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
«ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

Специальность10.05.03 -Информационная безопасность автоматизированных систем

Квалификация 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 01.12.2016 г. №1509

СОСТАВИТЕЛЬ:
кандидат физ.-мат. наук, доцент Д.В. Ильин

ОБСУЖДЕНО:
на заседании кафедры МиАОИС факультета ИВТ 30 августа 2017 г., 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

Цель дисциплины: Дисциплина “Теоретические основы компьютерной безопасности” имеет целью обучить студентов методическим вопросам оценки эффективности сложных систем, принципам хранения, обработки и передачи информации в автоматизированных системах (АС), показать им, что концепция баз данных стала определяющим фактором при создании эффективных систем автоматизированной обработки информации. Особое внимание необходимо обратить на вопросы безопасного функционирования автоматизированной системы.

Задачи дисциплины: дать основы

- построения и эксплуатации систем контроля доступа
- системного подхода к проблеме защиты информации в автоматизированных системах (АС);
- механизмов защиты информации и возможностей по их преодолению;

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

Дисциплина «Теоретические основы компьютерной безопасности» относится к вариативной части и является обязательной дисциплиной.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин «Языки программирования», «Основы информационной безопасности», «Дискретная математика».

Дисциплина «Теоретические основы компьютерной безопасности» является предшествующей для производственной и преддипломной практики и 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 проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

способность разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

способность участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21).

знать:

З1: смысл и методы абстрагирования данных;

З2: области применения и этапы проектирования автоматизированных систем;

З3: критерии защищенности АС;

З4: нормативные документы, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем

уметь:

У1: отображать предметную область на конкретную модель данных;

У2: пользоваться средствами защиты, предоставляемыми конкретными АС;

У3: предлагать и обосновывать выбор решений по обеспечению эффективного

применения автоматизированных систем в профессиональной деятельности;

У4: разрабатывать предложения по совершенствованию системы управления информационной безопасностью

владеть навыками:

Н1: работы со средствами поддержания интерфейса с различными категориями пользователей АС;

Н2: разработчика и администратора АС;

Н3: разрабатывать научно-техническую документацию, готовить научно-технические отчеты по результатам выполненных работ по обеспечению эффективного применения автоматизированных систем;

Н4: проектирования средств защиты информации автоматизированной системы.

4. Структура и содержание учебной 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, лабораторные работы), 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 основы построения и эксплуатации АС. Угрозы безопасности АС	ПК-6; ПК-7; ПК-11; ПК-13; ПК-19; ПК-21	З1-З4, У1-У4, Н1-Н4
Рассматривается история и роль автоматизированных систем, модели данных, критерии оценки защищенности, международные стандарты. Рассматриваются угрозы безопасности АС и их оценка		
Раздел 2. Архитектура и проектирование защищенных систем. Реализация механизмов безопасности АС.		
Рассматриваются принципы построения защищенных автоматизированных систем, понятие качества и эффективности таких систем, задачи и этапы проектирования систем. Рассматриваются методы реализации моделей безопасности.		
Раздел 3. Распределенные защищенные АС.		
Рассматриваются принципы построения распределенных защищенных автоматизированных систем и механизмы защиты.		
Экзамен	ПК-6; ПК-7; ПК-11; ПК-13; ПК-19; ПК-21	З1-З4, У1-У4, Н1-Н4

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

Аудиторные занятия	Всего час.	Контактная работа, час.				СРС, час.	ИФР, час	К, час.
		Л	П/р	Л/р	КСР			
Раздел 1. Теоретические основы построения и эксплуатации АС. Угрозы безопасности АС.								
Тема 1. История развития, назначение и роль АС	3	1	1	1			1	

Тема 2. Модели данных, систем и процессов защиты информации.	13	1	1	1		10	1	
Тема 3. Критерии оценки защищенности АС.	3	1	1	1			1	
Тема 4. Определение и содержания понятия угрозы безопасности АС.	13	1	1	1		10	1	
Тема 5. Оценка угроз безопасности АС.	3	1	1	1			1	
Тема 6. Методы и модели анализа угроз.	3	1	1	1			1	
Раздел 2. Архитектура и проектирование защищенных систем. Реализация механизмов безопасности АС.								
Тема 7. Принципы построения защищенных АС	3	1	1	1			1	
Тема 8. Понятие сложной системы.	3	1	1	1			1	
Тема 9. Понятие качества и эффективности.	3	1	1	1			1	
Тема 10. Функциональная и обеспечивающая часть сложной системы	3	1	1	1			1	
Тема 11. Задачи и этапы проектирования АС.	13	1	1	1		10	1	
Тема 12. Автоматизированное проектирование.	3	1	1	1			1	
Тема 13.Практические методы реализации моделей безопасности.	3	1	1	1			1	
Тема 14. Реализация систем контроля доступа	27	1	1	1		24	1	
Раздел 3. Распределенные защищенные АС.								
Тема 15. Принципы построения распределенных защищенных АС.	3	1	1	1			1	
Тема 16. Механизмы защиты в распределенных АС.	7	1	1	1		4	1	
Экзамен	**38**				**2**			**36**
Итого	**144 4 з.е.**	**16**	**16**	**16**	**2**	**58**	**16**	**36**

5. Содержание разделов дисциплины

5.1. Лекции.

Раздел 1. Теоретические основы построения и эксплуатации АС. Угрозы безопасности АС.

1. История развития, назначение и роль АС.

Этапы развития информационных систем. Классификация задач, решаемых с использованием АС. Модели данных, систем и процессов защиты информации. Отображение предметной области. Сущности и связи. Методы абстрагирования данных. Области применения моделей данных.

2. Критерии оценки защищенности АС.

Оценка защищенности на основе отечественных стандартов. Международные стандарты оценки защищенности. Определение и содержания понятия угрозы безопасности АС. Классификация угроз безопасности АС. Реальные и мнимые угрозы.

3. Оценка угроз безопасности АС.Цели и задачи оценки угроз безопасности АС. Методы и модели анализа угроз.

Раздел 2. Архитектура и проектирование защищенных систем. Реализация механизмов безопасности АС.

4. Принципы построения защищенных АС.Элементы и подсистемы, управление и информация, самоорганизация в АС. Понятие сложной системы.
Основные принципы системного подхода при создании сложных систем.

5. Понятие качества и эффективности.Характеристики качества, показатели и критерии эффективности, методические вопросы оценки эффективности сложных систем.Функциональная и обеспечивающая часть сложной системы; Технология функционирования сложной системы;

6. Задачи и этапы проектирования АС. Цели проектирования. Этапы проектирования АС. Методологии проектирования. Организация работ, функции заказчиков и разработчиков. Жизненный цикл автоматизированной системы. Структуризация предметной области. Классификация объектов проектирования. Автоматизированное проектирование. Средства автоматизации проектирования АС: общая характеристика, назначение и возможности, классификация.

7. Практические методы реализации моделей безопасности. Реализация ядра безопасности. Мониторинг взаимодействий в системе. Реализация систем контроля доступа. Способы представления информации о правах доступа.

Раздел 3. Распределенные защищенные АС.

8. Принципы построения распределенных защищенных АС.Основные положения концепции построения и использования распределенных АС. Механизмы защиты в распределенных АС. Архитектура механизмов защиты АС. Применяемые в распределенных АС методы защиты.

5.2 Лабораторные работы

1. Применение международных стандартов оценки защищенности АС.
2. Модели данных.
3. Методы абстрагирования данных.
4. Методы и модели анализа угроз.
5. Реализация систем контроля доступа.
6. Реализация ядра безопасности.
7. Применение программных средств для диаграмм IDEF.
8. Создание системы учета кадров с расширенной парольной защитой

5.3. Вопросы для самостоятельной работы студента в соответствии с содержанием разделов дисциплины

Тема	Вопрос	Часы
Модели данных, систем и процессов защиты информации.	Рассмотрение моделей данных, их отличия, применение на практике.	10
Определение и содержания понятия угрозы безопасности АС..	Классификация угроз безопасности	10
Задачи и этапы проектирования АС.	Разработка моделей IDEF с помощью BPWIN	10
Реализация систем контроля доступа	База данных с распределением прав доступа	24

6. Образовательные технологии

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

– диагностики;

– целеполагания;
– управления процессом освоения учебной информации;
– применения знаний на практике, поиска новой учебной информации;
– организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской, частично-поисковой, репродуктивной, творческой и пр.);
– контроля качества и оценивания результатов образовательной деятельности (технология оценивания качества знаний, рейтинговая технология оценки знаний и др.)

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 (SMARTдоски, 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: анализ литературы по теме, подготовка к лабораторным работам, подготовка реферативных сообщений, разработка проекта и др.

Формами контроля самостоятельной работы выступают оценивание проверка отчётов по результатам выполненных заданий и лабораторных работ. Результаты самостоятельной работы учитываются при оценке знаний наэкзамене.

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 зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся:

7.1. Примерный перечень вопросов к экзамену

1. Этапы развития информационных систем.
2. Классификация задач, решаемых с использованием АС.
3. Отображение предметной области.
4. Сущности и связи.

5. Методы абстрагирования данных.
6. Области применения моделей данных.
7. Оценка защищенности на основе отечественных стандартов.
8. Международные стандарты оценки защищенности.
9. Классификация угроз безопасности АС.
10. Реальные и мнимые угрозы.
11. Цели и задачи оценки угроз безопасности АС.
12. Методы и модели анализа угроз.
13. Принципы построения защищенных АС.
14. Элементы и подсистемы, управление и информация, самоорганизация в АС.
15. Основные принципы системного подхода при создании сложных систем.
16. Характеристики качества, показатели и критерии эффективности, методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы;
17. Технология функционирования сложной системы;
18. Цели проектирования. Этапы проектирования АС.
19. Методологии проектирования.
20. Жизненный цикл автоматизированной системы.
21. Структуризация предметной области. Классификация объектов проектирования.
22. Средства автоматизации проектирования АС: общая характеристика, назначение и возможности, классификация.
23. Практические методы реализации моделей безопасности.
24. Реализация ядра безопасности. Мониторинг взаимодействий в системе.
25. Технологический цикл реализации защищенной системы обработки и хранения информации.
26. Условия, способствующие повышению эффективности защиты информации в АС.
27. Способы представления информации о правах доступа.
28. Основные положения концепции построения и использования распределенных АС.
29. Архитектура механизмов защиты АС. Применяемые в распределенных АС методы защиты.

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 учебной 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 перечня и условия доступа представлены в Приложениях к рабочей программе)

№	Название
1.	Карпов В.В. Технология построения защищенных автоматизированных систем [Электронный ресурс] : учебное пособие / В.В. Карпов, В.А. Мельник. — Электрон. текстовые данные. — М. : Российский новый университет, 2009. — 232 c. Режим доступа: http://www.iprbookshop.ru/21326.html
2.	Методологические основы построения защищенных автоматизированных систем [Электронный ресурс] : учебное пособие / А.В. Душкин [и др.]. — Электрон. текстовые данные. — Воронеж: Воронежский государственный университет инженерных технологий, 2013. — 260 c. Режим доступа: http://www.iprbookshop.ru/47427.html
3.	Волкова Т.В. Основы проектирования компонентов автоматизированных систем [Электронный ресурс] : учебное пособие / Т.В. Волкова. — Электрон. текстовые данные. — Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2016. — 226 c. "Режим доступа: http://www.iprbookshop.ru/69921.html

8.2. Рекомендуемая дополнительная литература.

(ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе)

№	Название
1.	Торокин, А. А. Инженерно-техническая защита информации : [учебное пособие для вузов по специальостям в области информационной безопасности] / А. А. Торокин. - Москва : Гелиос АРВ, 2005. - 959с.
2.	Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : лабораторный практикум / М.А. Лапина [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 242 c.Режим доступа: http://www.iprbookshop.ru/62945.html

Нормативные правовые и методические документы в области защиты информации доступны по ссылке https://fstec.ru/component/tags/tag/informatsionnoe-soobshchenie

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 Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
2.	MS Windows/Linux (Ubuntu)	лицензия университета/ свободное лицензионное соглашение (http://ubuntu.ru/)
3.	SPID_AlgorithmPoC-0-4-6	https://sourceforge.net/projects/spid/files/
4.	Snort2_9_11_1	https://www.snort.org/
5.	Wireshark 2.6.3	https://www.wireshark.org/
6.	Zabbix	https://www.zabbix.com/download
7.	Clonezilla	https://clonezilla.org/downloads.php
8.	rsync	https://rsync.samba.org/
9.	AVG AntiVirus Free	https://www.avg.com/ru-ru/homepage#pc
10.	Avast Free Antivirus	http://avast-anti-virus.ru/?yclid=5762528100398929218
11.	Kaspersky Free	https://www.kaspersky.ru/free-antivirus

12.	360 Total Security	https://www.360totalsecurity.com/ru/

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 +	
3.	База данных угроз безопасности информации	https://bdu.fstec.ru/

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	Российская Государственная Библиотека	http://www.rsl.ru
2.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
3.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
4.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
5.	Научная электронная библиотека	http://elibrary.ru
6.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
7.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru
8.	ISO 27000 Международные стандарты управления информационной безопасностью.	http://iso27000.ru
9.	Информационная безопасность. Практика информационной безопасности.	http://dorlov.blogspot.com
10.	SecurityLab. Информационный портал по безопасности.	http://www.securitylab.ru

9. Материально-техническое обеспечение учебной 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
– настенный экран;
– интерактивная доска SMART;

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».

Учебная аудитория для лабораторных занятий в области защищенных автоматизированных систем, оснащена аппаратно-программными средствами управления доступом к данным, шифрования, средствами дублирования и восстановления данных, средствами мониторинга состояния автоматизированных систем, источниками бесперебойного и аварийного питания, средствами контроля и управления доступом в помещения, охранной и пожарной сигнализацией, климатическим контролем.

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. 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.

Формы организации студентов на лабораторных работах и практических занятиях: фронтальная и индивидуальная. При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу. При индивидуальной форме организации занятий каждый студент выполняет индивидуальное задание.

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.