МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

"Чувашский государственный аграрный университет"

(ФГБОУ ВО Чувашский ГАУ)

Кафедра Математики, физики и информационных технологий

УТВЕРЖДАЮ
Проректор по учебной
и научной работе

Л.М. Иванова

17.04.2025 г.

Б1.О.20

Информационная безопасность

рабочая программа дисциплины (модуля)

Направление подготовки 09.03.03 Прикладная информатика
Направленность (профиль) Прикладная информатика в агропромышленном комплексе

Квалификация	**Бакалавр**
Форма обучения	**заочная**
Общая трудоемкость	**4 ЗЕТ**

Часов по учебному плану	144
в том числе:	
аудиторные занятия	14
самостоятельная работа	121
часов на контроль	9

Виды контроля:
экзамен

Распределение часов дисциплины по курсам

Курс	4		Итого	
Вид занятий	УП	РП		
Лекции	6	6	6	6
Лабораторные	8	8	8	8
В том числе инт.	4	4	4	4
В том числе в форме практ.подготовки	4	4	4	4
Итого ауд.	14	14	14	14
Контактная работа	14	14	14	14
Сам. работа	121	121	121	121
Часы на контроль	9	9	9	9
Итого	144	144	144	144

Программу составил(и):
канд. техн. наук, доц., Кручинкина И.С.

При разработке рабочей программы дисциплины (модуля) "Информационная безопасность" в основу положены:

1. Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922).

2. Учебный план: Направление подготовки 09.03.03 Прикладная информатика
Направленность (профиль) Прикладная информатика в агропромышленном комплексе, одобренный Ученым советом ФГБОУ ВО Чувашский ГАУ от 17.04.2025 г., протокол № 14.

Рабочая программа дисциплины (модуля) проходит согласование с использованием инструментов электронной информационно-образовательной среды Университета.

СОГЛАСОВАНО:

Заведующий кафедрой Максимов А.Н.

Заведующий выпускающей кафедрой Максимов А.Н.

Председатель методической комиссии факультета Гаврилов В.Н.

Директор научно-технической библиотеки Викторова В.А.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	ознакомление студентов с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации при проектировании информационных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ОПОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Проектирование информационных систем
2.1.2	Учебная практика, научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)
2.1.3	Вычислительные системы, сети и телекоммуникации
2.1.4	Информационные системы и технологии
2.1.5	Правовые информационно-консультационные системы
2.1.6	Разработка программных приложений
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная практика, технологическая (проектно-технологическая) практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
ОПК-3.1 Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности
ОПК-3.2 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности
ОПК-3.3 Демонстрирует навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;
ОПК-4.1 Обосновывает применение основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы
ОПК-4.2 Определяет комплектность технической документации на различных стадиях жизненного цикла информационной системы
ОПК-4.3 Составляет техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы
ПК-1. Способен устанавливать и настраивать системное и прикладное программное обеспечение, необходимое для функционирования ИС
ПК-1.1 Владеет навыками установки и настройки операционных систем, СУБД и прикладных ПО
ПК-1.2 Демонстрирует навыки применения современного коммуникационного оборудования и сетевых протоколов
ПК-1.3 Использует современный отечественный и зарубежный опыт в профессиональной деятельности

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	студент помнит, понимает и может продемонстрировать широкий спектр фактических, концептуальных, процедурных знаний.
3.2	**Уметь:**
3.2.1	использовать изученный материал в конкретных условиях и в новых ситуациях; осуществлять декомпозицию объекта на отдельные элементы и описывать то, как они соотносятся с целым, выявлять структуру объекта изучения; оценивать значение того или иного материала - научно-технической информации, исследовательских данных и т. д.; комбинировать элементы так, чтобы получить целое, обладающее новизной.
3.3	**Иметь навыки и (или) опыт деятельности:**

3.3.1	по применению теоретических и практических знаний и умений при решении ситуационных задач, практической направленности по дисциплине.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Прак. подг.	Примечание
Раздел 1. Составляющие, уровни обеспечения и угрозы ИБ							
Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей. Идентификация и аутентификация /Лек/	4	1	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	1	0	Проблемная лекция
Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей. Идентификация и аутентификация /Лаб/	4	1	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Устный опрос, решение задач.
Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей. Идентификация и аутентификация /Ср/	4	20	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Устный опрос, решение задач
Криптография и шифрование. Методы разграничения доступа. Регистрация и аудит. Межсетевое экранирование /Лек/	4	1	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	1	0	Проблемная лекция
Криптография и шифрование. Методы разграничения доступа. Регистрация и аудит. Межсетевое экранирование /Лаб/	4	1	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Устный опрос, решение задач
Криптография и шифрование. Методы разграничения доступа. Регистрация и аудит. Межсетевое экранирование /Ср/	4	20	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Устный опрос, решение задач
Раздел 2. Вирусы и удаленные угрозы в сетях							

Введение в ИБ и составляющие ИБ. Формирование режима ИБ /Лек/	4	1	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Устный опрос, решение задач
Введение в ИБ и составляющие ИБ. Формирование режима ИБ /Лаб/	4	1	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	1	0	Учебная дискуссия
Введение в ИБ и составляющие ИБ. Формирование режима ИБ /Ср/	4	20	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Устный опрос, решение задач
Нормативно правовые основы ИБ в РФ. Стандарты ИБ. Административный уровень обеспечения информационной безопасности. Классификация угроз ИБ /Лек/	4	1	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Устный опрос, решение задач
Нормативно правовые основы ИБ в РФ. Стандарты ИБ. Административный уровень обеспечения информационной безопасности. Классификация угроз ИБ /Лаб/	4	1	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	1	0	Учебная дискуссия
Нормативно правовые основы ИБ в РФ. Стандарты ИБ. Административный уровень обеспечения информационной безопасности. Классификация угроз ИБ /Ср/	4	21	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Устный опрос, решение задач
Раздел 3. Принципы и методы защиты в вычислительных сетях							
Вирусы как угроза ИБ. Классификация компьютерных вирусов. Характеристика «вирусоподобных» программ. Антивирусные программные средства. Обнаружение и профилактика вирусных атак /Лек/	4	1	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Устный опрос, решение задач

Вирусы как угроза ИБ. Классификация компьютерных вирусов. Характеристика «вирусоподобных» программ. Антивирусные программные средства. Обнаружение и профилактика вирусных атак /Лаб/	4	2	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	2	Устный опрос, решение задач, участие в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью
Вирусы как угроза ИБ. Классификация компьютерных вирусов. Характеристика «вирусоподобных» программ. Антивирусные программные средства. Обнаружение и профилактика вирусных атак /Ср/	4	20	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Устный опрос, решение задач
Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях /Лек/	4	1	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Устный опрос, решение задач
Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях /Лаб/	4	2	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	2	Устный опрос, решение задач, участие в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью
Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях /Ср/	4	20	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Устный опрос, решение задач
Раздел 4. Экзамен							
Составляющие, уровни обеспечения и угрозы ИБ. Вирусы и удаленные угрозы в сетях. Принципы и методы защиты в вычислительных сетях /Экзамен/	4	9	ПК-1.1 ПК-1.2 ПК-1.3 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1Л2.1	0	0	Экзамен

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Примерный перечень вопросов к зачету

Не предусмотрено учебным планом.

5.2. Примерный перечень вопросов к экзамену

1. Понятие информационной безопасности. Вопросы информационной безопасности в системе обеспечения национальной безопасности.

2. Основные составляющие и аспекты информационной безопасности.
3. Классификация угроз информационной безопасности: для личности, для общества, для государства.
4. Понятие информационной войны. Особенности информационной войны. Понятие информационного превосходства.
5. Концепция «информационной войны» по оценкам российских спецслужб.
6. Понятие информационного оружия. Что отличает информационное оружие от обычных средств поражения?
7. Сфера применения информационного оружия.
8. Особенности информационного оружия. Организация защиты.
9. Основные задачи в сфере обеспечения информационной безопасности.
10. Отечественные стандарты в области информационной безопасности
11. Зарубежные стандарты в области информационной безопасности
12. Понятие защиты информации. Какая система считается безопасной? Какая система считается надёжной?
13. Основные критерии оценки надежности: политика безопасности и гарантированность.
14. Понятие государственной тайны. Понятие профессиональной тайны.
15. Понятие коммерческой тайны. Понятие служебной тайны. Понятие банковской тайны.
16. Основные конституционные гарантии по охране и защите прав и свобод в информационной сфере.
17. Понятие надежности информации в автоматизированных системах обработки данных. Что понимается под системной защитой информации.
18. Уязвимость информации в автоматизированных системах обработки данных.
19. Элементы и объекты защиты в автоматизированных системах обработки данных.
20. Методы защиты информации от преднамеренного доступа.
21. Защита информации от исследования и копирования.
22. Опознавание с использованием простого пароля. Метод обратимого шифрования.
23. Использование динамически изменяющегося пароля. Методы модификации схемы простых паролей.
24. Использование динамически изменяющегося пароля. Метод «запрос-ответ».
25. Использование динамически изменяющегося пароля. Функциональные методы
26. Криптографические методы защиты информации в автоматизированных системах. Основные направления использования криптографических методов. Симметричные криптосистемы. Системы с открытым ключом.
27. Электронная (цифровая) подпись. Цели применения электронной подписи.
28. Понятие криптостойкости шифра. Требования к криптографическим системам защиты информации.
29. Классификация методов криптографического закрытия.
30. Особенности защиты информации в персональных ЭВМ. Основные цели защиты информации.
31. Угрозы информации в персональных ЭВМ.
32. Обеспечение целостности информации в ПК. Физическая зашита ПК и носителей информации.
33. Защита ПК от несанкционированного доступа.
34. Способы опознавания (аутентификации) пользователей и используемых компонентов обработки информации. Дать краткую характеристику.
35. Классификация закладок. Причины защиты ПК от закладок. Аппаратные закладки.
36. Программные закладки. Классификация критериев вредоносного воздействия закладок.
37. Общие характеристики закладок.
38. Методы и средства защиты от закладок.
39. Компьютерный вирус. Какая программа считается зараженной.
40. По каким признакам классифицируются вирусы?
41. Способы заражения программ. Стандартные методы заражения.
42. Как работает вирус?
43. Методы защиты от вирусов.
44. Антивирусные программы. Программы-детекторы. Программы- доктора.
45. Антивирусы-полифаги. Эвристические анализаторы.
46. Программы-ревизоры. Программы-фильтры.
47. Цели, функции и задачи защиты информации в сетях ЭВМ. Угрозы безопасности для сетей передачи данных.
48. В чём заключаются задачи защиты в сетях передачи данных?
49. Проблемы защиты информации в вычислительных сетях.
50. Понятие сервисов безопасности: идентификация / аутентификация, разграничение доступа.
51. Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление.
52. Архитектура механизмов защиты информации в сетях ЭВМ.

5.3. Тематика курсовых работ (курсовых проектов)

Не предусмотрено учебным планом.

5.4. Фонд оценочных средств для проведения текущего контроля

Темы рефератов (примерные)

1. Основные составляющие информационной безопасности.
2. Уровни режима информационной безопасности.
3. Административный уровень обеспечения информационной безопасности.
4. Классификация угроз ИБ.
5. Вирусы как угроза ИБ. Классификация компьютерных вирусов.
6. Характеристика «вирусоподобных» программ.
7. Антивирусные программные средства.

8. Обнаружение и профилактика вирусных атак.
9. Особенности обеспечения информационной безопасности в компьютерных сетях.
10. Сетевые модели передачи данных и безопасность.
11. Модель взаимодействия открытых систем OSI/ISO и проблемы ИБ.
12. Адресация в глобальных сетях и проблемы ИБ.
13. Классификация удаленных угроз в вычислительных сетях.
14. Типовые удаленные атаки и их характеристика.
15. Примеры и причины успешной реализации удаленных угроз в вычислительных сетях.
16. Принципы защиты распределенных вычислительных сетей.
17. Идентификация и аутентификация.
18. Криптография и шифрование. Методы разграничения доступа.
19. Регистрация и аудит. Межсетевое экранирование.
20. Технология виртуальных частных сетей VPN.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: НГТУ, 2019	Электронный ресурс

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Баланов А. Н.	Комплексная информационная безопасность: учебное пособие	Санкт-Петербург: Лань, 2024	Электронный ресурс

6.3.1 Перечень программного обеспечения

6.3.1.1	ОС Windows XP
6.3.1.2	MapInfo
6.3.1.3	Access 2016
6.3.1.4	GIMP
6.3.1.5	MozillaFirefox
6.3.1.6	MozillaThinderbird
6.3.1.7	7-Zip
6.3.1.8	ОС Windows 7
6.3.1.9	ОС Windows 8
6.3.1.10	SuperNovaReaderMagnifier

6.3.2 Перечень информационных справочных систем

6.3.2.1	Электронный периодический справочник «Система ГАРАНТ». Полнотекстовый, обновляемый. Доступ по локальной сети академии
6.3.2.2	Электронная библиотечная система издательства «Лань». Полнотекстовая электронная библиотека. Индивидуальный неограниченный доступ через фиксированный внешний IP адрес академии неограниченному количеству пользователей из любой точки, в которой имеется доступ к сети Интернет.http://e.lanbook.com

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Вид работ	Назначение	Оснащенность
1-308		Учебная аудитория	Демонстрационное оборудование (экран Lumien Eco Picture LEP-100102 180*180 см (1 шт.), проектор Acer X127H DLP3600Lm (1204*768) (1 шт.), ноутбук Lenovo (1 шт.) и учебно-наглядные пособия, доска ученическая настенная трехэлементная (1 шт.), осветитель доски (1 шт.), скамейка 4-х местная на металлокаркасе (17 шт.), стол ученический 4-х местный (17 шт.), кафедра лектора настольная (1 шт.), стол преподавательский однотумбовый (1 шт.), стул полумягкий (1 шт.)
1-402		Учебная аудитория	Компьютерная техника CPU AMD Athllon II X4620 AM3 (11 шт.), доска ученическая настенная трехэлементная (1 шт.), стул полумягкий (9 шт.), стол компьютерный (11 шт.), стол ученический 2-х местный на металокаркасе (10 шт.), стул ученический на металлокаркасе (15 шт.)

1-204		Помещение для самостоятельной работы	Столы (28 шт.), стулья (48 шт.), шкаф и стеллажи с литературой, компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации(4 шт.).
1-501		Помещение для самостоятельной работы	Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации (персональные компьютеры) (3 шт.). Стол ученический 2-х местный (5 шт.), стул ученический (7 шт.)

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методика изучения курса предусматривает наряду с лекциями и лабораторными занятиями, организацию самостоятельной работы студентов, проведение консультаций, руководство докладами студентов для выступления на научно-практических конференциях, осуществление текущего, промежуточного форм контроля.

Система знаний по дисциплине «Информационная безопасность» формируется в ходе аудиторных и внеаудиторных (самостоятельных) занятий. Используя лекционный материал, учебники и учебные пособия, дополнительную литературу, проявляя творческий подход, студент готовится к лабораторным занятиям, рассматривая их как пополнение, углубление, систематизацию своих теоретических знаний.

Для освоения дисциплины студентами необходимо:

1. посещать лекции, на которых в сжатом и системном виде излагаются основы дисциплины. Студенту важно понять, что лекция есть своеобразная творческая форма самостоятельной работы. Надо пытаться стать активным соучастником лекции: думать, сравнивать известное с вновь получаемыми знаниями, войти в логику изложения материала лектором, следить за ходом его мыслей, за его аргументацией, находить в ней кажущиеся вам слабости. Во время лекции можно задать лектору вопрос, желательно в письменной форме, чтобы не мешать и не нарушать логики проведения лекции. Слушая лекцию, следует зафиксировать основные идеи, положения, обобщения, выводы. Работа над записью лекции завершается дома. На свежую голову (пока еще лекция в памяти) надо уточнить то, что записано, обогатить запись тем, что не удалось зафиксировать в ходе лекции, записать в виде вопросов то, что надо прояснить, до конца понять. Важно соотнести материал лекции с темой учебной программы и установить, какие ее вопросы нашли освещение в прослушанной лекции. Тогда полезно обращаться и к учебнику. Лекция и учебник не заменяют, а дополняют друг друга.
2. посещать лабораторные занятия, к которым следует готовиться и активно на них работать. Задание к лабораторному занятию выдает преподаватель. Задание включает в себя основные вопросы, задачи, тесты и рефераты для самостоятельной работы, литературу. Лабораторные занятия начинаются с вступительного слова преподавателя, в котором называются цель, задачи и вопросы занятия. В процессе проведения занятий преподаватель задает основные и дополнительные вопросы, организует их обсуждение. На лабораторных занятиях решаются конкретные задачи. Студенты, пропустившие занятие, или не подготовившиеся к нему, приглашаются на консультацию к преподавателю. Лабораторное занятие заканчивается подведением итогов: выводами по теме и защитой работы.
3. систематически заниматься самостоятельной работой, которая включает в себя изучение курса лекций, учебников, освоение теоретических сведений к выполнению заданий, решение ситуационных задач, написание докладов, рефератов. Задания для самостоятельной работы выдаются преподавателем.

ПРИЛОЖЕНИЯ

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ
в 20___ /20___ учебном году

Актуализированная рабочая программа рассмотрена и одобрена на заседании выпускающей кафедры, протокол № ___ от ______________________

Заведующий выпускающей кафедрой ___________________________________

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ
в 20___ /20___ учебном году

Актуализированная рабочая программа рассмотрена и одобрена на заседании выпускающей кафедры, протокол № ___ от ______________________

Заведующий выпускающей кафедрой ___________________________________

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ
в 20___ /20___ учебном году

Актуализированная рабочая программа рассмотрена и одобрена на заседании выпускающей кафедры, протокол № ___ от ______________________

Заведующий выпускающей кафедрой ___________________________________

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ
в 20___ /20___ учебном году

Актуализированная рабочая программа рассмотрена и одобрена на заседании выпускающей кафедры, протокол № ___ от ______________________

Заведующий выпускающей кафедрой ___________________________________

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ
в 20___ /20___ учебном году

Актуализированная рабочая программа рассмотрена и одобрена на заседании выпускающей кафедры, протокол № ___ от ______________________

Заведующий выпускающей кафедрой ___________________________________

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ
в 20___ /20___ учебном году

Актуализированная рабочая программа рассмотрена и одобрена на заседании выпускающей кафедры, протокол № ___ от ______________________

Заведующий выпускающей кафедрой ___________________________________