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
«Основы информационной безопасности»

Направление подготовки (специальность) – 10.03.01 «Информационная безопасность»

Квалификация (степень) выпускника – бакалавр

Профиль «Информационно-аналитические системы финансового мониторинга»

Академический бакалавриат

Чебоксары – 2017

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 _____ Д.В. Ильин

СОГЛАСОВАНО:

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 6
5.2. Лабораторные работы 8
5.3. Вопросы для самостоятельной работы студента. 8
6. Образовательные технологии 9
7. Формы аттестации и оценочные материалы 9
7.1. Вопросы к зачету 10
7.2. Оценивание результатов зачета. 10
8. Учебно-методическое и информационное обеспечение дисциплины 11
8.1. Рекомендуемая основная литература 11
8.2. Рекомендуемая дополнительная литература 11
8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы. . 11
8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы. 12
9. Материально-техническое обеспечение дисциплины 12
10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями 12
11. Методические рекомендации по освоению дисциплины 13

1. Цель и задачи обучения по дисциплине

Дисциплина «Основы информационной безопасности» направлена на изучение комплексного подхода к обеспечению информационной безопасности в организациях и состоит в изучении способов управления методами и средствами защиты информации, а так же приёмов их интеграции в инфраструктуру предприятия. Основными задачами дисциплины являются:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности.

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

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

Дисциплина является предшествующей для дисциплин: «Техническая защита информации», «Криптографические методы защиты информации», «Программно-аппаратные средства защиты информации», «Основы управления информационной безопасностью», «Безопасность операционных систем».

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

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

- способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);
- способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);
- способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);
- способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13).

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

знать:

- принципы и способы обеспечения информационной безопасности (З1);
- угрозы безопасности информации и возможные пути их реализации (З2);
- теоретические, нормативно-правовые, организационно-режимные и технические методы обеспечения информационной безопасности (З3);
- основные принципы защиты информации (З4);

уметь:

– проводить исследование информационных ресурсов требующих защиту (У1);

– анализировать структуру и содержание информационных процессов и особенностей функционирования объекта защиты (У2);

– применять прикладные и специальные программные средства, системы программирования для реализации методов защиты информации (У3);

– применять полученные знания для решения базовых задач обеспечения информационной безопасности (У4);

владеть навыками:

– поиска информации в области обеспечения информационной безопасности и защиты интересов личности, общества и государства (Н1);

– исследования угроз безопасности информации и возможных путей их реализации (Н2);

– специальными программными средствами используемыми для защиты информации (Н3);

– применения теоретических, нормативно-правовых, организационно-режимных и технических методов обеспечения информационной безопасности (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 (семинары, практические занятия, лабораторные работы, практикумы), 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. Теоретические методы обеспечения информационной безопасности	ОК-5, ОПК-7, ПК-2, ПК-13	З1-З4, У1-У4, Н1-Н2
Тема 1.1. Информация, информационная безопасность		
Тема 1.2. Теоретические методы информационной безопасности.		
Тема 1.3. Обеспечение конфиденциальности, целостности, доступности.		
Раздел 2. Нормативно-правовое обеспечение информационной безопасности	ОПК-7, ПК-13	З2, З4, У2, У4
Тема 2.1. Компьютерное право и преступления.		
Тема 2.2. Нормы информационной безопасности.		
Раздел 3. Организационно-режимное обеспечение ИБ	ОК-5, ОПК-7, ПК-13	З1, З2, З4, У1, У2, У4
Тема 3.1. Управление информационной безопасностью.		
Тема 3.2. Планы безопасности.		
Раздел 4. Техническое обеспечение ИБ	ПК-2	З3, У3, Н3
Тема 4.1. Технические средства защиты информации.		
Зачет	ОПК-7, ПК-2, ПК-13	З1-З4, У1-У4, Н1-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. Теоретические методы обеспечения информационной безопасности								
Тема 1.1. Информация, информационная безопасность	6	2	2			2	2	
Тема 1.2. Теоретические методы информационной безопасности.	12	4	4			4	2	
Тема 1.3. Обеспечение конфиденциальности, целостности, доступности.	23	6	8			9	4	
Раздел 2. Нормативно-правовое обеспечение информационной безопасности								
Тема 2.1. Компьютерное право и преступления.	6	2	2			2	2	
Тема 2.2. Нормы информационной безопасности.	14	4	4			6	2	
Раздел 3. Организационно-режимное обеспечение ИБ								
Тема 3.1. Управление информационной безопасностью.	14	4	4			6	2	
Тема 3.2. Планы безопасности.	12	4	4			4	2	
Раздел 4. Техническое обеспечение ИБ								
Тема 4.1. Технические средства защиты информации.	19	6	4			9	2	
Зачет	2				2			
Итого	108 3 з.е.	32	32	0	2	42	18	0

5. Содержание разделов дисциплины

5.1. Лекции

Раздел 1. Теоретические методы обеспечения информационной безопасности=6

Тема 1.1. Информация, информационная безопасность

Лекция 1. Информационная безопасность

1. Информация. Определение, особенности, виды информации.

2. Компрометация информации. Базовые критерии информационной безопасности. Конфиденциальность, целостность, доступность.

3. Информационная безопасность. Определение и структура ИБ. Подходы к обеспечению и управлению ИБ. Классификация способов защиты информации

Тема 1.2. Теоретические методы информационной безопасности.

Лекция 2. Риски информационной безопасности

1. Понятие риска. Определение и структура риска. Термины риск-менеджмента.

2. Классификация угроз, уязвимостей, последствий. Особенности рисков ИБ.

3. Управление рисками. Процесс риск-менеджмента: анализ, оценка, обработка.

Лекция 3. Теория защиты информации

1. Основы ТЗИ. Аксиомы, понятия, принципы ТЗИ. Формальное описание процессов ТЗИ.

2. Формальная модель безопасности. Роль и классификация. Проблемы и принципы использования моделей.

3. Наиболее распространённые модели безопасности. Описание наиболее распространённых моделей, их достоинств и недостатков.

Тема 1.3. Обеспечение конфиденциальности, целостности, доступности.

Лекция 4. Обеспечение конфиденциальности. Шифрование

1. Криптология. Цели и задачи криптографии и криптологии.

2. Шифрование и расшифрование. Принципы и способы шифрования. Типы шифров.

3. Атаки на шифры. Классификация способов атак на шифры.

4. Стеганография. Цели и задачи стеганографии.

Лекция 5. Обеспечение целостности. Хеширование.

1. Хеширование. Цели, задачи, принципы хеширования. Процесс хеширования.

2. Хеш-функция. Виды хеш-функций.

3. Атаки на хеш. Проблемы и способы атак на хеш.

4. Цифровая подпись. Сущность ЦП, отличие от шифрования.

Лекция 6. Обеспечение доступности. Контроль доступа.

1. Авторизация. Цели и задачи принципы авторизации

2. Модели авторизации. Принцип работы подсистемы авторизации. Критерии авторизации. Модели управлением допуском.

3. Атаки на подсистему авторизации. Проблемы и классификация атак.

4. Архивация. Элементы обеспечения сохранности и доступности данных.

Раздел 2. Нормативно-правовое обеспечение информационной безопасности

Тема 2.1. Компьютерное право и преступления.

Лекция 7. Киберправо.

1. Компьютерные преступления. Цели и задачи киберправа. Категории и виды компьютерных преступлений.

2. Трансграничные преступления. Особенности и проблемы трансграничных преступлений.

3. Расследование киберпреступлений. Проблемы и способы расследований киберпреступлений.

Тема 2.2. Нормы информационной безопасности.

Лекция 8. Проверка информационной безопасности.

1. Проверка информационной безопасности. Цели и задачи оценки ИБ. Способы оценки ИБ.

2. Аудит. Цели, принципы, виды аудита. Требования к аудитору.

3.Пентест.

Лекция 9. Стандарты и методические указания.

1. Оранжевая книга. Структура стандарта, достоинства и недостатки. Требования и классы защищенности.

2. Общие критерии. Структура стандарта. Функциональные и доверительные требования.

3. Серия стандартов 27000. Состав серии, основные стандарты и их содержание.

Раздел 3. Организационно-режимное обеспечение ИБ

Тема 3.1. Управление информационной безопасностью.

Лекция 10. СУИБ

1. Структура СИУБ. Определение и структура СУИБ.

2. Проектирование СУИБ. Принципы построения. План и проект СУИБ

3. Жизненный цикл СУИБ. Переход от проекта СМИБ к плану его построения.

Лекция 11. Политика безопасности организации

1. Понятие политики безопасности. Определение, виды и структура политики.

2. Формализация принципов защиты. Модели защищенности, угроз, нарушителей.

3. Архитектура безопасности организации. Модель доступа и доверенная компьютерная база.

Тема 3.2. Планы безопасности.

Лекция 12. Непрерывность бизнес-процессов

1. Реагирование на инциденты. Процесс реагирования на инциденты. Анализ влияния на бизнес. Планы непрерывности.

2. Разработка плана непрерывности бизнеса. Состав плана непрерывности. Процедура разработки плана непрерывности.

Лекция 13. Расследование инцидентов

1. Расследование компьютерных преступлений. Особенности расследований компьютерных преступлений. Принципы расследования. Способы расследования.

2. Процедура расследования инцидента. Последовательность действий при расследовании инцидента. Способы локализации места преступления.

Раздел 4. Техническое обеспечение ИБ

Тема 4.1. Технические средства защиты информации.

Лекция 14. Инженерно-технические

1. Физические угрозы ИБ. Классификация и виды угроз. Направления защиты.

2. Средства физической защиты. Виды защиты и особенности применения.

3. Аппаратные средства защиты.

Лекция 15. Программно-аппаратные средства защиты.

1. Средства администрирования. Управление ключами (Publickeyinfrastructure). Служба каталогов

2. Контроль периметра. Сетевые экраны. Демилитаризованная зона (DMZ)

3. Защита служб. Антивирусы.

4. Восстановление целостности. Резервные копии, Транзакции. RAID.

5. Средства мониторинга. Система обнаружения атак (IDS, IPS). Системы защиты от утечек (DLP).

5.2. Лабораторные работы

Тема	Количество часов
Лабораторная работа 1. Конфиденциальность, целостность, доступность.	2
Лабораторная работа 2. Риски ИБ.	2
Лабораторная работа 3. Модели безопасности.	2
Лабораторная работа 4. Шифрование.	2
Лабораторная работа 5. Хеширование.	2
Лабораторная работа 6. Контроль доступа.	4
Лабораторная работа 7. Киберпреступления.	2
Лабораторная работа 8. Анализ защищенности.	4
Лабораторная работа 9. Организационно-режимные меры.	2
Лабораторная работа 10. Архитектура системы безопасности.	2
Лабораторная работа 11. Реагирование на инциденты.	2
Лабораторная работа 12. Расследование инцидентов.	2
Лабораторная работа 13. Физическая защита информации.	2
Лабораторная работа 14. Применение СЗИ.	2
Итого	32

5.3. Вопросы для самостоятельной работы студента.

Раздел 1. Теоретические методы обеспечения информационной безопасности

1. Классификация угроз, уязвимостей, последствий.
2. Описание наиболее распространённых моделей, их достоинств и недостатков.
3. Стеганография.
4. Цифровая подпись
5. Архивация.

Раздел 2. Нормативно-правовое обеспечение информационной безопасности

1. Киберэтика.

2. Аудит.
3. Оранжевая книга.

Раздел 3. Организационно-режимное обеспечение ИБ

1. Жизненный цикл СУИБ.
2. Архитектура безопасности организации.
3. Анализ влияния на бизнес.
4. Способы расследования компьютерных преступлений.

Раздел 4. Технические средства защиты информации.

1. Средства физической защиты информации.
2. Программно-аппаратные средства защиты.

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 (учебно-познавательной, научно-исследовательской, частично-поисковой, репродуктивной, творческой и пр.).

В соответствии с требованиями ФГОС ВО для реализации компетентностного 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.;

– лабораторные занятия, проводимые под руководством преподавателя в учебной лаборатории с использованием компьютеров и учебного оборудования, направленные на закрепление и получение новых умений и навыков, применение знаний и умений, полученных на теоретических занятиях, при решении практических задач 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 отчётов по результатам выполненных. 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. Чем угроза ИБ отличается от уязвимости ИБ?
2. Дайте определение понятию риска.
3. Приведите примеры наиболее распространённых современных уязвимостей.
4. Чем отличается модель безопасности Белла-ЛаПадулы от
5. модели дискреционного доступа (DAC)?
6. Что такое RBAC?
7. Что означает слово «криптология» и кем оно введено?
8. Какие недостатки имеют несимметричные методы шифрования перед симметричными?
9. В чем заключается проблема управления ключами?
10. Где используется стеганография?
11. В каких случаях применяется хеширование?
12. Какие существуют хеш-функции?
13. Опишите принцип работы цифровой подписи документа.
14. Опишите принципы контроля доступа.
15. Опишите принципы цифрового хранения информации.
16. Что такое киберправо?
17. Перечислите категории компьютерных преступлений?
18. Какие существуют способы оценки ИБ.
19. Что такое аудит?
20. Перечислите критерии оценки доверенных компьютерных систем ?
21. Почему в оранжевой книге представлена информация не о безопасных, а о доверенных системах?
22. Кто использует РД ФСТЭК?
23. Назовите цели, задачи и принципы международного стандарта 15408?
24. Какие преимущества дают общие критерии?
25. Какую роль играют организационно-режимные меры в сфере ИБ?
26. Опишите принципы построение системы защитных мер.
27. Дайте определение понятию политика безопасности.
28. Как вы понимаете термин «непрерывность бизнеса»?
29. Опишите процедуру расследования инцидента.
30. Назовите основные угрозы физической безопасности.
31. Назовите программные средства для контроля периметра.
32. Опишите принципы работы антивируса?
33. Какие существуют виды сетевых экранов?

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 лабораторные работы в течение семестра, чей уровень знаний, умений и навыков соответствует уровню оценок «отлично», «хорошо» или «удовлетворительно» (п.2.1). Оценка «не зачтено» проставляется студенту, не выполнившему и (или) не защитившему в полном объеме лабораторные работы в течение семестра, либо чей уровень знаний, умений и навыков соответствует уровню оценки «неудовлетворительно».

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.	Нестеров С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С.А.. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 c. Режим доступа: http://www.iprbookshop.ru/43960.html
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 c. Режим доступа: http://www.iprbookshop.ru/67463.html
3.	Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c. Режим доступа: http://www.iprbookshop.ru/52209.html

8.2. Рекомендуемая дополнительная литература

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

№ п/п	Наименование
1.	Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс] : учебно-методический комплекс / Ю.Н. Сычев. — Электрон. текстовые данные. — М. : Евразийский открытый институт, 2012. — 342 c. Режим доступа: http://www.iprbookshop.ru/14642.html.
2.	Горбенко А.О. Основы информационной безопасности (введение в профессию) [Электронный ресурс] : учебное пособие / А.О. Горбенко. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 335 c. Режим доступа: http://www.iprbookshop.ru/66797.html
3.	Информационная безопасность и защита информации [Электронный ресурс] : учебно-методический комплекс — Алматы: Нур-Принт, 2012. — 98 c. Режим доступа: http://www.iprbookshop.ru/67055.html

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/CentOS	лицензия университета/ свободное лицензионное соглашение (https://www.centos.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 информационной безопасности.	http://dorlov.blogspot.com
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, лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных 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 лабораторным работам 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. 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 лабораторных работах фронтальная. При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу.

Если в результате выполнения лабораторной работы запланирована подготовка письменного отчета, то отчет о выполненной работе необходимо оформлять в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.