МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета компьютерных технология и информационной безопасности
_____ П.Ю. Гусев
«___» августа 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

«Системы противодействия компьютерным атакам»

Специальность 10.05.01 Компьютерная безопасность

Специализация специализация № 4 "Безопасность распределенных компьютерных систем и сетей (связь, информационные и коммуникационные технологии)"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Автор программы _____ /Белоножкин В.И/

Заведующий кафедрой систем информационной безопасности _____ /Остапенко А.Г./

Руководитель ОПОП _____ Остапенко А.Г /

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Формирование и закрепление общепрофессиональных и профессиональных компетенций, направленных на знание и владение современными методами и технологиями противодействия информационным атакам и операциям, реализуемым в компьютерных системах и сетях.

1.2. Задачи освоения дисциплины

- ознакомление с основными принципами построения систем противодействия компьютерным атакам, способами обнаружения и нейтрализации последствий вторжений в компьютерные системы;
- формирование умений анализировать защищенность компьютерных систем, управлять системами противодействия компьютерным атакам;
- приобретение навыков выявления и устранения уязвимостей компьютерных систем, настройки систем противодействия компьютерным атакам.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Системы противодействия компьютерным атакам» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б.1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Системы противодействия компьютерным атакам» направлен на формирование следующих компетенций:

ПК-4.7 - Способен участвовать в работах по противодействию информационным атакам и операциям, реализуемым в компьютерных системах и сетях

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-4.7	знать основные принципы построения и механизмы функционирования систем противодействия компьютерным атакам, особы обнаружения и нейтрализации последствий вторжений в компьютерные системы
	уметь анализировать защищенность компьютерных систем, управлять системами противодействия компьютерным атакам
	владеть навыками выявления и устранения уязвимостей компьютерных систем, настройки систем противодействия компьютерным атакам.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Системы противодействия компьютерным атакам» составляет 7 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		9	10
Аудиторные занятия (всего)	126	54	72
В том числе:			
Лекции	72	36	36
Практические занятия (ПЗ)	54	18	36
Самостоятельная работа	126	18	108
Курсовой проект	+	+	
Виды промежуточной аттестации – зачет, зачет с оценкой	+	+	+
Общая трудоемкость: академические часы зач.ед.	 252 7	 72 2	 180 5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	СРС	Всего, час
1	Системный подход к обеспечению защиты от компьютерных атак	Компьютерные системы и их компоненты как объекты защиты от угроз безопасности. Направления, методы и методики построения защищенных компьютерных систем. Организационные методы и средства защиты компьютерных систем от атак.	24	10	10	74
2	Средства выявления и локализации уязвимостей компьютерных систем к воз-действию угроз безопасности	Методы и средства оценки защищенности, контроля доступа к компонентам компьютерных систем. Методы и средства обеспечения безопасности электропитания компьютерных систем, гарантированного уничтожения информации, выявления и локализации утечек информации по техническим каналам	12	8	8	52
3	Методы и средства обнаружения и отражения сетевых атак	Методы и средства обнаружения сетевых атак и вредоносных программ. Контентная фильтрация и межсетевое экранирование. Средства создания виртуальных частных сетей.	18	20	60	46
4	Комплексные системы защиты от компьютерных атак	Доверенные аппаратные среды. Подсистемы безопасности операционных систем, СУБД, прикладного программного обеспечения. Комплексные системы защиты локальных и корпоративных сетей.	18	16	48	44

		Системы контроля работы пользователей компьютерных систем. Оснащение центров Государственной системы обнаружения и противодействия компьютерным атакам РФ.				
		Итого	**72**	**54**	**126**	**252**

5.2. Перечень лабораторных работ

Не предусмотрено учебным планом.

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсового проекта в 9 семестре для очной формы обучения.

Примерная тематика курсового проекта: «Разработка алгоритмов компьютерной атаки и методики противодействия».

Задачи, решаемые при выполнении курсового проекта:

- Сбор и обобщение информации о реализациях заданного вида компьютерных атак.
- Анализ возможных методов противодействия заданному виду компьютерных атак.
- Построение алгоритмов компьютерной атаки и методики противодействия ей.

Курсовой проект включат в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-4.7	знать основные принципы построения и механизмы функционирования систем противодействия компьютерным атакам, особы обнаружения и нейтрализации последствий вторжений в компьютерные системы	Ответ на вопрос преподавателя	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	уметь анализировать защищенность компьютерных систем, управлять системами противодействия компьютерным атакам	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками выявления и устранения уязвимостей компьютерных систем, настройки систем противодействия компьютерным атакам.	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 7, 8 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПК-4.7	знать основные принципы построения и механизмы функционирования систем противодействия компьютерным атакам, особы обнаружения и нейтрализации последствий вторжений в компьютерные системы	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь анализировать защищенность компьютерных систем, управлять системами противодействия компьютерным атакам	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть навыками выявления и устранения уязвимостей компьютерных систем, настройки систем противодействия компьютерным атакам.	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

или

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-4.7	знать основные принципы построения и механизмы функционирования систем противодействия компьютерным атакам, особы обнаружения и нейтрализации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	последствий вторжений в компьютерные системы					
	уметь анализировать защищенность компьютерных систем, управлять системами противодействия компьютерным атакам	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками выявления и устранения уязвимостей компьютерных систем, настройки систем противодействия компьютерным атакам.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2. Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Компьютерная атака - это:

а) реализация угрозы безопасности;

б) целенаправленное воздействие на компьютерную систему программно-техническими средствами, направленное на нарушение доступности, целостности, конфиденциальности информации;

в) проявление уязвимости компьютерной системы.

2. Угрозы безопасности компьютерным системам могут быть классифицированы:

а) по направленности реализации

б) по типу уязвимости;

в) по способу устранения негативных последствий.

3. Завершающим этапом компьютерной атаки является:

а) получение несанкционированного доступа;

б) маскировка следов атаки;

в) планирование атаки

4. Уязвимость компьютерной системы - это:

а) свойство ее компонента или процесса, путем использования которого может быть осуществлено несанкционированное воздействие на объекты защиты;

б) проявление воздействия угрозы безопасности;

в) нарушение работы средств защиты информации.

5. К идентификационным признакам контроля доступа к компьютерным системам относятся:

а) биометрические характеристики;

б) паспортные жанные;

в) IP-адрес компьютера.

7. К основным направлениям контроля эффективности защиты от атак относятся:

а) мониторинг работы пользователей;

б) моделирование компьютерных атак;

в) проверка журналов системных событий.

8. В состав функций средств обнаружения вторжений входит:

а) конфигурирование сетевых устройств;

б) контроль работы системного администратора;

в) выявление атак и подозрительной сетевой активности.

9. Сеть-приманка - это:

а) защищенный ресурс, который служит объектом атак;

б) атакуемый фрагмент корпоративно сети;

в) средство выявления утечек информации.

10. Корпоративный центр ГосСОПКА должен включать в себя:

а) удостоверяющий центр ЭЦП;

б) центр операций по обеспечению безопасности;

в) центр управления ключевой информацией.

7.2.2 Примерный перечень заданий для решения стандартных задач

1. К техническим характеристикам электронных замков относится:

а) быстродействие;

б) способ считывания информации;

в) компания-производитель.

2. Рекомендации по использованию программных СЗИ нужны для:

а) выбора оптимального состава СЗИ;

б) подготовки эксплуатационной документации;

в) организации работы службы информационной безопасности.

3. В архитектуру типовой комплексной СЗИ для локальных сетей входит:

а) рабочее место администратора;

б) подсистема шифрования трафика;

в) криптоядро.

4. В защищенной операционной системе базовые средства защиты располагаются в:

а) прикладных программах;

б) ядре;

в) системных службах.

5. Риск компьютерной атаки рассчитывается как:

а) сумма ущербов от реализованной атаки;

б) произведение вероятности реализации атаки и возможного ущерба ;

в) произведение рейтинга атаки и ее длительности.

6. DOS-атака нарушает:

а) конфиденциальность;
б) доступность;
в) своевременность.
7. Основное свойство компьютерного вируса:
а) уничтожение информации;
б) размножение;
в) скрытность.
8. Системы контроля пользователей применяются для:
а) выявления инсайдерских утечек информации;
б) мониторинга внешней сетевой активности;
в) подтверждения лояльности сотрудников.
9. Для обнаружения компьютерных атак используются:
а) наборы правил;
б) сигнатуры;
в) шаблоны и макросы.
10. В число отличий локальной и корпоративной сетей входит:
а) количество сетевых соединений;
б) вид сетевого протокола;
в) расположение линий связи относительно контролируемой зоны.

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Настройка веб-браузера для обеспечения безопасной работы в Интернет включает в себя:
а) установку дополнений;
б) отключение всплывающих окон;
в) блокировку загрузки файлов.
2. Описание примерного алгоритма обнаружения атаки типа "отказ в обслуживании" начинается с:
а) формулировки задачи;
б) перечисления контролируемых портов;
в) поиска злоумышленника.
3. Разграничение доступа пользователей на основе дискреционного принципа контроля использует механизм:
а) ролей;
б) меток безопасности;
в) набора правил.
4. Функции управления СЗИ "Secret Net Studio" разделяютя для:
а) пользователей сети;
б) сотрудников ИТ-службы;
в) администраторов безопасности.
5. Основные настройки персонального межсетевого экрана для обеспечения безопасной работы в Интернет регулируют:
а) входящий трафик;
б) отображение графики на экране;
в) количество запускаемых приложений.

6. Типовая структура подсистемы безопасности операционной системы включает в себя:

а) средства аутентификации;

б) сетевые драйверы;

в) модуль ввода-вывода.

7. Защищенная СУБД отличается наличием:

а) подсистемы безопасности;

б) средств шифрования;

в) сетевых служб.

8. Средства моделирования атак используют:

а) алгоритмы известных атак;

б) перебор случайных воздействий;

в) многократное повторение базовых операций ввод-вывода.

9. К техническим характеристикам средств обнаружения и блокирования сетевых атак относится:

а) время реагирования;

б) наличие функции отключения;

в) нагрузочная способность.

10. Набор функций AAA для беспроводных сетей включает:

а) авторизацию;

б) ассоциацию;

в) атрибутизацию.

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Классификация угроз безопасности компьютерным системам.
2. Системные принципы защиты информации в компьютерных системах.
3. Стратегические направления государственной политики России в сфере противодействия компьютерным атакам
4. Методика построения комплексной защиты компьютерных систем.
5. Информационные технологии, повышающие защищенность компьютерных систем.
6. Структура и функции ГосСОПКА.
7. Методика расследования компьютерных атак
8. Характеристика средств защиты целостности и бесперебойности функционирования компьютерных систем.
9. Методика организации защищенного электропитания компьютерных систем.
10. Методы и средства контроля эффективности защиты информации в компьютерных системах.

7.2.5 Примерный перечень вопросов для подготовки к экзамену

Не предусмотрено учебным планом.

7.2.6 Методика выставления оценки при проведении промежуточной аттестации

Зачет проводится по тест-билетам, каждый из которых содержит 5 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, верное решение адачи оценивается в 5 баллов. Максимальное количество набранных баллов – 10.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 2 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 2 до 4 баллов.

3. Оценка «Хорошо» ставится в случае, если студент набрал от 5 до 7 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 8 до 10 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Системный подход к обеспечению защиты от компьютерных атак	ПК-4.7	Тест, контрольное задание, защита реферата
2	Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности	ПК-4.7	Тест, требования к курсовому проекту
3	Методы и средства обнаружения и отражения сетевых атак	ПК-4.7	Тест, контрольная работа
4	Комплексные системы защиты от компьютерных атак	ПК-4.7	Тест

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи

компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсового проекта осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8. УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1. Перечень учебной литературы, необходимой для освоения дисциплины

1. Лукацкий А.В. Обнаружение атак. - СПб.: BHV, 2003. -596 с.
2. Синадский Н. И., Хорьков Д. А. Защита информации в компьютерных сетях: учебное пособие . — Екатеринбург : УрГУ,
2008. -225 с.
3. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). - М.: Горячая линия — Телеком, 2013, -220 с.
4. Новак Д., Норткатт С., Маклахен Д. Как обнаружить вторжение в сеть. 2016. -384 с.
5. Ларина Е.С., Овчинский В.С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. – М.: Книжный мир, 2014. -352 с.
6. Белоножкин В.И., Системы обнаружения компьютерных атак: учебное пособие. ВГТУ, 2015. [Эл.ресурс].
7. Мельников Д.А. Информационная безопасность открытых систем : учебник / Д.А. Мельников. — М.: ФЛИНТА : Наука, 2013. -448 с.
Бабин С. А. Лаборатория хакера. — СПб.: БХВ-Петербург, 2016. -240 с.
8. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.
9. Остапенко А.Г. Сетео-информационная эпидемиология: учебное пособие для вузов. - М.: Горячая линия – Телеком, 2021. -216с.

8.2. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

– Электронный ресурс "Безопасность информационных систем", http://infobez.com;

– Банк данных угроз безопасности информации. Электрон. дан. - Режим доступа: http://www.bdu.fstec.ru

– Стандарт Common Vulnerabilities and Exposures. Электрон. дан. - Режим доступа: http://cve.mitre.org

– База данных с информационными бюллетенями (Secunia Advisories), содержащими сведения об обнаруженных угрозах и уязвимостях ПО Secunia Advisory and Vulnerability Database Электрон. дан. - Режим доступа: https://secuniaresearch.flexerasoftware.com/community/advisories

– База уязвимостей VND (Vulnerability Notes Database Электрон. дан. - Режим доступа: https://www.kb.cert.org/vuls

– База сценариев эксплуатации уязвимостей Exploit Database Электрон. дан. - Режим доступа: https://www.exploit-db.com

– Агрегатор информации об уязвимостях CVEDetails. Электрон. дан. - Режим доступа: https://www.cvedetails.com

– Information Security Информационная безопасность. Электрон. дан. - Режим доступа: http://www.itsec.ru

– Securitylab.ru by Positive Technologies. Электрон. дан. - Режим доступа: https://www.securitylab.ru/
– Anti-Malware.ru. Электрон. дан. - Режим доступа: https://www.anti-malware.ru/news
– Iso27000.ru Искусство управления информационной безопасностью. Электрон. дан. - Режим доступа: http://www.iso27000.ru/
– SecurityPolicy.ru Документы по информационной безопасности. Электрон. дан. - Режим доступа: http://securitypolicy.ru/
– SearchInform – Информационная безопасность. Электрон. дан. - Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/
– Информационная безопасность предприятия. Электрон. дан. -
Режим доступа: Ekrost.ru
– Портал «Код информационной безопасности» https://codeib.ru/;
– Портал «Anti-Malware» https://www.anti-malware.ru;
– портал «Information Security» https://www.itsec.ru;
– электронный журнал «Information Security» http://lib.itsec.ru/imag/;
– операционные системы Microsoft Windows, Linux;
– офисное ПО «Libre Office»;
– СУБД «Линтер»;
– СПО «Vipnet client»;
– антивируное ПО «Kaspersky free”;
- веб-браузеры Firefox, Chrome, Yandex;
- почтовые клиенты Thunderbird, Outlook.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ

ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Аудитория с компьютерными рабочими местами, локальная сеть, презентационное оборудование.

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

По дисциплине «Системы противодействия компьютерным атакам» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков использования методов и средств выявления и локализации последствий компьютерных атак. Занятия проводятся путем решения конкретных задач в аудитории.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные

	перед зачетом, зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.