Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Методы атакующего воздействия на информационные ресурсы

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2024 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Практические	32	32	32	32
Итого ауд.	96	96	96	96
Контактная работа	96	96	96	96
Сам. работа	12	12	12	12
Часы на контроль	36	36	36	36
Итого	144	144	144	144

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): д.э.н., профессор, Тищенко Е.Н.

Зав. кафедрой: к.э.к., доц. Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Изучение и анализ способов нарушения информационной безопасности, потенциально опасные пути несанкционированного доступа к информации, модель поведения потенциального нарушителя, организации удаленных атак и способы защиты от них.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-4: способен принимать участие в проведении экспериментальных исследований объекта информационной безопасности

В результате освоения дисциплины обучающийся должен:
Знать:
Методы проведения экспериментальных исследований объекта информационной безопасности (соотнесено с индикатором ПК-4.1)
Уметь:
Применять методы проведения экспериментальных исследований объекта информационной безопасности (соотнесено с индикатором ПК-4.2)
Владеть:
Применения методов проведения экспериментальных исследований объекта информационной безопасности (соотнесено с индикатором ПК-4.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Виды деструктивного воздействии на информационные ресурсы

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Классификация вредоносного программного обеспечения. Вторжения в информационные системы. Сетевые черви, компьютерные вирусы, троянские программы, хакерские утилиты. Основные признаки атак. / Лек /	5	4	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
1.2	Классификация хакерских атак. Определение хакерской атаки. Основные типы хакерских атак. Этапы подготовки и проведения атак / Лек /	5	4	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
1.3	Составление досье с использованием интернет-ресурсов для оценки воздействия ИКТ-технологий на неприкосновенность частной жизни / Лаб /	5	8	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
1.4	Классификация вредоносного программного обеспечения. Заражение прямым действием / Пр /	5	8	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
1.5	Деструктивные программы и хакинг мобильных устройств / Ср /	5	4	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2

Раздел 2. Вирусы, троянские программы, почтовые черви, снифферы, Rootkit- ы и другие специальные средства

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	Сетевые компьютерные атаки. Цели сетевых атак. Классификация. Уязвимости ПО. Основных тенденций развития защиты информации от сетевых атак. / Лек /	5	4	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
2.2	Ботнеты - новый характер угроз. Ботнет как основная угроза интернетсетей. Способы создания ботсетей. Типы атак и применяемые шпионские программы. Цели атака. Инструментальные и программные способы противодействия. / Лек /	5	4	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2

2.3	Разработка макета простейшей троянской программы / Лаб /	5	8	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
2.4	Зомби-сети. (моделирование сети ботнет). / Пр /	5	8	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
2.5	DDoS-атаки и методы борьбы с ними Man in the middle (M1TM) Дефейс веб-сайтов и его классификация / Ср /	5	4	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2

Раздел 3. Хакинг и антнхакинг информационных систем

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
3.1	Организация зашиты операционной системы. Критерии оценки надежности системы. Компоненты зашиты и их характеристика. Работа и объекты системы зашиты. / Лек /	5	4	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
3.2	Хакинг браузеров Web. Злонамеренный код HTML. Генерация диалогов. Переполнение памяти. Запуск программ. Тег IFRAME. Подмена Webсайтов. Методы социальной инженерии. Методы защиты. / Лек /	5	4	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
3.3	Хакинг информационных систем. Хакинг почтовых клиентов. Введение в функционирование почтовых сервисов, технология вставки активного кода в почтовое вложение для запуска на атакованном компьютере, некоторые недостатки электронной почты, управляемой с Web-страниц. / Лек /	5	4	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
3.4	Введение в функционирование почтовых сервисов. / Лаб /	5	8	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
3.5	Назначение и использование программ Backdoor Kits и Log Bashers / Пр /	5	8	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
3.6	Спуфинг (Spoofing) - имитация соединения / Ср /	5	4	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2

Раздел 4. Хакинг и антихакинг клиентов интернет-сервисов

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
4.1	Хакинг межсетевых экранов. Компоненты межсетевого экрана. Настройка шлюзов с фильтрацией пакетов. Уязвимости шлюзов с фильтрацией пакетов. Программные посредники. / Лек /	5	2	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
4.2	Перехват сетевых данных. Технологии сетевого хакинга, основанные на перехвате сетевых пакетов (прослушивания сетевого трафика с целью хишения ценной информации, для организации перехвата данных с целью атаки "человек посредине", для перехвата TCP-соединений) Программы-сниферы для прослушивания сетевых пакетов. / Лек /	5	2	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
4.3	Взлом паролей операционной системы, использование программы PasswordCrackers / Лаб /	5	8	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2
4.4	Программы SafeSuite и SATAN. Назначение и использование / Пр /	5	8	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2

Раздел 5. Промежуточная аттестация					
№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
5.1	/ Экзамен /	5	36	ПК-4	Л1.1, Л1.2, Л2.1, Л2.3, Л2.2

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Бердюгин А. А., Дудка А. Б., Конявская С. В., Конявский В. А., Назаров И. Г., Ревенков П. В.	Кибербезопасность в условиях электронного банкинга: практическое пособие	Москва: Прометей, 2020	https://biblioclub.ru/index.php?page=book&id=610688 неограниченный доступ для зарегистрированных пользователей
Л1.2	Сэрра Э.	Кибербезопасность: правила игры: как руководители и сотрудники влияют на культуру безопасности в компании: практическое руководство	Москва: Альпина Паблишер, 2022	https://biblioclub.ru/index.php?page=book&id=707494 неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Родичев Ю. А.	Информационная безопасность: нормативно-правовые аспекты: учеб. пособие для студентов, обучающихся по спец. 090102 "Компьютер. безопасность", 090105 "Комплекс. обеспечение информ. безопасности автоматизир. систем"	СПб.: Питер, 2008	10
Л2.2	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	https://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей
Л2.3	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2012	https://biblioclub.ru/index.php?page=book&id=211299 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Информационная справочная правовая система "Консультант Плюс"
Информационная справочная правовая система "Гарант" https://internet.garant.ru

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
Офисный пакет LibreOffice (кроссплатформенное свободно распространяемое программное обеспечение)

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и свободно распространяемыми программными средствами и выходом в Интернет.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-4: способен принимать участие в проведении экспериментальных исследований объекта информационной безопасности			
Знать методы проведения экспериментальных исследований объекта информационной безопасности	Описывает способы решения стандартных задач профессиональной деятельности в области информационной безопасности при формировании системы защиты информации при ответе на вопросы	Полный, развёрнутый ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное	Опрос (вопросы 1-20) Вопросы к экзамену (вопросы 1-48)
Уметь применять методы проведения экспериментальных исследований объекта информационной безопасности	Анализирует состояние системы защиты информации, выявляет ее уязвимые места и определяет направления ее совершенствования при выполнении практико-ориентированного и практического задания	Полнота и правильность решения практико-ориентированного задания или практического задания	Лабораторные задания (задания 1-4) Практические задания (задания 1-4) Практико-ориентированные задания к экзамену (задания 1-9)
Владеть навыками применения методов проведения экспериментальных исследований объекта информационной безопасности	Использует методы и средства защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России при выполнении практико-ориентированного и практического задания	Обоснованность и правильность обращения к нормативным источникам, методам и средствам при выполнении практико-ориентированного и практического задания	Лабораторные задания (задания 1-4) Практические задания (задания 1-4) Практико-ориентированные задания к экзамену (задания 1-9)

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляются в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

84-100 баллов (оценка «отлично»)

67-83 баллов (оценка «хорошо»)

50-66 баллов (оценка «удовлетворительно»)

0-49 баллов (оценка «неудовлетворительно»)

2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к экзамену

1. Основные классы вредоносного программного обеспечения.
2. Сетевые черви.
3. Классически вирусы
4. Троянские программы

5. Виды хакерских атак
6. Mailbombing
7. Переполнение буфера
8. Сниффинг пакетов 9.1P-спуфинг
9. Man-in-the-Middle
10. Инъекция
11. Отказ в обслуживании
12. Сетевые компьютерные атаки. Классификация.
13. Ботнеты, общая классификация.
14. Структура ботнетов.
15. Способы организации ботнетов.
16. Диагностика ботнетов, методы обнаружения и локализации.
17. Средства защиты в операционной системе.
19. Диспетчер SAM (Security Account Manager) и Служба AD (Active Directory)
20. Объекты системы зашиты
21. Регистрация в домене
22. Антихакинг в системе защиты операционной системы
23. Этапы проникновения в ОС выделенного компьютера.
24. Применение утилиты NTFSDOS Pro для проникновения ОС выделенного компьютера.
25. Взлом паролей BIOS и экранной заставки.
26. Взлом базы SAM и расширение привилегий.
27. Хакинг Web броузеров (генерация диалогов, злонамеренные HTML)
28. Хакинг Web броузеров (запуск программ, переполнение памяти)
29. Хакинг Web броузеров (запуск программ)
30. Хакинг Web броузеров (тег IFRAME)
31. Злонамеренные an.ien.i и сценарии при хакингс Web броузеров.
32. Считывание файлов "куки".
33. Подмена Web-сайтов.
34. Хакинг SSL (протокол защищенных сокетов)
35. Методы социальной инженерии при защите от хакинга
36. Протоколы электронной почты
37. Формат сообщение электронной почты.
38. Хакинг электронной почты, последовательность действий злоумышленника.
39. Установление удалённого контроля с помощью электронной почты.
40. Деструкция почтового клиента.
41. Этапы хакинга Web-сайта.
42. Сканирование и инвентаризация сервера.
43. Хакинг http. 44. Уязвимости сценариев Web-серверов.
45. Программы для офлайнового просмотра Web-сайтов.
46. Что даёт хакеру исследование кода HTML Web-caftTa
47. Последовательность действий хакера при взломе пароля к страничке Web.
48. Разновидности атак DoS.

Практико-ориентированные задания к экзамену

1. Разработка концепции, программы и плана исследования.
2. Выбор метода исследования на различных этапах работы.
3. Получение первичной информации об объекте исследования с использованием инструментальных методов.
4. Обработка первичной информации об объекте исследования.
5. Разработка модели информационной безопасности электронного документооборота
6. Разработка модели атаки на информационную систему электронного документооборота
7. Разработка комплекта типовых эксплуатационных документов системы электронного документооборота

8. Подбор и обоснование выбора средств защиты информации и их компонентов.
9. Проведение аудита защищенности системы электронного документооборота по требованиям контролирующих органов

Экзаменационное задание включает 2 теоретических вопроса (раздел «Вопросы к экзамену») и 1 практико-ориентированное задание (формируется из перечня заданий, представленных в разделе «Практико-ориентированные задания к экзамену»).

Критерии оценивания:
Максимальное количество баллов за экзаменационное задание – 100 (30 баллов максимально за каждый теоретический вопрос, 40 баллов максимально за практико-ориентированное задание).

Критерии оценивания одного теоретического вопроса:
- 25-30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;
- 20-24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;
- 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;
- 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Критерии оценивания практико-ориентированного задания:
- 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы.
- 25-34 балла выставляется, если задание решено полностью, но при ответе допущены незначительные ошибки.
- 11-24 балла выставляется, если задание решено частично.
- 0-10 баллов выставляется, если решение неверно или отсутствует.

Итоговый результат формируется из суммы набранных баллов за выполнение экзаменационного задания и соответствует шкале:

84-100 баллов (оценка «отлично»)
67-83 баллов (оценка «хорошо»)
50-66 баллов (оценка «удовлетворительно»)
0-49 баллов (оценка «неудовлетворительно»)

Опрос

Вопросы для опроса:
1. Понятие удаленной сетевой атаки. Уязвимости стека протоколов TCP/IP. Уязвимости телекоммуникационных систем.
2. Классификация удаленных сетевых атак: по характеру воздействия, по цели воздействия, по условию начала воздействия, по наличию обратной связи, по расположению субъекта атаки, по уровням эталонной модели OSI.
3. Объекты атаки удаленной сетевой атаки, цели атаки, этапы атаки, инструменты атаки, топология атаки.
4. IP-спуфинг (Blind Spoofing): особенности, алгоритм реализации.
5. TCP Hijacking/Man in the middle: особенности, алгоритм реализации.

6. Инъекции: особенности, алгоритм реализации.
7. DoS (Denial of Service)/DDoS (Distributed Denial of Service)/Flooding: особенности, алгоритм реализации.
8. Понятие межсетевого экрана. Классификация межсетевых экранов: классы, типы, по объекту защиты, по типу фильтрации, по особенностям реализации.
9. Требования, предъявляемые к межсетевым экранам. Схемы подключения межсетевых экранов.
10. Понятие систем обнаружения/предотвращения аномалий (вторжений) (IDS/IPS). Классификация IDS/IPS-систем. Архитектура IDS/IPS-систем.
11. Методы обнаружения вторжений IDS/IPS-системами.
12. Понятие и структура ГосСОПКи. Алгоритмы работы ГосСОПКи.
13. Понятие аудита информационной безопасности. Цель, аудита, исполнители, направления проведения аудита.
14. Классификация типов аудита. Последовательность проведения аудита.
15. Экспертный аудит: цели, задачи, последовательность реализации.
16. Инструментальный аудит: цели, задачи, последовательность реализации, средства проведения аудита.
17. Методы анализа данных, полученных при проведении аудита. Нормативное сопровождение аудита.
18. Структура отчета аудита. Основные требования к отчету аудита.
19. Средства защиты в операционной системе.
20. Этапы проникновения в ОС выделенного компьютера

Критерии оценивания*:*
Максимальное количество баллов, которые обучающийся может набрать – 20 баллов (за 20 ответов).
Ответ на вопрос оценивается:

- 1 балл – правильный и полный ответ;
- 0 баллов – неправильный ответ или ответ не представлен.

Лабораторные задания

Задание 1.
Разработка макета простейшей троянской программы.

Задание 2
Конфигурирование почтовых сервисов.

Задание 3.
Взлом паролей операционной системы, использование программы PasswordCrackers.

Задание 4.
Составление досье с использованием интернет-ресурсов для оценки воздействия ИКТ-технологий на неприкосновенность частной жизни.

Критерии оценивания:
Максимальное количество баллов, которые обучающийся может набрать – 40 баллов (за 4 задания).
Каждое задание оценивается:

- 10 баллов. – задание выполнено верно;
- 9-7 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;
- 6-3 баллов. – при выполнении задания были допущены ошибки;
- 2- 1 баллов. – при выполнении задания были допущены существенные ошибки;
- 0 баллов. – задание не выполнено.

Практические задания

Задание 1.

Зомби-сети (моделирование сети ботнет).

Задание 2
Назначение и использование программ Backdoor Kits и Log Bashers.

Задание 3.
Программы SafeSuite и SATAN. Назначение и использование.

Задание 4.
Классификация вредоносного программного обеспечения. Заражение прямым действием.

Критерии оценивания:
Максимальное количество баллов, которые обучающийся может набрать – 40 баллов (за 4 заданий).
Каждое задание оценивается:

- 10 баллов. – задание выполнено верно;
- 9-7 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;
- 6-3 баллов. – при выполнении задания были допущены ошибки;
- 2- 1 баллов. – при выполнении задания были допущены существенные ошибки;
- 0 баллов. – задание не выполнено.

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме экзамена.

Экзамен проводится по расписанию промежуточной аттестации в устной форме. Количество вопросов в экзаменационном задании – 3 (2 теоретических, 1 практико-ориентированное задание). Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные работы;
- практические занятия.

В ходе лекционных занятий рассматриваются основные понятия в области криптографической защиты информации, методы криптографии и криптоанализа, даются рекомендации для самостоятельной работы и подготовки к лабораторным работам и практическим занятиям.

В ходе лабораторных работ и практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач по криптографической защите.

При подготовке к лабораторным работам и практическим занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной или практической работы;

В процессе подготовки к лабораторным работам и практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях, лабораторных работах и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных источников. Выделить непонятные термины и найти их значение в энциклопедических словарях.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.