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
«Защита информации в распределенных вычислительных системах»

Специальность – 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) выпускника – Специалист по защите информации

Специализация – «Безопасность открытых информационных систем»

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом Министерства образования и науки №1509 от 01.12.2016 г.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):
Доцент, к.ф.-м.н. Д.В.Ильин
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 4
4. Структура и содержание дисциплины 5
4.1. Содержание дисциплины 6
4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения 6
5. Содержание разделов дисциплины 7
5.1. Лекции и практические занятия 7
5.2. Лабораторные работы 9
5.3. Вопросы для самостоятельной работы студента. 9
6. Образовательные технологии 9
7. Формы аттестации и оценочные материалы 10
7.1. Вопросы к экзамену 10
7.2. Оценивание результатов экзамена 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 13

1. Цель и задачи обучения по дисциплине

Целью преподавания дисциплины является формирование целостного представления об организации информационной безопасности открытых информационных систем, получение теоретических знаний о принципах построения и архитектуре открытых систем (в том числе распределенных), обеспечивающих организацию вычислительных процессов в корпоративных информационных системах экономического, управленческого, производственного, научного и другие назначения, а также практических навыков по созданию (настройке) конфигурации информационной системы для реализации бизнес процессов в корпоративных сетях предприятий.

Задачами дисциплины являются:

- раскрытие сущности, целей и задач открытых информационных систем;
- изучение и исследование механизмов обеспечения информационной безопасности в открытых информационных системах;
- знакомство с процессами обеспечения информационной безопасности в открытых информационных системах и освоение подходов их моделирования.

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

Дисциплина «Защита информации в распределенных вычислительных системах» 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 дисциплин: «Управление информационной безопасностью», «Открытые информационные системы».

Дисциплина является предшествующей для прохождения практик и государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

- способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);
- способностью проводить анализ защищенности автоматизированных систем (ПК-3);
- способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);
- способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);
- способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.5);
- способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.2);
- способностью участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы (ПСК-4.4).

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

знать:

- подходы к интеграции сетей в распределенных информационных системах (З1);

- принципы работы сетевых протоколов и технологий передачи данных в распределенных информационных системах (З2);
- основные методы и средства реализации удаленных сетевых атак на распределенных информационные системы (З3);
- о политиках безопасности и мерах защиты в распределенных информационных системах (З4);
- о комплексном подходе к построению эшелонированной защиты для распределенных информационных систем (З5);
- состав и структуру политики информационной безопасности открытых информационных систем (З6);
- способы контроля обеспечения информационной безопасности открытой информационной системы (З7);

уметь:

- проектировать защищенные распределенные информационные системы (У1);
- определять и устранять основные угрозы информационной безопасности для распределенных информационных систем (У2);
- строить модель нарушителя информационной безопасности для распределенных информационных систем (У3);
- выявлять и устранять уязвимости в основных компонентах распределенных информационных систем (У4);
- применять стандартные решения для защиты информации в распределенных информационных системах и квалифицированно оценивать их качество (У5);
- используя современные методы и средства, разрабатывать и оценивать политику безопасности для распределенных информационных систем (У6);
- применять правила, процедуры, практические приемы, руководящие принципы, методы, средства для обеспечения информационной безопасности открытых информационных систем (У7);

владеть:

- навыками поиска информации о примерах применения нормативных правовых актов при построении распределенных вычислительных систем (Н1);
- терминологией и системным подходом построения защищенных распределенных информационных систем (Н2);
- инструментами используемых для создания средств защиты информации автоматизированной системы(Н3);
- навыками анализа угроз информационной безопасности и уязвимостей в распределенных информационных системах (Н4);
- эффективно применять комплекс мер для обеспечения информационной безопасности открытых информационных систем (Н5);
- навыками построения политик безопасности для распределенных информационных систем виртуальных сетей (Н6);
- проведения проверки обеспечения информационной безопасности открытой информационной системы (Н7).

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. Архитектура распределенных систем	ОПК-6, ПК-3, ПСК-4.5	З1,2,5, У1,2,5, Н1,2,5
Тема 1.1. Стандартизация и модельное представление распределенных информационных систем.		
Тема 1.2. Интранет как открытая система.		
Раздел 2. Угрозы распределенным системам	ПК-3, ПК-24, ПСК-4.4	З2,4,7, У2,4,7, Н2,4,7
Тема 2.1. Уязвимость распределенных систем		
Тема 2.2. Атаки на распределенные системы		
Раздел 3. Защита распределенных систем	ПК-13, ПК-24, ПСК-4.5, ПСК-4.2	З3,4,5,6, У3,4,5,6, Н3,4,5,6
Тема 3.1. Обеспечение информационной безопасности в распределенных системах.		
Тема 3.2. Аутентификация субъектов и объектов взаимодействия в распределенных системах.		
Тема 3.3. Виртуальные вычислительные сети.		
Тема 3.4. Межсетевые экраны.		
Экзамен	ПК-3, ПСК-4.5, ПСК-4.2, ПСК-4.4, ПК-24	З2,4-7, У2,4-7, Н2,4-7

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. Архитектура распределенных систем								
Тема 1.1. Стандартизация и модельное представление распределенных информационных систем.	14	2	2	4		6	2	
Тема 1.2. Интранет как открытая система.	12	2	2	4		4		
Раздел 2. Угрозы распределенным системам								
Тема 2.1. Уязвимость распределенных систем	12	2	2	4		4		
Тема 2.2. Атаки на распределенные системы	14	2	2	4		6	2	
Раздел 3. Защита распределенных систем								
Тема 3.1. Обеспечение информационной безопасности в распределенных системах.	12	2	2	4		4		
Тема 3.2. Аутентификация субъектов и объектов взаимодействия в открытых системах.	14	2	2	4		6	2	
Тема 3.3. Виртуальные вычислительные сети.	14	2	2	4		6	2	
Тема 3.4. Межсетевые экраны.	14	2	2	4		6	2	
Экзамен	38				2			36
Итого	144 4 з.е.	16	16	32	2	42	10	36

5. Содержание разделов дисциплины

5.1. Лекции и практические занятия

Раздел 1. Архитектура распределенных систем

Тема 1.1. Стандартизация и модельное представление распределенных информационных систем.

1. Роль стандартов в технологии распределенных систем. Основные группы стандартов и организации по стандартизации. Модель OSI и POSIX.
2. Основные элементы технологии открытых и распределенных информационных систем.
3. Совместимость открытых систем. Переносимость. Способность к взаимодействию.
4. Основные модели открытых систем.

Тема 1.2. Интранет как открытая система.

1. Разработка и управление Политикой использования ресурсов интранета
2. Понятие интранета. Интранет как часть среды открытых систем.
3. Интранет и экстранет. Портал и интранет.

Раздел 2. Угрозы распределенным системам

Тема 2.1. Уязвимость распределенных систем на примере интранета

1. Анализ угроз ИБ ресурсам интранета и причины их реализации.
2. Уязвимости операционных систем, серверов, рабочих станций, каналов связи.
3. Угрозы ресурсам интранета и причины их реализации.
4. Уязвимость архитектуры клиент-сервер.
5. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, World Wide Web, RPC, email.
6. Слабости современных технологий программирования.
7. Ошибки в программном обеспечении. Сетевые вирусы.

Тема 2.2. Атаки на распределенные системы

1. Атаки на открытые системы: анализ сетевого трафика, подмена доверенного объекта или субъекта, ложный объект, «отказ в обслуживании», удаленный контроль над станцией в сети.
2. Этапы реализации и уровни атак.
3. Атаки с использованием сетевых протоколов.
4. Удаленные атаки на открытые системы. Типичные сценарии и уровни атак.
5. Классические и современные методы, используемые нападающими для проникновения в открытые системы.

Раздел 3. Защита распределенных систем

Тема 3.1. Обеспечение информационной безопасности в распределенных системах.

1. Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408.
2. Разработка политики безопасности для открытых систем.
3. Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление.

4. Четырехуровневая модель открытой системы. Специфика защиты ресурсов открытых систем на примере интранета. Выбор сетевой топологии интранета при подключении к другим внешним сетям. Принципы создания защищенных средств связи объектов в открытых системах. Политика безопасности для открытых систем. Средства обеспечения информационной безопасности в открытых системах. Создание комплексной системы обеспечения безопасности открытых систем.

Тема 3.2. Аутентификация субъектов и объектов взаимодействия в распределенных системах.

1. Построение единых систем аутентификации, авторизации, персонализации, делегированного управления данными о субъектах и объектах и аудита доступа.
2. Анализ типовой модели аутентификации.
3. Подсистема аутентификации. Российский рынок средств аутентификации.

Тема 3.3. Виртуальные вычислительные сети.

1. Определение виртуальных частных вычислительных сетей (ВЧВС). Цели и задачи построения ВЧВС.
2. Виды ВЧВС в зависимости от решаемых задач: Intranet VPN, Client/server VPN, Extranet VPN, Remote Access VPN.
3. Специфика построения ВЧВС. Туннелирование в ВЧВС. Схема ВЧВС.
4. Политики безопасности для ВЧВС. Стандартные протоколы построения ВЧВС. Варианты построения ВЧВС. Виды ВЧВС в зависимости от решаемых задач. Топологии ВЧВС.
5. VPN-консорциум о ВЧВС. Рекомендации специалистов по выбору решений для построения ВЧВС. Проблемы и уязвимости современных ВЧВС. Виртуальные локальные вычислительные сети.

Тема 3.4. Межсетевые экраны.

1. Системы анализа защищенности. Системы обнаружения и предотвращения вторжений.
2. Типы межсетевых экранов: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, межсетевые экраны экспертного уровня, персональные межсетевые экраны.
3. Системы анализа защищенности. Системы обнаружения и предотвращения вторжений Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым экранам. Профили защиты для межсетевых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана. Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов.
4. Аудит и мониторинг информационной безопасности в открытых системах. Место и задачи систем анализа защищенности в защите открытых систем. Классификации систем анализа защищенности. Сетевые сканеры. Сканеры безопасности для приложений.
5. Критерии выбора сканеров безопасности. Методы отражения вторжений. Основы построения систем обнаружения вторжений. Системное обнаружение вторжений. Сетевое обнаружение вторжений.
6. Поведенческое обнаружение вторжений. Интеллектуальное обнаружение вторжений.
7. Комплексное обнаружение вторжений. Выбор системы обнаружения вторжений.

5.2. Лабораторные работы

Тема	Количество часов
Лабораторная работа 1. Моделирование распределенной вычислительной системы.	2
Лабораторная работа 2. Политика предоставления ресурсов распределенной системы.	2
Лабораторная работа 3. Атаки с помощью снифферов.	2
Лабораторная работа 4. DOS-атаки.	2
Лабораторная работа 5. Политика безопасности распределенных систем.	2
Лабораторная работа 6. Модульная система аутентификации – PAM.	2
Лабораторная работа 7. Виртуальные частные сети.	2
Лабораторная работа 8. Межсетевые экраны.	2
Итого	16

5.3. Вопросы для самостоятельной работы студента.

1. Угрозы ресурсам интранета и причины их реализации.
2. Уязвимость архитектуры клиент-сервер.
3. Слабости системных утилит, команд и сетевых сервисов.
4. Сетевые вирусы.
5. Удаленные атаки на открытые системы.
6. Виртуальные вычислительные сети.
7. Системы анализа защищенности.
8. Системы обнаружения и предотвращения вторжений.

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).

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.;

– 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.;

– 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: подготовка к лабораторным работам, подготовка реферативных сообщений, разработка проекта и др.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента на практическом занятии, его доклада; проверка письменных отчётов по результатам выполненных заданий и лабораторных работ; защита исследовательской работы. Результаты самостоятельной работы учитываются при оценке знаний на экзамене и 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 экзамена. Принимается экзамен преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся.

7.1. Вопросы к экзамену

2.Основные элементы технологии распределенных информационных систем.
3.Совместимость распределенных систем.
4.Базовая модель информационной системы.
5.Основные модели распределенных систем.
6.Понятие интранета. Структура интранета. Эталонная модель интранета. Этапы создания интранета. Виды интранета. Стандарты создания интранета.
7.Интранет как часть среды распределенных систем.
8.Интранет и экстранет.
9.Портал и интранет.
10.Угрозы ресурсам интранета и причины их реализации.
11.Уязвимость архитектуры клиент-сервер.
12.Слабости системных утилит, команд и сетевых сервисов.
13.Сетевые вирусы.
14.Удаленные атаки на распределенные системы.
15.Типичные сценарии и уровни атак.
16.Классические и современные методы, используемые нападающими для проникновения в открытые системы.
17.Четырехуровневая модель открытой системы.
18.Специфика защиты ресурсов распределенных систем на примере интранета.
19.Выбор сетевой топологии интранета при подключении к другим внешним сетям.
20.Принципы создания защищенных средств связи объектов в распределенных системах.
21.Сервисы безопасности.
22.Средства обеспечения информационной безопасности в распределенных системах.
23.Управление безопасностью распределенных систем.
24.Организационно-правовые методы защиты распределенных систем.

25.Аутентификация субъектов и объектов взаимодействия в распределенных системах.
26.Виртуальные вычислительные сети.
27.Системы анализа защищенности.
28.Системы обнаружения и предотвращения вторжений.

7.2. Оценивание результатов экзамена

Экзаменационный билет для проведения промежуточной аттестации включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Общими критериями, определяющими оценку знаний, умений и навыков на экзамене, являются:

для оценки «отлично» - наличие глубоких и исчерпывающих знаний в объёме пройденного программного материала правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, знание дополнительно рекомендованной литературы;

для оценки «хорошо» - наличие твердых и достаточно полных знаний программного материала, незначительные ошибки при освещении заданных вопросов, правильны действия по применению знаний на практике, четкое изложение материала;

для оценки «удовлетворительно» - наличие твердых знаний пройденного материала, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость наводящих вопросов, правильные действия по применению знаний на практике;

для оценки «неудовлетворительно» - 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.	Карпов А.С. Теоретические основы и практические подходы построения распределенных вычислительных систем [Электронный ресурс] : учебно-методическое пособие / А.С. Карпов. — Электрон. текстовые данные. — М. : Российский государственный университет инновационных технологий и предпринимательства, 2012. — 48 c. — 978-5-98427-047-2. — Режим доступа: http://www.iprbookshop.ru/33843.html
2.	Горев А.И. Обработка и защита информации в компьютерных системах [Электронный ресурс] : учебно-практическое пособие / А.И. Горев, А.А. Симаков. — Электрон. текстовые данные. — Омск: Омская академия МВД России, 2016. — 88 c. — 978-5-88651-642-5. — Режим доступа: http://www.iprbookshop.ru/72856.html
3.	Метелица Н.Т. Вычислительные сети и защита информации [Электронный ресурс] : учебное пособие / Н.Т. Метелица. — Электрон. текстовые данные. — Краснодар: Южный институт менеджмента, 2013. — 48 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/25962.html

8.2. Рекомендуемая дополнительная литература

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

№ п/п	Наименование
1.	Разработка системы технической защиты информации [Электронный ресурс] : учебное пособие / В.И. Аверченков [и др.]. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 187 c. — 5-89838-358-1. — Режим доступа: http://www.iprbookshop.ru/7005.html

2.	Помешкин А.А. Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса «SECRET NET 5.0» [Электронный ресурс] : учебно-методическое пособие / А.А. Помешкин, И.В. Коротких. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2012. — 47 с. — 978-5-7782-1990-8. — Режим доступа: http://www.iprbookshop.ru/45015.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
1.	MS Windows/ CentOS	лицензия университета/ свободное лицензионное соглашение (https://www.centos.org/download/)
2.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
3.	Средства дублирования и восстановления данных	Clonezilla https://clonezilla.org/downloads.php, rsync https://rsync.samba.org/
4.	Средства мониторинга состояния автоматизированных систем	Zabbix https://www.zabbix.com/download

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.	Xgu.ru.	http://xgu.ru/wiki/
2.	Российская Государственная Библиотека	http://www.rsl.ru
3.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
4.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
5.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
6.	Научная электронная библиотека	http://elibrary.ru
7.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
8.	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 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», телекоммуникационным оборудованием (коммутаторы, Wifi-роутеры); программно-аппаратными комплексами защиты информации (АПКШ «Континент» Платформа IPC-25).

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 и 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 и практических занятиях: групповая. При групповой форме организации занятий одна и та же работа выполняется бригадами по 2 - 5 человек.

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.