МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Чувашский государственный университет имени И.Н. Ульянова»
(ФГБОУ ВО «ЧГУ им. И.Н.Ульянова»)

Факультет информатики и вычислительной техники
Кафедра математического и аппаратного обеспечения информационных систем

Утверждена в составе образовательной программы высшего образования

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Научная специальность – 2.3.6. Методы и системы защиты информации, информационная безопасность
Форма обучения – очная
Год начала освоения – 2022

Чебоксары – 2024

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

Заведующий кафедрой математического
и аппаратного обеспечения
информационных систем, к.ф.-м.н., доцент
Т.Н. Копышева

ОБСУЖДЕНО:
На заседании кафедры математического и
аппаратного обеспечения информационных систем
05 ноября 2024 г., протокол № 4
Заведующий кафедрой
Т.Н. Копышева

СОГЛАСОВАНО:
Декан факультета А.В. Щипцова

Начальник отдела подготовки и
повышения квалификации
научно-педагогических кадров С.Б. Харитонова

1. Цель и задачи освоения дисциплины (модуля).

Целью изучения дисциплины является формирование у обучающихся фундаментальных знаний и навыков, позволяющих им использовать различные средства защиты информации для детектирования, защиты и противодействия угрозам, расследования и восстановления последствий инцидентов, а также для анализа защищенности.

Задачами дисциплины являются:

- изучение средств защиты информации и методов их применения,
- понимание принципов, лежащих в основе работы средств защиты информации для их эффективного применения,
- способность разрабатывать на основе современных средств защиты информации систему защиты информации.

2. Планируемые результаты освоения дисциплины (модуля).

В процессе освоения данной дисциплины, обучающиеся формируют следующие результаты освоения дисциплины:

К7 – способность к разработке научных основ, принципиально новых методов анализа и синтеза, научных подходов и технических принципов создания систем защиты информации и информационной безопасности (далее – ИБ);

К8 – способность самостоятельно исследовать свойства и создавать алгоритмы для методов и систем защиты информации;

К9 – способность использовать в профессиональной деятельности современные языки программирования, базы данных, операционные системы, электронные библиотеки и пакеты математических и специализированных программ, сетевые технологии, а также умение применять новые поколения программного и аппаратного обеспечения в области математического моделирования процессов защиты информации.

3. Структураисодержаниедисциплины (модуля).

3.1. Структурадисциплины (модуля).

№ п/п	Наименование раздела дисциплины (модуля)	Формируемые компетенции	Форма текущего контроля
1	Раздел 1. Принципы комплексного обеспечения ИБ. Архитектура защищенной сети. Контроль доступа.	К7, К8, К9	Задания на практических занятиях
2	Раздел 2. Управление угрозами ИБ. Управление инцидентами	К7, К8, К9	Индивидуальные творческие задания

3.2. Объем дисциплины (модуля) и виды учебной работы.

№ п/п	Темы занятий	Лекции	Практические занятия	Самостоятельная работа	Всего часов
	Семестр 3				
	Раздел 1. Принципы комплексного обеспечения ИБ. Архитектура защищенной сети. Криптография				
1.	Тема 1. Принципы комплексного обеспечения ИБ	2	0	10	12
2.	Тема 2. Архитектура защищенной сети	6	6	15	27
3.	Тема 3. Контроль доступа	8	10	15	33
	Итого за 3 сем., час	**16**	**16**	**40**	**72**
	Семестр 4				
	Раздел 2. Управление угрозами ИБ. Управление инцидентами ИБ				
4.	Тема 4. Управление угрозами ИБ	8	10	38	56
5.	Тема 5. Управление инцидентами	8	6	38	52
	Итого за 4 сем., час	**16**	**16**	**76**	**108**
	Итого, час	**32**	**32**	**116**	**180**
	Итого, з.е.				**5**

Видпромежуточнойаттестации:
зачет – семестр 3;
кандидатский экзамен – семестр 4.

3.3. Темызанятийикраткоесодержание.

Раздел 1. Принципы комплексного обеспечения ИБ. Архитектура защищенной сети. Контроль доступа

Тема 1. Принципы комплексного обеспечения ИБ

Лекция 1. Принципы комплексного обеспечения ИБ
- эшелонированная защита
- многоуровневая защита
- управление рисками
- контроль доступа
- hardening
- доверенныесистемы
- фреймворки безопасности: Common Criteria, ISO 27000, NIST CSF, CIS Top 20, Cyber Essentials

Тема 2. Архитектура защищенной сети

Лекция 2. Анализ сетевого траффика
- Принцип работы снифферов
- Программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других Wireshark

- Утилита UNIX, позволяющая перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программаTcpdump

Практическое занятие 1. Анализ сетевого трафика.

Лекция 3. Блокирование нежелательного трафика
- Сетевые экраны
- Брандмауэр Windows
- Гибкая утилита межсетевого экрана Iptables

Практическое занятие 2. Ограничение сетевого доступа

Лекция 4. Системы обнаружения вторжений
- Принцип работы систем обнаружения вторжений
- Система обнаружения вторжений и система предотвращения вторжений на основе открытого исходного кода. Snort, Suricata
-Платформа сетевого анализа программного обеспечения с открытым исходным кодом Bro/Zeek

Практическое занятие 3. Детектирование подозрительного трафика

Тема 3. Контроль доступа

Лекция 5. Протокол AAA.
- принципы аутентификации
- принципы авторизации
- принципы контроля ресурсов
- модели управления доступом
- Токены и биометрия

Практическое занятие. 4 Проектирование системы контроля доступа

Лекция 6. Парольная защита
- Оценка стойкости пароля
- Хеширование
- Хранение паролей в ОС Windows, Linux

Практическое занятие 5. Способы защиты данных паролем

Лекция 7. Утилиты подбора пароля
- Атака перебором и подбором по словарю
- Свободная программа, предназначенная для восстановления паролей по их хешам Johntheripper
- Программное обеспечение с открытым исходным кодом для перебора паролей в реальном времени от различных онлайн сервисов, веб-приложений, FTP, SSH и других протоколов THC Hydra

Практическое занятие 6.Оценка стойкости паролей

Лекция 8. Средства доверенной загрузки
- Контроль целостности объектов файловой системы
- средства доверенной загрузки уровня базовой системы ввода-вывода
- средства доверенной загрузки уровня платы расширения

- средства доверенной загрузки уровня загрузочной записи
- технология «доверенной загрузки»Intel TXT (Trusted Execution Technology)
- протокол UEFI Secure Boot

Практические занятия 7,8. Установка и настройка доверенной загрузки

Раздел 2. Управление угрозами ИБ. Управление инцидентами ИБ

Тема 4. Управление угрозами ИБ

Лекция 9. Основы управления уязвимостями ПО
- Определения: угроза, уязвимость, инцидент
- База данных общеизвестных уязвимостей информационной безопасностиCVE, система категорий для слабых мест и уязвимостей программного обеспечения CWE, - открытый проект обеспечения безопасности веб-приложенийOWASPTop 10
- открытый стандарт, используемый для расчета количественных оценок уязвимости в безопасности компьютерной системы CVSS, коэффициент возврата инвестиций ROI, коэффициент возврата инвестиций ROSI
- Банк данных угроз безопасности информации ФСТЭК

Лекция 10. Анализ защищенности с применением сканеров безопасности
- видимые адреса (hping3)
- открытые порты (nmap)
- уязвимыесервисы (GVM/ScanOval/linys/Retina)

Практическое занятие 9. Анализ защищенности инфраструктуры

Лекция 11. Укрепление защищенности ОС
- Инфраструктура безопасности Windows
- Контроль доступа
- Групповая политика безопасности
- Управление ролями и службами
- Архитектура безопасности Windows
- Разграничение доступа в Linux
- Утилиты Безопасности
- Управление конфигурацией и службами

Практическое занятие 10. Укрепление безопасности Windows
Практическое занятие 11. Укрепление безопасности Linux

Лекция 12. Защита от вредоносного кода и эксплойтов
- Принцип работы антивирусов
- Правила представляют собой описание сигнатур целевых атак и вторжений в IT-инфраструктуру организации Yararules

Практические занятия 12, 13. Настройка антивирусного комплекса

Тема 5. Управление инцидентами

Лекция 13. Основы работы с инцидентами
- 6-шаговый процесс реагирования на инциденты
- Матрица атак
- Стратегии защиты

- Мониторинг компьютерных сетей, серверов и сетевого оборудования
- стратегия мониторинга журналов
- принцип работы SIEM
- унифицированный формат описания правил детектирования, основанных на данных из логов SigmaRules
- корпоративное решение для мониторинга безопасности с открытым исходным кодом для обнаружения угроз, мониторинга целостности, реагирования на инциденты и соответствия требованиям. Wazuh.

Практическое занятие 14. Анализ следов атаки

Лекция 14. Реагирование и расследование инцидентов
- Принципы компьютерной форензики
- Инверсия управления IOC
- Extended Detection and Response (XDR)
- Мониторинг артефактов Velociraptor

Практическое занятие 15. Расследование и устранение воздействия атаки

Лекция 15. Восстановление данных
- Виды и способы архивирования
- Восстановление и уничтожение объектов файловой системы
- Копирование дисков. Partclone, Partimage, ddrescue

Практическое занятие 16. Восстановление удаленных файлов

Лекция 16. Автоматизация реагирования на инциденты
- Оперативные центры обеспечения кибербезопасности (Security Operations Center, SOC)
- Incident Response Platform
- Сценарии реагирования (плейбуки)

4. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины (модуля).

Формы и виды контроля знаний аспирантов, предусмотренные по данной дисциплине:
текущий контроль;
промежуточная аттестация (зачет, кандидатский экзамен).

Критерии получения зачета по дисциплине (модулю):
- оценка «зачтено» ставится, если обучающийся выполнил не менее половины аудиторных контрольных работ, домашних заданий, докладов, ответил на половину вопросов к зачету;
- оценка «не зачтено» ставится, если обучающийся выполнил менее половины аудиторных контрольных работ, домашних заданий, докладов, не ответил на половину вопросов к зачету.

Критерии экзаменационной оценки:
- 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, правильные 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.

4.1. Примерный перечень вопросов к зачету

1. Чем угроза ИБ отличается от уязвимости ИБ?
2. Дайте определение понятию риска.
3. Приведите примеры наиболее распространенных современных уязвимостей.
4. Чем отличается модель безопасности Белла-Ла Падулы от модели дискреционного доступа (DAC)?
5. Что такое RBAC?
6. Что означает слово «криптология» и кем оно введено?
7. Какие недостатки имеют несимметричные методы шифрования перед симметричными?
8. В чем заключается проблема управления ключами?
9. Где используется стеганография?
10. В каких случаях применяется хеширование?
11. Какие существуют хеш-функции?
12. Опишите принцип работы цифровой подписи документа.
13. Опишите принципы контроля доступа.
14. Опишите принципы цифрового хранения информации.
15. Перечислите критерии оценки доверенных компьютерных систем?
16. Для чего используется БДУ ФСТЭК?
17. Опишите принципы построение системы защитных мер.
18. Опишите процедуру расследования инцидента.
19. Назовите основные угрозы физической безопасности.
20. Назовите программные средства для контроля периметра.
21. Опишите принципы работы антивируса?
22. Какие существуют виды сетевых экранов?

4.2. Примерный перечень вопросов к экзамену

1. Основные понятия информационной безопасности: информация, конфиденциальность, целостность, доступность, защита данных, информационная безопасность, обеспечение информационной безопасности
2. Подходы к обеспечению информационной безопасности и защиты информации.
3. Аппаратно-программные средства защиты информационных систем.
4. Организационные меры защиты информационных систем.
5. Способы выявления, идентификации, классификации угроз нарушения информационной безопасности.
6. Способы защиты от угроз информационной безопасности в открытых компьютерных сетях, включая Интернет.
7. Средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.
8. Формирование комплекса средств противодействия угрозам информационной безопасности.

9. Риски нарушения информационной безопасности. Способы управления рисками.
10. Способы анализа и оценки рисков нарушения информационной безопасности.
11. Модели и методы оценки защищенности информации и информационной безопасности объекта.
12. Модели и методы оценки эффективности средств и мер обеспечения информационной безопасности.
13. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов.
14. Модели и системы разграничения доступа. Политика безопасности по доступу к объектам.
15. Способы выявления и противодействия распространению ложной и вредоносной информации.
16. Политика обеспечения информационной безопасности.
17. Регламенты и правила информационной безопасности.
18. Принцип работы различных средств защиты информации и обеспечения информационной безопасности.
19. Модели, методы и средства обеспечения аудита и мониторинга состояния объекта защиты.
20. Способы реагирования и расследования инцидентов информационной безопасности.
21. Жизненный цикл инцидентов информационной безопасности.
22. Средства мониторинга и управления инцидентами информационной безопасности.
23. Принципы разработки безопасного программного обеспечения.
24. Способы анализа дефектов безопасности (уязвимостей) программного обеспечения.
25. Понятие скрытого канала передачи и способы выявления и противодействия.
26. Выявление уязвимостей в компьютерных системах и сетях.
27. Управление обеспечением информационной безопасности, непрерывного функционирования и восстановления систем, противодействию отказу в обслуживании.
28. Криптографические алгоритмы. Криптографические протоколы.
29. Криптографические методы и средства защиты хранящихся данных.
30. Криптографические методы и средства защиты передаваемых данных по сети.
31. Нормативно-правовое обеспечение информационной безопасности.
32. Способы защиты от вредоносного кода.
33. Способы защиты от методов социальной инженерии и фишинга.

Каждому аспиранту на экзамене дополнительно задаются вопросы по теме диссертации на соискание ученой степени кандидата наук.

5. Учебно-методические материалы, библиотечные фонды и библиотечно-справочные системы, информационные, информационно-справочные системы, профессиональные базы данных.

5.1. Рекомендуемые основные учебно-методические материалы.

№	Название
1.	Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268
2.	Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ;

	под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2023. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511700
3.	Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2023. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512423

5.2. Рекомендуемые дополнительные учебно-методические материалы.

№	Название
1.	Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2023. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511890
2.	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513300
3.	Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515435
4.	Ковцур, М. М. Безопасность беспроводных локальных сетей : учебно-методическое пособие / М. М. Ковцур, Д. В. Юркин, Е. Ю. Герлинг. — Санкт-Петербург :СПбГУТ им. М.А. Бонч-Бруевича, 2021. — 40 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/279476 . — Режим доступа: для авториз. ользователей.
5.	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512861
6.	Рацеев, С. М. Математические методы защиты информации и их основы. Сборник задач / С. М. Рацеев. — Санкт-Петербург : Лань, 2023. — 140 с. — ISBN 978-5-507-45197-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/292913. — Режим доступа: для авториз. пользователей
7.	Сертификация средств защиты информации : учебное пособие / А. А. Миняев, Юркин, М. М. Ковцур, К. А. Ахрамееева. — Санкт-Петербург :СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 88 с. — ISBN 978-5-89160-213-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180100. — Режим доступа: для авториз. пользователей.
8.	Хамадулин, Э. Ф. Методы и средства измерений в телекоммуникационных системах : учебное пособие для вузов / Э. Ф. Хамадулин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 315 с. — (Высшее образование). —

	ISBN 978-5-534-15706-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/509492
9.	Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998

5.3. Библиотечные фонды, библиотечно-справочные системы, информационные, информационно-справочные системы, профессиональные базы данных.

№	Перечень библиотечных фондов, библиотечно-справочных систем, информационных, информационно-справочных систем, профессиональных баз данных
1.	Научная библиотека ЧувГУ [Электронный ресурс]. – Режим доступа: http://library.chuvsu.ru
2.	Электронно-библиотечная система IPRBooks [Электронный ресурс]. – Режим доступа: http://www.iprbookshop.ru
3.	Образовательная платформа «Юрайт»: для вузов и ссузов [Электронный ресурс]. – Режим доступа: https://www.urait.ru
4.	Единое окно к образовательным ресурсам[Электронный ресурс]. – Режим доступа: http://window.edu.ru
5.	Российская государственная библиотека [Электронный ресурс]. – Режим доступа: http://www.rsl.ru
6.	Российская национальная библиотека [Электронный ресурс]. – Режим доступа: http://www.nlr.ru
7.	Научная электронная библиотека «Киберленинка» [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru
8.	Научная электронная библиотека «Elibrary» [Электронный ресурс]. – Режим доступа: www.elibrary.ru
9.	Цифровая библиотека по философии [Электронный ресурс]. – Режим доступа: http://filosof.historic.ru
10.	Институт философии Российской Академии Наук: Электронная библиотека [Электронный ресурс]. – Режим доступа: https://iphras.ru/elib.htm
11.	Философия онлайн [Электронный ресурс]. – Режим доступа: http://phenomen.ru

Профессиональные базы данных, информационные справочные системы, предоставляемые Университетом, доступны для скачивания по ссылке http://ui.chuvsu.ru//. Единый реестр российских программ для электронных вычислительных машин и баз данных, в том числе свободно распространяемых, доступен по ссылке https://reestr.digital.gov.ru/reestr/.

6. Материально-техническоеобеспечениедисциплины (модуля).

Учебные аудитории для лекционных и практических занятий по дисциплине оснащены мультимедийным проектором и настенным экраном.

Учебные аудитории для самостоятельных занятий по дисциплине оснащены компьютерной техникой с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

7. Средства адаптации преподавания дисциплины (модуля) 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.

8. Методические рекомендации обучающимся по выполнению самостоятельной работы.

Самостоятельная работа определяется спецификой дисциплины и методикой ее преподавания, временем, предусмотренным учебным планом, а также ступенью обучения, на которой изучается дисциплина.

Для самостоятельной подготовки можно рекомендовать следующие источники: конспекты лекций и/или практических и лабораторных занятий, учебную литературу соответствующего профиля.

Преподаватель в начале чтения курса информирует обучающихся о формах, видах и содержании самостоятельной работы, разъясняет требования, предъявляемые к результатам самостоятельной работы, а также формы и методы контроля и критерии оценки.

Методические рекомендации по подготовке к зачету

Подготовка к зачету начинается с первого занятия по дисциплине, на котором обучающиеся получают предварительный перечень вопросов к зачёту и список рекомендуемой литературы, их ставят в известность относительно критериев выставления зачёта и специфике текущей и промежуточной аттестации. С самого начала желательно планомерно осваивать материал, руководствуясь перечнем вопросов к зачету и списком рекомендуемой литературы, а также путём самостоятельного конспектирования материалов занятий и результатов самостоятельного изучения учебных вопросов.

Темы, вынесенные на самостоятельное изучение, необходимо законспектировать. В конспекте кратко излагается основная сущность учебного материала, приводятся необходимые обоснования, табличные данные, схемы, эскизы, графики и т.п. Конспект целесообразно составлять целиком на тему. При этом имеется возможность всегда дополнять составленный конспект материалами из журналов, данных из Интернета и других источников. Таким образом, конспект становится сборником необходимых материалов, куда аспирант вносит всё новое, что он изучил, узнал. Такие конспекты представляют, большую ценность при подготовке к занятиям.

Основные этапы самостоятельного изучения учебных вопросов:

1. Первичное ознакомление с материалом изучаемой темы по тексту учебника, дополнительной литературе.

2. Выделение главного в изучаемом материале, составление обычных кратких записей.

3. Подбор к данному тексту опорных сигналов в виде отдельных слов, определённых знаков, графиков, рисунков.

4. Продумывание схематического способа кодирования знаний, использование различного шрифта и т.д.

5. Составление опорного конспекта.

Методические рекомендации по подготовке к экзамену

Экзамен преследует цель оценить работу обучающегося за определенный курс: полученные теоретические знания, их прочность, развитие логического и творческого мышления, приобретение навыков самостоятельной работы, умения анализировать и синтезировать полученные знания и применять на практике решение практических задач.

Формулировка вопросов совпадает с формулировкой перечня вопросов, доведенного до сведения обучающихся за один месяц до экзаменационной сессии. В процессе подготовки к экзамену организована предэкзаменационная консультация для всех учебных групп. Результат экзамена выражается оценкой «отлично», «хорошо», «удовлетворительно».

С целью уточнения оценки экзаменатор может задать не более одного-двух дополнительных вопросов, не выходящих за рамки требований рабочей программы дисциплины. Под дополнительным вопросом подразумевается вопрос, не связанный с тематикой вопросов билета. Дополнительный вопрос, также, как и основные вопросы билета, требует развернутого ответа. Кроме того, преподаватель может задать ряд уточняющих и наводящих вопросов, связанных с тематикой основных вопросов билета. Число уточняющих и наводящих вопросов не ограничено.