МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ С.М. Пасмурнов

«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Математическое моделирование информационных операций и атак»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация Обеспечение информационной безопасности распределѐнных информационных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ / Чопоров О.Н./

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

Руководитель ОПОП _____ / Остапенко А.Г./

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Целью изучения дисциплины является подготовка специалистов к деятельности, связанной с разработкой математических моделей информационных атак и операций и эффективной реализацией методов разработки программных средств для решения профессиональных задач.

1.2. Задачи освоения дисциплины – формирование знаний, умений и навыков, позволяющих применять современные методы обнаружения вторжений в компьютерные сети, составлять спецификации на оборудование и программное обеспечение.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Математическое моделирование информационных операций и атак» относится к дисциплинам вариативной части (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Математическое моделирование информационных операций и атак» направлен на формирование следующих компетенций:

ПК-2 - способностью создавать и исследовать модели автоматизиро-ванных систем

ПК-5 - способностью проводить анализ рисков информационной безопасности автоматизированной системы;

ПК-6 - способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**
ПК-2	знать основные понятия и определения, используемые при описании моделей безопасности компьютерных систем
	уметь разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем
	владеть способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах
ПК-5	знать способы и средства контроля эффективности защиты информации
	уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы

ПК-6	знать методики аудита защищенности информационно-технологических ресурсов распределенных информационных систем
	уметь проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Математическое моделирование информационных операций и атак» составляет 6 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		5	6
Аудиторные занятия (всего)	134	54	80
В том числе:			
Лекции	76	36	40
Лабораторные работы (ЛР)	58	18	40
Самостоятельная работа	46	18	28
Курсовой проект	+		+
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 216 6	 72 2	 144 4

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	Лаб. зан.	СРС	Всего, час
1	Основные определения и понятия	Понятие «атака» и «операция» в информационном аспекте. Классификация атак. Этапы реализации атак: сбор информации, основные механизмы реализации атак, реализация атак, завершение атаки. Принципы построения СОВ. Классификация и архитектура.	14	10	6	30
2	Технологии построения СОВ	Существующие технологии СОВ. Повышение эффективности систем. Характеристика	14	10	8	32

		направлений и групп методов обнаружения вторжений. Сравнительный анализ существующих СОВ.				
3	Анализ существующих моделей защиты автоматизированных систем от информационных атак	Табличные и диаграммные модели информационных атак Формализованные модели информационных атак Анализ существующих моделей процесса обнаружения информационных атак Сигнатурные модели процесса обнаружения атак Поведенческие модели процесса выявления атак Модели процесса оценки рисков информационной безопасности АС Модель, заложенная в основу программного комплекса оценки рисков «Кондор» Модель, заложенная в основу программного комплекса оценки рисков «Гриф» Модель, заложенная в основу программного комплекса оценки рисков «RiskMatrix» Модель, заложенная в основу методики оценки рисков «OCTAVE»	12	10	8	30
4	Разработка математических моделей защиты автоматизированных систем от информационных атак	Математическая модель информационных атак на ресурсы автоматизированных систем. Формальное описание модели информационных атак Особенности использования разработанной математической модели информационных атак Математическая модель процесса обнаружения информационных атак Математическая модель процесса оценки рисков информационной безопасности автоматизированных систем. Описание модели процесса оценки рисков информационной безопасности. Особенности использования модели оценки рисков безопасности. Методика разработки рекомендаций по повышению уровня защиты автоматизированных систем на основе модели оценки рисков безопасности	12	10	8	30
5	Формирование математической модели процесса	Выбор разработанного прототипа системы обнаружения атак, построенного на основе	12	10	8	30

	выявления информационных атак	поведенческой модели Объект и цель испытаний Функциональные требования к прототипу системы обнаружения атак. Технические и программные средства проведения испытаний Порядок проведения испытаний Результаты проведѐнных испытаний Описание системы обнаружения атак, предназначенной для промышленной реализации Хостовые датчики системы обнаружения атак. Сетевые датчики системы обнаружения атак Агенты системы обнаружения атак Модуль реагирования системы обнаружения атак. Информационный фонд системы обнаружения атак. Консоль администратора системы обнаружения атак Модуль координации потоков информации системы обнаружения атак				
6	Моделирование террористических атак и операций в информационном аспекте	Анализ террористической деятельности. Сценарные модели наиболее масштабных террористических операций в информационном аспекте. Вероятностные и энтропийные модели террористических атак. Вероятностные модели информационно-психологических последствий террористических актов	12	8	8	28
		Итого	**76**	**58**	**46**	**180**

5.2 Перечень лабораторных работ

1. Свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом IDS/IPS Snort

2. Suricata — open source IPS/IDS система.

3. Сетевой анализатор Wireshark.

4.Среда тестирования на проникновение Metsploit Framework. Анализ уязвимостей, тестирование известных эксплойтов и полная оценка безопасности.

5. Инструмент анализа веб-безопасности Burp Suite Scanner.

6. Тестер на проникновение для оценки безопасности веб-браузера. BeEF (Browser Exploitation Framework).

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

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсового проекта в 6 семестре для очной формы обучения.

Примерная тематика курсового проекта: «Обнаружение аномалий трафика на основе нейронных сетей»»

Задачи, решаемые при выполнении курсового проекта:

• знакомство с аппаратом интеллектуального анализа данных – нейронными сетями;

• выявление аномалий сетевой активности с применением аппарата искуственных нейросетей;

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-2	знать основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	знание основных понятиий и определения, используемые при описании моделей безопасности компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем	умение разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах	владение способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-5	знать способы и средства контроля эффективности защиты информации	знание способов и средств контроля эффективности защиты информации	Выполнение работ в срок, предусмотренный в рабочих	Невыполнение работ в срок, предусмотренный в

			программах	рабочих программах
	уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	умение разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-6	знать методики аудита защищенности информационно-технологических ресурсов распределенных информационных систем	знать методики аудита защищенности информационно-технологических ресурсов распределенных информационных систем		
	уметь проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	умение проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем		

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 5, 6 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПК-2	знать основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПК-5	знать способы и средства контроля эффективности защиты информации	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь разрабатывать предложения по совершенствованию системы	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве	Задачи не решены

	управления информационной безопасностью автоматизированной системы		задач	
ПК-6	знать методики аудита защищенности информационно-технологических ресурсов распределенных информационных систем			
	уметь проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем			

или «отлично»; «хорошо»; «удовлетворительно»; «неудовлетворительно».

Компе-тенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ПК-2	знать основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем	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 способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах	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
ПК-5	знать способы и средства контроля эффективности защиты информации	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью	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 большинс	Задачи не решены

	автоматизированной системы				тве задач	
ПК-6	знать методики аудита защищенности информационно-технологических ресурсов распределенных информационных систем	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	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

7.2.1. Примерный перечень заданий для решения стандартных задач

ПК-2 - способностью создавать и исследовать модели автоматизированных систем	
1.	Поясните отличия понятий множества и системы.
2.	Обоснуйте мотивы формирования систем из множеств и наоборот.
3.	Приведите базовые свойства системы.
4.	Поясните сущность понятий угроза, уязвимость, ущерб и безопасность.
5.	Поясните сущность информационно-кибернетических и информационно-психологических операций
6.	Перечислите основные виды информационных операций
7.	Приведите теоретико-множественную постановку задачи управления социотехническими системами
8.	Поясните сущность функций чувствительности в приложении к оценке безопасности социотехнических систем
9.	Приведите выражения для интегрального, усредненного, элементарного риска и защищен ности социотехнических систем
10.	Поясните мотивы соперничества и сотрудничества социотехнических систем?
11.	Перечислите качества информации, существенные для ее безопасности, а также операции, нарушающие безопасность
12.	Приведите классификацию сетевых угроз и атак
13.	На моделях поясните сущность атак, основанных на подборе имени пароля посредством перебора
14.	Приведите модели атак, основанных на анализе сетевого трафика
15.	На моделях поясните сущность атак, основанных на сканировании портов
ПК-5 - способностью проводить анализ рисков информационной безопасности автоматизированной системы	
1.	Приведите модели атак, основанных на внедрении ложного доверенного объекта
2.	На моделях поясните сущность атак, приводящих к отказу в обслуживании.
3.	Поясните сущность интегрального усредненного риска и защищенности систем на примере различных законов дискретных распределений вероятностей успеха кибератаки
4.	Приведите модели простейших операций информационно-психологического управления
5.	Поясните сущность неформальных организаций
6.	Приведите специфику информационных технологий деструктивных культов.

7.	Покажите особенности информационных операций, реализуемых в рамках политических технологий
8.	Перечислите средства противодействия деструктивным информационно-психологическим операциям
9.	Приведите стохастические модели информационно-управляющего воздействия
10.	Поясните стратегии информационно-управляющих воздействий
11.	На основе теории конфликтов проведите анализ мотивов террористической деятельности
12.	Поясните специфику информационных операций террористического характера
13.	На моделях покажите сущность процессов последействия информационных операций террористического характера.
14.	Приведите сценарные модели информационных операций террористического характера
15.	Перечислите меры противодействия информационным операциям террористического характера
ПК-6 - способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	
1.	Перечислите приемы кибертерроризма
2.	Опишите кризисный период, режим бифуркации и запас устойчивости социотехнических систем с учетом риска теракта
3.	Поясните качественно динамику информационного противоборства на основе поверхности риска теракта
4.	Обоснуйте сравнение теракта с детонатором информационной бомбы.
5.	Табличные и диаграммные модели информационных атак
6.	Формализованные модели информационных атак
7.	Анализ существующих моделей процесса обнаружения информационных атак
8.	Сигнатурные модели процесса обнаружения атак
9.	Поведенческие модели процесса выявления атак
10	Модели процесса оценки рисков информационной безопасности АС
11.	Модель, заложенная в основу программного комплекса оценки рисков «Кондор»
12.	Модель, заложенная в основу программного комплекса оценки рисков «Гриф»
13.	Модель, заложенная в основу программного комплекса оценки рисков «Risk Matrix»
14.	Модель, заложенная в основу методики оценки рисков «OCTAVE»
15.	Математическая модель информационных атак на ресурсы автоматизированных систем

7.2.2. Примерный перечень заданий для решения прикладных задач

ПК-2 - способностью создавать и исследовать модели автоматизированных систем	
1	*1.К основным категориям атак относятся:* **А. атаки на отказ в обслуживании** Б. атаки прохода В. атаки трансформации
2	*К основным категориям атак относятся:* **А. атаки модификации** **Б. атаки на отказ от обязательств** В. атаки прохода
3	*Атака доступа - это:*

	А. попытка получения злоумышленником информации, для просмотра Б. которой у него нет разрешений В. попытка неправомочного изменения информации атака, запрещающая легальному пользователю использование системы, информации или возможностей компьютеров попытка дать неверную информацию о реальном событии или транзакции
4	*Атака доступа направлена на:* А. уничтожение информации Б. уничтожение компьютера **В. нарушение конфиденциальности информации**
5	*Где возможна атака доступа?* А. только в сети интернет Б. только в локальных сетях **В. везде где существует информация и средства ее передачи**
6	*Наиболее надежный способ аутентификации:* А. парольная защита Б. смарт-карты **В. биометрические методы**
7	*Если логин сотрудника компании ivanovVV, то использование какого пароля не допустимо?* **А. ivanovVV** Б. й2ц3у4к5 В. безопасность Г. аО4тг7й6
8	*Какие из этих описаний характеризует централизованные DoS-атаки?* **А. это злонамеренные действия, выполняемые для запрещения легальному пользователю доступа к системе, сети, приложению или информации** **Б. для осуществления атаки система-отправитель посылает огромное количество TCP SYN-пакетов (пакетов с синхронизирующими символами) к системе-получателю, игнорируя ACK-пакеты, добиваясь переполнения буфера очереди соединений** В. в осуществлении атаки участвует большое количество систем, которыми управляет одна главная система и один хакер. Выход системы из строя достигается путем огромного объема передаваемых данных
9	*Какие из этих описаний характеризует распределенные DoS-атаки?* **А. это злонамеренные действия, выполняемые для запрещения легальному пользователю доступа к системе, сети, приложению или информации** Б. для осуществления атаки система-отправитель посылает огромное количество TCP SYN-пакетов (пакетов с синхронизирующими символами) к системе-получателю, игнорируя ACK-пакеты, добиваясь переполнения буфера очереди соединений **В. в осуществлении атаки участвует большое количество систем, которыми управляет одна главная система и один хакер. Выход системы из строя достигается путем огромного объема передаваемых данных**
10	*Выберите верное утверждение:* А. прослушивание (снифинг) работают только в сетях с разделяемой пропускной способностью с сетевыми концентраторами – хабами; использование коммутаторов обеспечивает достаточно надежную защиту от прослушивания **Б. прослушивание (снифинг) хорошо работают в сетях с разделяемой пропускной способностью с сетевыми концентраторами – хабами; использование коммутаторов снижает эффективность снифинга** В. прослушивание (снифинг) работают только в сетях с коммутируемой средой,

	использующей коммутаторы; использование концентраторов исключает возможность снифинга
11	*Хакеры используют для перенаправления трафика:* **А. ARP-спуфинг** **Б. дублирование MAC-адресов** **В. имитация доменного имени** Г. подмену IP-адреса
12	*Какие из перечисленных служб наиболее уязвимы для атаки с изменением IP-адреса?* А. веб-службы Б. электронная почта **В. rlogin** **Г. rsh**
13	*Что входит в величину ущерба, нанесенного при совершении компьютерного преступления?* **А. исправление повреждений от взлома** **Б. стоимость определения величины ущерба** В. ущерб от взлома конфиденциальных данных
14	*Какая атака на компьютерную систему с целью мошенничества с кредитными картами считается преступлением?* **А. сумма ущерба превышает 1000 долл. и злоумышленник завладел 20 номерами кредитных карт** Б. сумма ущерба превышает 1000 долл. и злоумышленник завладел 10 номерами кредитных карт **В. сумма ущерба не превышает 1000 долл. и злоумышленник завладел 20 номерами кредитных карт**
15	*Какая атака на компьютерную систему с целью мошенничества с кредитными картами считается преступлением?* А. сумма ущерба превышает 1000 долл. и злоумышленник завладел 10 номерами кредитных карт Б. сумма ущерба не превышает 5000 долл. и злоумышленник завладел 10 номерами кредитных карт **В. сумма ущерба превышает 5000 долл. и злоумышленник завладел 15 номерами кредитных карт**
16	*По типу, модели обнаружения информационных атак делятся на:* **А. сигнатурные и поведенческие** Б. сигнатурные и автоматные В. автоматные и вероятностные Г. вероятностные и стохастические Д. статистические и гибридные
17	*По типу представления , модели обнаружения информационных атак делятся на:* **А. гибридные, текстовые, графические** Б. сигнатурные и поведенческие В. сигнатурные и автоматные Г. автоматные и вероятностные Д. вероятностные и стохастические Е. статистические и гибридные
18	*По возможности идентификации процесса принятия решения, модели обнаружения информационных атак делятся на (возможно несколько вариантов):* **А. модели, предусматривающие возможность описания процесса принятия**

	решения о выявлении атаки **Б. модели, в которых отсутствует возможность описания процесса принятия решения о выявлении атаки** В. модели, базирующиеся на аппарате математической статистики Г. модели, базирующиеся на аппарате теории графов и сетей Петри Д. модели, базирующиеся на аппарате экспертных систем Е. модели, базирующиеся на аппарате биологических систем (нейросети, иммунные сети, генетические, алгоритмы)
19	*По типу математического аппарата, модели обнаружения информационных атак делятся на (возможно несколько вариантов):* А. модели, предусматривающие возможность описания процесса принятия решения о выявлении атаки Б. модели, в которых отсутствует возможность описания процесса принятия решения о выявлении атаки **В. модели, базирующиеся на аппарате математической статистики** **Г. модели, базирующиеся на аппарате теории графов и сетей Петри** **Д. модели, базирующиеся на аппарате экспертных систем** **Е. модели, базирующиеся на аппарате биологических систем (нейросети, иммунные сети, генетические, алгоритмы)**
20	*По зависимости от наличия формализованного описания атаки или штатного процесса функционирования АС, модели обнаружения информационных атак делятся на (возможно несколько вариантов):* **А. модели, которые могут быть использованы при отсутствии формализованного описания обнаруживаемых атак или штатного процесса функционирования АС** **Б. модели, которые требуют наличия формализованного описания обнаруживаемых атак или штатного процесса функционирования АС** В. модели, базирующиеся на аппарате математической статистики Г. модели, базирующиеся на аппарате теории графов и сетей Петри Д. модели, базирующиеся на аппарате экспертных систем Е. модели, базирующиеся на аппарате биологических систем (нейросети, иммунные сети, генетические, алгоритмы)
21	*Одним из критериев, по которым можно определить эффективность той или иной модели процесса обнаружения атак, является расширяемость. Дайте определение данного критерия:* А. возможность выявления атак, описание которых известно и заложено в параметры модели; Б. возможность выявления новых атак, описание которых еще неизвестно; возможность идентификации причин, по которым было принято решение о факте выявления атаки в АС; **В. свойство, обеспечивающее возможность внесения в модель дополнительных параметров, позволяющих обнаруживать новые типы атак;** Г. возможность использования математического аппарата при описании параметров модели
22	*Одним из критериев, по которым можно определить эффективность той или иной модели процесса обнаружения атак, является формализуемость. Дайте определение данного критерия:* А. возможность выявления атак, описание которых известно и заложено в параметры модели; Б. возможность выявления новых атак, описание которых еще неизвестно; возможность идентификации причин, по которым было принято решение о факте

	выявления атаки в АС; В. свойство, обеспечивающее возможность внесения в модель дополнительных параметров, позволяющих обнаруживать новые типы атак; **Г. свойство, которое указывает на возможность использования математического аппарата при описании параметров модели;** Д. свойство, позволяющее быстро и удобно настраивать параметры модели; Е. свойство, которое позволяет не уменьшать значительно время работы модели при увеличении количества ее параметров, позволяющих обнаруживать новые типы атак.
23	*Одним из критериев, по которым можно определить эффективность той или иной модели процесса обнаружения атак, является масштабируемость. Дайте определение данного критерия:* А. возможность выявления атак, описание которых известно и заложено в параметры модели; Б. возможность выявления новых атак, описание которых еще неизвестно; возможность идентификации причин, по которым было принято решение о факте выявления атаки в АС; В. свойство, обеспечивающее возможность внесения в модель дополнительных параметров, позволяющих обнаруживать новые типы атак; Г. свойство, которое указывает на возможность использования математического аппарата при описании параметров модели; Д. свойство, позволяющее быстро и удобно настраивать параметры модели; **Е. свойство, которое позволяет не уменьшать значительно время работы модели при увеличении количества ее параметров, позволяющих обнаруживать новые типы атак.**
24	*Наиболее распространенной сигнатурной моделью процесса выявления атак является модель….* **А. контекстного поиска определенного множества символов в исходных данных;** Б. регуляризации выражений В. синтаксические модели случайного поиска
25	*К основным характеристикам поведенческой модели процесса выявления атак по критерию возможности выявления известных атак относятся* **А. модель может быть эффективно использована для обнаружения известных типов атак, так как большая часть из них может быть описана в терминах отклонений от штатного протокола сетевого взаимодействия между узлами АС** Б. модель может быть эффективно применена для выявления новых типов атак, проведение которых будет приводить к отклонению от штатного протокола сетевого взаимодействия АС В. модель позволяет проследить процесс принятия решения о наличии или отсутствии атаки в АС. Это может быть сделано путем регистрации результатов выполнения семантических операторов, заложенных в основу модели Г. модель является расширяемой, поскольку она предусматривает возможность увеличения количества обнаруживаемых атак за счет добавления новых элементов в множества состояний и семантических операторов конечного автомата-распознавателя Д. модель является формализованной, так как может быть описана при помощи математического аппарата теории автоматов
26	*Количественная оценка актуальности угрозы атаки может быть формализована следующим образом*: $P_{0a} = 1 - \prod_{r=1}^{R}(1 - P_{0yr})$ *

	$$P_{0\text{узис}} = 1 - \left(1 - P_{0\text{у}}\right)(1 - P_{0\text{сзи}}),$$ $$P_{0\text{азис}} = 1 - (1 - P_{0\text{сзи}}) \prod_{r=1}^{R} (1 - P_{0\text{у}r})$$
27	*Вероятность того, что защищенная в отношении уязвимости информационная система будет готова к безопасной эксплуатации, может быть определена следующим образом* $$P_{0\text{узис}} = 1 - \left(1 - P_{0\text{у}}\right)(1 - P_{0\text{сзи}})*$$ $$P_{0\text{а}} = 1 - \prod_{r=1}^{R} (1 - P_{0\text{у}r})$$ $$P_{0\text{азис}} = 1 - (1 - P_{0\text{сзи}}) \prod_{r=1}^{R} (1 - P_{0\text{у}r})$$
28	*Вероятность угрозы атаки, возникающую за время эксплуатации t информационной системы, может быть определена следующим образом* $$\boldsymbol{P}_{\text{у}\boldsymbol{aI}} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{I}} \boldsymbol{K}_{\text{г}} (\mathbf{1} - \boldsymbol{K}_{\text{г}})^{\boldsymbol{i-1}}*$$ $$P_{0\text{а}} = 1 - \prod_{r=1}^{R} (1 - P_{0\text{у}r})$$ $$P_{0\text{азис}} = 1 - (1 - P_{0\text{сзи}}) \prod_{r=1}^{R} (1 - P_{0\text{у}r})$$
ПК-5 - способностью проводить анализ рисков информационной безопасности автоматизированной системы	
1	*Программный комплекс «Кондор» позволяет …* **А. автоматически сформировать перечень рекомендаций по минимизации значения риска за счет выполнения тех требований, которым не удовлетворяет АС.** Б. вычислить значение риска информационной безопасности на основе алгоритма, интегрированного в комплекс. При этом параметры алгоритма запрограммированы в комплексе и не могут изменяться оператором. Г. вычислять оценки рисков информационной безопасности на основе содержимого таблицы, заполняемой оператором
2	*Программный комплекс «Гриф» позволяет …* А. автоматически сформировать перечень рекомендаций по минимизации значения риска за счет выполнения тех требований, которым не удовлетворяет АС. **Б. вычислить значение риска информационной безопасности на основе алгоритма, интегрированного в комплекс. При этом параметры алгоритма запрограммированы в комплексе и не могут изменяться оператором.** В. вычислять оценки рисков информационной безопасности на основе содержимого таблицы, заполняемой оператором.
3	*Программный комплекс «Risk Matrix» позволяет …* А. автоматически сформировать перечень рекомендаций по минимизации значения риска за счет выполнения тех требований, которым не удовлетворяет АС. Б. вычислить значение риска информационной безопасности на основе алгоритма, интегрированного в комплекс. При этом параметры алгоритма запрограммированы в комплексе и не могут изменяться оператором. **В. вычислять оценки рисков информационной безопасности на основе содержимого таблицы, заполняемой оператором**
4	*Преимуществом модели, заложенной в основу методики «OCTAVE», является* **А. возможность использования сценариев атак, имеющих текстовое или Б. графическое представление, а также возможность применения качественных шкал для оценки уровня риска**

	В. простота ее использования и возможность табличного представления модели оценки рисков
5	*К недостаткам модели, заложенной в основу методики «OCTAVE», является* **А. неформализуемость, невозможность учета вероятности проведения атаки при оценки риска, а также отсутствие возможности описания сложных сценариев проведения атак** Б. не предусматривает возможность оценки рисков безопасности для сложных сценариев атак
6	*К недостаткам модели комплекса «Гриф» относятся (несколько вариантов):* **А. отсутствие возможности настройки параметров атак, что не позволяет использовать ее для оценки риска сценариев атак, состоящих из нескольких этапов.** **Б. высокая сложность настойки параметров модели.** В. неформализуемость, невозможность учета вероятности проведения атаки при оценки риска, а также отсутствие возможности описания сложных сценариев проведения атак Г. не предусматривает возможность оценки рисков безопасности для сложных сценариев атак
7	***Укажите верную последовательность этапов разработки м****одели оценки рисков, базирующаяся на основе графовой модели атак* А) формирование множества, элементами которого являются защищаемые информационные ресурсы АС; Б) формирование множества, элементами которого является программное и аппаратное обеспечение, используемое для обработки, хранения или передачи защищаемых информационных ресурсов АС; В) определение информационных потоков доступа пользователей АС к защищаемым ресурсам АС; Г) формирование множества, элементами которого являются средства защиты АС; Д) оценка возможного ущерба в случае нарушения конфиденциальности, целостности или доступности защищаемых ресурсов; Е) оценка вероятности проведения атак на защищаемые информационные ресурсы; Ж) расчет значения рисков информационной безопасности. **А-В-Г-Д-Е-Ж-З** **А-Б-В-Г-Д-Е-Ж** **Б-А-Ж-В-Г-Д-Е**
8	*Этап формирования множества защищаемых информационных ресурсов АС в рамках разработки м****одели оценки рисков, базирующаяся на основе графовой модели атак характеризуется тем, что…*** **А. определяется множество информационных ресурсов АС — D, которые должны защищаться от возможных атак нарушителей (файловые ресурсы; служебные данные, хранящиеся в СУБД; пользовательские документы и др.)** Б. формируются два множества: S — множество ПО и H — множество аппаратного обеспечения, которое используется в АС для хранения и обработки информационных ресурсов, входящих в множество D. В. определяется множество категорий пользователей АС — U, а также права доступа этих пользователей к информационным ресурсам множества D. Г. определяется множество средств защиты Z, которые используются в АС. В множество Z включаются как организационные, так и технические средства

	защиты. Д. определяется вероятность того, что в случае проведения атак на защищаемые ресурсы могут быть успешно преодолены все средства защиты, используемые в АС. Е. вычисляется значение риска R на основе ранее определенного уровня ущерба и вероятности атак
9	*Этап определения информационных потоков доступа в рамках разработки **м**одели оценки рисков, базирующаяся на основе графовой модели атак характеризуется тем, что…* А. определяется множество информационных ресурсов АС — D, которые должны защищаться от возможных атак нарушителей (файловые ресурсы; служебные данные, хранящиеся в СУБД; пользовательские документы и др.) **Б. формируются два множества: S — множество ПО и H — множество аппаратного обеспечения, которое используется в АС для хранения и обработки информационных ресурсов, входящих в множество D.** В. определяется множество категорий пользователей АС — U, а также права доступа этих пользователей к информационным ресурсам множества D. определяется множество средств защиты Z, которые используются в АС. В множество Z включаются как организационные, так и технические средства защиты. Г. определяется вероятность того, что в случае проведения атак на защищаемые ресурсы могут быть успешно преодолены все средства защиты, используемые в АС. Д. вычисляется значение риска R на основе ранее определенного уровня ущерба и вероятности атак
10	*Этап формирования множества средств защиты АС в рамках разработки **м**одели оценки рисков, базирующаяся на основе графовой модели атак характеризуется тем, что…* А. определяется множество информационных ресурсов АС — D, которые должны защищаться от возможных атак нарушителей (файловые ресурсы; служебные данные, хранящиеся в СУБД; пользовательские документы и др.) Б. формируются два множества: S — множество ПО и H — множество аппаратного обеспечения, которое используется в АС для хранения и обработки информационных ресурсов, входящих в множество D. **В. определяется множество категорий пользователей АС — U, а также права доступа этих пользователей к информационным ресурсам множества D.** Г. определяется множество средств защиты Z, которые используются в АС. В множество Z включаются как организационные, так и технические средства защиты. Д. определяется вероятность того, что в случае проведения атак на защищаемые ресурсы могут быть успешно преодолены все средства защиты, используемые в АС. Е. вычисляется значение риска R на основе ранее определенного уровня ущерба и вероятности атак.
ПК-6 - способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	
1	*Инструмент Nmap в Kali Linux предназначен для* **А. сбора информации** Б. аудита безопасности, тестирования соответствия и защиты системы В. аудита безопасности WordPress Г. оценки безопасности сети WiFi

	Д. взлома пар логин / пароль Е. сетевой анализатор Ж. тестирования на проникновение
2	*Инструмент Линис в Kali Linux предназначен для* А. сбора информации **Б. аудита безопасности, тестирования соответствия и защиты системы** В. аудита безопасности WordPress Г. оценки безопасности сети WiFi Д. взлома пар логин / пароль Е. сетевой анализатор Ж. тестирования на проникновение
3	*Инструмент WPScan в Kali Linux предназначен для* А. сбора информации Б. аудита безопасности, тестирования соответствия и защиты системы **В. аудита безопасности WordPress** Г. оценки безопасности сети WiFi Д. взлома пар логин / пароль Е. сетевой анализатор Ж. тестирования на проникновение
4	*Инструмент Aircrack-ng в Kali Linux предназначен для* А. сбора информации Б. аудита безопасности, тестирования соответствия и защиты системы В. аудита безопасности WordPress **Г. оценки безопасности сети WiFi** Д. взлома пар логин / пароль В. сетевой анализатор Г. тестирования на проникновение
5	*Инструмент Гидра в Kali Linux предназначен для* А. сбора информации Б. аудита безопасности, тестирования соответствия и защиты системы В. аудита безопасности WordPress Г. оценки безопасности сети WiFi **Д. взлома пар логин / пароль** Е. сетевой анализатор Ж. тестирования на проникновение
6	*Инструмент Whireshark в Kali Linux предназначен для* А. сбора информации Б. аудита безопасности, тестирования соответствия и защиты системы В. аудита безопасности WordPress Г. оценки безопасности сети WiFi Д. взлома пар логин / пароль **Е. сетевой анализатор** Ж. тестирования на проникновение
7	*Инструмент Metasploit Framework в Kali Linux предназначен для* А. сбора информации Б. аудита безопасности, тестирования соответствия и защиты системы В. аудита безопасности WordPress Г. оценки безопасности сети WiFi Д. взлома пар логин / пароль Е. сетевой анализатор **Ж. тестирования на проникновение**
8	*Инструмент Skipfish в Kali Linux предназначен для*

	А. сбора информации Б. аудита безопасности, тестирования соответствия и защиты системы В. аудита безопасности WordPress Г. оценки безопасности сети WiFi Д. взлома пар логин / пароль Е. сетевой анализатор **Ж. сканер веб-приложений**
9	*Инструмент Мальтего в Kali Linux предназначен для* А. сбора информации Б. аудита безопасности, тестирования соответствия и защиты системы В. аудита безопасности WordPress Г. оценки безопасности сети WiFi Д. взлома пар логин / пароль Е. сетевой анализатор **Ж инструмент для анализа данных**
10	*Инструмент Несс в Kali Linux предназначен для* А. сбора информации Б. аудита безопасности, тестирования соответствия и защиты системы В. аудита безопасности WordPress Г. оценки безопасности сети WiFi Д. взлома пар логин / пароль Е. сетевой анализатор **Ж. поиск уязвимостей**

7.2.3. Примерный перечень вопросов для подготовки к зачету

Понятие «атака» и «операция» в информационном аспекте. Классификация атак. Этапы реализации атак: сбор информации, основные механизмы реализации атак, реализация атак, завершение атаки. Принципы построения СОВ. Классификация и архитектура.

Существующие технологии СОВ. Повышение эффективности систем. Характеристика направлений и групп методов обнаружения вторжений. Сравнительный анализ существующих СОВ.

Табличные и диаграммные модели

информационных атак

Формализованные модели

информационных атак

Анализ существующих моделей процесса обнаружения информационных атак Сигнатурные модели процесса обнаружения атак

Поведенческие модели процесса

выявления атак Модели процесса оценки рисков информационной безопасности АС Модель, заложенная в основу программного комплекса оценки рисков

«Кондор» Модель, заложенная в основу программного комплекса оценки рисков «Гриф»

Модель, заложенная в основу

программного комплекса оценки рисков «RiskMatrix»

Модель, заложенная в основу методики оценки рисков «OCTAVE»

7.2.4.Примерный перечень заданий для решения прикладных задач

Понятие «атака» и «операция» в информационном аспекте.

Классификация атак. Этапы реализации атак: сбор информации, основные механизмы реализации атак, реализация атак, завершение атаки. Принципы построения СОВ. Классификация и архитектура.

Существующие технологии СОВ. Повышение эффективности систем. Характеристика направлений и групп методов обнаружения вторжений. Сравнительный анализ существующих СОВ.

Табличные и диаграммные модели

информационных атак

Формализованные модели

информационных атак

Анализ существующих моделей процесса обнаружения информационных атак Сигнатурные модели процесса обнаружения атак

Поведенческие модели процесса

выявления атак Модели процесса оценки рисков информационной безопасности АС Модель, заложенная в основу программного комплекса оценки рисков

«Кондор» Модель, заложенная в основу программного комплекса оценки рисков «Гриф»

Модель, заложенная в основу

программного комплекса оценки рисков «RiskMatrix»

Модель, заложенная в основу методики оценки рисков «OCTAVE».

Математическая модель информационных атак на ресурсы автоматизированных систем. Формальное описание модели информационных атак Особенности использования разработанной математической модели информационных атак Математическая модель процесса обнаружения информационных атак Математическая модель процесса оценки рисков информационной безопасности автоматизированных систем. Описание модели процесса оценки рисков информационной безопасности. Особенности использования модели оценки рисков безопасности. Методика разработки рекомендаций по повышению уровня защиты автоматизированных систем на основе модели оценки рисков безопасности.

Выбор разработанного прототипа системы обнаружения атак, построенного на основе поведенческой модели.

Объект и цель испытаний

Функциональные требования к прототипу системы обнаружения атак. Технические и программные средства проведения

испытаний Порядок проведения испытаний Результаты проведѐнных испытаний Описание системы обнаружения атак, предназначенной для промышленной реализации Хостовые датчики системы обнаружения атак. Сетевые датчики системы обнаружения атак Агенты системы обнаружения атак Модуль реагирования системы обнаружения атак. Информационный фонд системы обнаружения атак.

Консоль администратора системы обнаружения атак Модуль координации потоков информации системы обнаружения атак.

Анализ террористической деятельности. Сценарные модели наиболее

масштабных террористических операций в информационном аспекте. Вероятностные и энтропийные модели террористических атак. Вероятностные модели информационно-психологических последствий террористических актов

7.2.5. Методика выставления оценки при проведении промежуточной аттестации

(Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.6 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основные определения и понятия	ПК-2; ПК-5; ПК-6	Тест, защита лабораторных работ, требования к курсовому проекту
2	Технологии построения СОВ	ПК-2; ПК-5; ПК-6	Тест, защита лабораторных работ, требования к курсовому проекту
3	Анализ существующих моделей защиты автоматизированных систем от информационных атак	ПК-2; ПК-5; ПК-6	Тест, защита лабораторных работ, требования к курсовому проекту
4	Разработка математических моделей защиты автоматизированных систем от информационных атак	ПК-2; ПК-5; ПК-6	Тест, защита лабораторных работ, требования к курсовому проекту
5	Формирование математической модели процесса выявления информационных атак	ПК-2; ПК-5; ПК-6	Тест, защита лабораторных работ, требования к курсовому

			проекту
6	Моделирование террористических атак и операций в информационном аспекте	ПК-2; ПК-5; ПК-6	Тест, защита лабораторных работ, требования к курсовому проекту

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 курсовой работы, курсового проекта или отчета по всем видам практик 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.Остапенко А.Г. Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обеспечением [Электронный ресурс] : Учеб.пособие. - Электрон.текстовые, граф. дан. (112 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.

Дополнительная литература

1.Методические указания к самостоятельным работам по дисциплинам «Математические модели информационного противоборства», «Математическое моделирование информационных операций и атак» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост.: О. Н. Чопоров, Е. А. Шварцкопф. - Электрон.текстовые, граф. дан. (262

Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

2.Макоха А.Н. Основы вычислительной математики, математического и информационного моделирования [Электронный ресурс]: лабораторный практикум/ Макоха А.Н., Дерябин М.А.— Электрон.текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2018.— 196 с.— Режим доступа: http://www.iprbookshop.ru/83228.html.— ЭБС «IPRbooks».

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:

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой. Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

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

По дисциплине «Математическое моделирование информационных операций и атак» читаются лекции, проводятся лабораторные работы, выполняется курсовой проект.

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

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

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.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
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, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.