – лабораторные работы, п/р – практические занятия, КСР – контроль самостоятельной работы, СРС – самостоятельная работа студента, ИФР – интерактивная форма работы, К – контроль.

4.1. Содержание дисциплины

Содержание	Формируемые компетенции	Формируемые ЗУН
Раздел 1. Правовые основы защиты ИБ.	ОК-4, ОПК-5	31,32, У1, У2
Тема 1.1. Система нормативно-правовых актов в сфере ИБ.		
Тема 1.2. Государственная система защиты информации.		
Тема 1.3. Государственная информация.		
Тема 1.4. Коммерческая информация.		
Тема 1.5. Персональная информация.		
Тема 1.6. Частная информация.		
Тема 1.7. Ответственность за нарушение в сфере ИБ.		
Тема 1.8. Лицензирование в области защиты информации.		
Тема 1.9. Сертификация и стандартизация.		
Тема 1.10. Стандарты и методические указания.		
Раздел 2. Организационные меры защиты ИБ.	ПК-10, ПК-15	33,34, У3,У4, Н3,Н4
Тема 2.11. Организационные меры		
Тема 2.12. Организация режимов и мероприятий по обеспечению информационной безопасности.		
Тема 2.13. Организация работы с источниками и носителями данных.		
Тема 2.14. Организация работы с программно-аппаратными средствами организации.		
Тема 2.15. Организация работы с персоналом.		

Тема 2.16. Организация аналитической работы и контроля.		
Зачет	ОПК-5, ПК-10, ПК-15	32, 33, 34, У2, У3, У4, Н2, Н3, Н4

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения

Содержание	Всего, час	Контактная работа, час				СРС, час	ИФР, час	К, час
		Л	л/р	п/р	КСР			
Раздел 1. Правовые основы защиты ИБ.								
Тема 1.1. Система нормативно-правовых актов в сфере ИБ.	6	2		2		2	2	
Тема 1.2. Государственная система защиты информации.	6	2		2		2	2	
Тема 1.3. Государственная информация.	6	2		2		2	2	
Тема 1.4. Коммерческая информация.	6	2		2		2	2	
Тема 1.5. Персональная информация.	6	2		2		2	2	
Тема 1.6. Частная информация.	6	2		2		2	2	
Тема 1.7. Ответственность за нарушение в сфере ИБ.	6	2		2		2	2	
Тема 1.8. Лицензирование в области защиты информации.	6	2		2		2	2	
Тема 1.9. Сертификация и стандартизация.	6	2		2		2	2	
Тема 1.10. Стандарты и методические указания.	8	2		2		4	2	
Раздел 2. Организационные меры защиты ИБ.								
Тема 2.11. Организационные меры	8	2		2		4	2	
Тема 2.12. Организация режимов и мероприятий по обеспечению информационной безопасности.	8	2		2		4	2	
Тема 2.13. Организация работы с источниками и носителями данных.	6	2		2		2	2	
Тема 2.14. Организация работы с программно-аппаратными средствами организации.	6	2		2		2	2	
Тема 2.15. Организация работы с персоналом.	6	2		2		2	2	
Тема 2.16. Организация аналитической работы и контроля.	8	2		2		4	2	
Зачет	4				2	2		
Итого	108 3 з.е.	32	0	32	2	42	32	0

5. Содержание разделов дисциплины

5.1. Лекции и практические занятия

Раздел 1. Правовые основы защиты ИБ.

Тема 1.1. Система нормативно-правовых актов в сфере ИБ.

Лекция 1. Система нормативно-правовых актов в сфере ИБ.

1. Иерархия нормативно-правовых документов РФ. Виды и источники нормативно-правовых актов.

2. Источники правового регулирования информационных отношений. Международные договоры, конституционно-правовые акты и стратегии в области информации.

3. Классификация информации. Виды информации согласно №149-ФЗ и других нормативно-правовых актов.

Практическое занятие 1. Справочно-правовые системы.

Тема 1.2. Государственная система защиты информации.

Лекция 2. Государственная система защиты информации.

1. Роль государства в сфере информационной безопасности. Постановление о государственной системе защиты информации.

2. Структура ГСЗИ. Взаимосвязь между государственными органами в ГСЗИ. Требования к госслужащим.

3. Государственные органы по защите ИБ. Сфера ответственности и регламент работы государственных органов.

Практическое занятие 2. Регламенты ГСЗИ.

Тема 1.3. Государственная информация.

Лекция 3. Государственная информация.

1. Государственные информационные системы. Особенности ГИС-ов, положения и требования регламентирующие их работу.

2. Государственная тайна. Виды информации составляющие государственную тайну. Требования по защите государственной тайны.

3. Служебная тайна, тайна следствия и судопроизводства. Понятие служебной тайны. Законодательное регулирование служебных тайн.

Практическое занятие 3. ГИС.

Тема 1.4. Коммерческая информация.

Лекция 4. Коммерческая информация.

1. Коммерческая тайна. Законодательное регулирование коммерческой тайны. Защита коммерческой тайны.

2. Профессиональная тайна и тайна изобретения. Особенности профессиональной тайны и тайны изобретения.

3. Банковская тайна. Центробанк РФ. Источники требований по соблюдению банковской тайны.

Практическое занятие 4. Коммерческая тайна.

Тема 1.5. Персональная информация.

Лекция 5. Персональная информация.

1. Персональные данные. Предпосылки правового регулирования персональных данных.

2. Закон о персональных данных. Основные понятия, права субъекта, ответственность и обязанности оператора, требования государства.

3. Защита персональных данных. Требования руководящих документов по защите персональных данных.

Практическое занятие 5. Персональные данные.

Тема 1.6. Частная информация.

Лекция 6. Гражданская информация.

1. Частная тайна. Понятие личной и семейной тайны. Тайна переписки и связи.

2. Интеллектуальная собственность. Виды интеллектуальной собственности. Регулирование отношений связанных с интеллектуальной собственностью.

3. Электронная подпись. Виды электронных подписей. Требования к содержанию и работе.

Практическое занятие 6. Цифровая подпись.

Тема 1.7. Ответственность за нарушение в сфере ИБ.

Лекция 7. Ответственность за нарушение в сфере ИБ.

1. Уголовный кодекс. Уголовная ответственность за преступления связанные с информационной безопасностью.

2. Кодекс об административных правонарушениях. Административные правонарушения в области информационной безопасности.

3. Гражданский кодекс. Защита гражданских прав в области информационной безопасности.

Практическое занятие 7. Юридическая ответственность.

Тема 1.8. Лицензирование в области защиты информации.

Лекция 8. Лицензирование в области защиты информации.

1. Лицензирование. Сфера действия, основные понятия, лицензионный контроль.

2. Лицензирование криптографии. Область действия. Виды деятельности и лицензионные требования.

3. Лицензирование специальных технических средств и работ с ними. Область действия. Виды деятельности и лицензионные требования.

4. Лицензирование средств и деятельности по защите ИБ. Область действия. Виды деятельности и лицензионные требования.

Практическое занятие 8. Лицензирование.

Тема 1.9. Сертификация и стандартизация.

Лекция 9. Сертификация и стандартизация.

1. Техническое регулирование. ФЗ "О техническом регулировании". Основные понятия и принципы технического регулирования.

2. Сертификация и аттестация средств защиты информации.

3. Нормы аудита. Требования к проведению аудиторских проверок.

Практическое занятие 9. Сертификация средств.

Тема 1.10. Стандарты и методические указания.

Лекция 10. Руководящие документы ФСТЭК.

1. Приказы ФСТЭК в области технической защиты информации. Требования к обеспечению защиты информации.

2. Специальные нормативные документы ФСТЭК в области защиты информации. Меры защиты и методические указания.

Практическое занятие 10. Руководящие документы ФСТЭК.

Раздел 2. Организационные меры защиты ИБ.

Тема 2.11. Организационные меры

Лекция 11. Организационные меры

1. Область действия организационно-режимных мер. Роль организационно-режимных мер в системе информационной безопасности.

2. Требования к организационно-режимным мерам. Принципы и ограничения организационно-режимных мер.

3. Особенности организационно-режимных мер. Достоинства и недостатки организационно-режимных мер.

Практическое занятие 11. Требования к организационно-режимным мерам.

Тема 2.12. Организация режимов и мероприятий по обеспечению информационной безопасности.

Лекция 12. Организация режимов и мероприятий по обеспечению информационной безопасности.

1. Режим безопасности в организации. Организация внутриобъектового и пропускного режимов. Работа с посетителями, клиентами и поставщиками.

2. Физическая защита информационной безопасности. Охрана информационной безопасности на физическом уровне.

Практическое занятие 12. Служба безопасности.

Тема 2.13. Организация работы с источниками и носителями данных.

Лекция 13. Организация работы с источниками и носителями данных.

1. Организация хранения и использования документов и носителей. Определение правил выдачи, ведение журналов выдачи и использования

2. Правила использования внешних и внутренних источников данных. Определение режима доступа в сеть Интернет. Регламента обслуживания систем хранения данных.

Практическое занятие 13. Источники информации.

Тема 2.14. Организация работы с программно-аппаратными средствами организации.

Лекция 14. Организация работы с программно-аппаратными средствами организации.

1. Правила использования средств защиты. Политика настроек антивирусов и сетевых экранов.

2. Правила использования средств аутентификации. Политика использования паролей и токенов.

Практическое занятие 14. Средства защиты.

Тема 2.15. Организация работы с персоналом.

Лекция 15. Организация работы с персоналом.

1. Управление персоналом. Основные этапы работы с сотрудниками: найм, обучение, контроль, увольнение.

2. Обеспечение выполнения правил персоналом. Направления деятельности по предотвращению нарушений. Методы мотивации.

Практическое занятие 15. Управление персоналом.

Тема 2.16. Организация аналитической работы и контроля.

Лекция 16. Организация аналитической работы и контроля.

1. Служба безопасности. Права и ограничения службы безопасности. Этика службы безопасности. Внешняя разведка и мониторинг безопасности.

2. Расследование инцидентов. Принципы и способы расследования. Процесс расследования.

Практическое занятие 16. Служба безопасности.

5.2. Вопросы для самостоятельной работы студента.

Раздел 1. Правовые основы защиты ИБ.

1. Иерархия нормативно-правовых документов РФ по ГИС.
2. Иерархия нормативно-правовых документов РФ по государственной тайне.
3. Иерархия нормативно-правовых документов РФ по служебной тайне.
4. Иерархия нормативно-правовых документов РФ по коммерческой тайне.
5. Иерархия нормативно-правовых документов РФ по профессиональной тайне.
6. Иерархия нормативно-правовых документов РФ по банковской тайне.
7. Иерархия нормативно-правовых документов РФ по персональным данным.
8. Иерархия нормативно-правовых документов РФ по интеллектуальной собственности.
9. Иерархия нормативно-правовых документов РФ личной, семейной тайне, тайне связи и сообщений.

Раздел 2. Организационные меры защиты ИБ.

1. Правила работы с источниками и носителями данных.
2. Правила работы с работы с программно-аппаратными средствами организации.
3. Правила работы с средствами защиты информации.
4. Правила работы с персоналом

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

- применения знаний на практике, поиска новой учебной информации;
- организации совместной и самостоятельной деятельности обучающихся;

В соответствии с требованиями ФГОС ВО для реализации компетентного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

- лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;
- практические занятия, проводимые под руководством преподавателя в учебной аудитории, направленные на углубление и овладение определенными методами самостоятельной работы, могут включать коллективное обсуждение материала, дискуссии, решение и разбор конкретных практических ситуаций, компьютерные симуляции, тренинги и др.;

Все занятия обеспечены мультимедийными средствами (SMART доски, проекторы, экраны) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: аннотирование и конспектирование литературы по теме, составление вопросов и тестов к теме.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента на практическом занятии, его доклада; проверка письменных отчетов по результатам выполненных заданий. Результаты самостоятельной работы учитываются при оценке знаний на зачёте.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся.

7.1. Вопросы к зачету

1. Иерархия нормативно-правовых документов РФ
2. Виды информации согласно 149ФЗ
3. Особенности ГИС.
4. Источники официальной информации.
5. Чем ограничивается численность госслужащих.
6. Требования к госслужащим.
7. Структура ГСЗИ.
8. Что такое государственная тайна.
9. Особенности защиты государственной тайны.

10. Регламентация служебной тайны.
11. Другие виды служебной тайны.
12. Как установить режим коммерческой тайны?
13. Роль ЦБ в системе защиты информации.
14. Зачем нужно защищать персональную информации.
15. Законы и приказы регулирующие персональную информацию.
16. Зачем нужна защита авторского и интеллектуального права?
17. Правовой статус цифровой подписи.
18. Ответственность за незаконное распространение ПО.
19. Ответственность за намеренное искажение и заведомо ложную информацию.
20. Максимальная и минимальная ответственность за нарушение ИБ.
21. Основные этапы получения лицензии.
22. Как сэкономить на получении лицензии на криптографии и деятельности по защите ИБ.
23. Как сэкономить на получении лицензии на производство и выявление "жучков".
24. Зачем нужны различные виды сертификации.
25. Получение технических регламентов и стандартов.
26. Особенности аудита ИБ.
27. Взаимосвязь РД ФСТЭК.
28. Достоинства и недостатки организационно-режимных мер.
29. Проект и план ИС.
30. Виды правил безопасности ISO/IEC 27002.
31. Статистика нарушений ИБ персоналом.
32. Этика службы безопасности.
33. Права и ограничения службы безопасности.

7.2. *Оценивание результатов зачета.*

Зачет проводится по окончании занятий по дисциплине до начала экзаменационной сессии в период недели контроля самостоятельной работы.

Билет для проведения промежуточной аттестации в форме зачета включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Оценка «зачтено» проставляется студенту, выполнившему и защитившему в полном объеме практические задания в течение семестра, имеются твердые и полные знания программного материала, правильные действия по применению знаний на практике, четкое изложение материала

Оценка «не зачтено» проставляется студенту, не выполнившему и (или) не защитившему в полном объеме практические задания в течение семестра, либо наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке <http://library.chuvsu.ru/>

8.1. *Рекомендуемая основная литература*

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс] : учебное пособие / Ю.Н.

	Сычев. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 195 с. — 978-5-4487-0128-3. — Режим доступа: http://www.iprbookshop.ru/72345.html
2.	Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учебное пособие / Г.П. Жигулин. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2014. — 174 с. Режим доступа: http://www.iprbookshop.ru/67451.html

8.2. Рекомендуемая дополнительная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Тихонов, В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты : [учебное пособие для вузов] / В. А. Тихонов, В. В. Райх. - М. : Гелиос АРВ, 2006. - 527с.
2.	Гатчин Ю.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Ю.А. Гатчин, Е.В. Климова. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2009. — 84 с. Режим доступа: http://www.iprbookshop.ru/67463.html
3.	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017. — 325 с. Режим доступа: www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-E6BAEF354847 .

8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке <http://ui.chuvsu.ru/>*

8.3.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
	MS Windows/Arch linux	лицензия университета/ свободное лицензионное соглашение (https://www.archlinux.org/download/)
	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)

8.3.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)*
2.	Консультант +	

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	ISO 27000 Международные стандарты управления информационной безопасностью.	http://iso27000.ru
2.	Информационная безопасность. Практика	http://dorlov.blogspot.com

	информационной безопасности.	
3.	SecurityLab. Информационный портал по безопасности.	http://www.securitylab.ru
4.	Xgu.ru.	http://xgu.ru/wiki/
5.	Российская Государственная Библиотека	http://www.rsl.ru
6.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
7.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
8.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
9.	Научная электронная библиотека	http://elibrary.ru
10.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
11.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

- ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);
- мультимедийный проектор с дистанционным управлением;

Учебные аудитории для практических и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединённых локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

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

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

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

11. Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к практическим занятиям рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. Желательно подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие. Готовясь к докладу или реферативному сообщению, рекомендуется обращаться за методической помощью к преподавателю, составить план-конспект своего выступления, продумать примеры с целью обеспечения тесной связи изучаемой теории с практикой. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании выпускной квалификационной работы.

Формы организации студентов на практических занятиях: фронтальная. При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу.