АНО ВО «Межрегиональный открытый социальный институт»

УТВЕРЖДАЮ
Зав. кафедрой информационной
безопасности _____П.В. Никитин
Протокол заседания кафедры
№ 2 «20» марта 2017 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине	Б1.В.ДВ.1.1 Методы и средства защиты информации (наименование)
направление подготовки программы аспирантуры	10.06.01 Информационная безопасность
направленность подготовки программы аспирантуры (профиль)	Методы и системы защиты информации, информационная безопасность
квалификация (степень) выпускника	Исследователь. Преподаватель-исследователь
форма обучения	Очная / заочная

ПРОГРАММА РАЗРАБОТАНА

д-р техн. наук, проф.
А. В. Горохов
(должность, Ф. И. О., ученая степень, звание автора(ов) программы)

Йошкар-Ола, 2017

Содержание

1. Пояснительная записка

Цель изучения дисциплины: в соответствии с общими целями основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура) (далее - образовательная программа послевузовского профессионального образования) являются:

- усвоение аспирантами знаний об основных результатах в изучаемой области;
- формирование математической культуры аспиранта, фундаментальная подготовка в области математических методов защиты информации;
- овладение основными понятиями и методами, используемыми в криптографической защите информации для дальнейшего использования при решении теоретических и прикладных задач

Место дисциплины в учебном плане:

Дисциплина «Методы и средства защиты информации» относится к факультативам, программы подготовки научно-педагогических кадров в аспирантуре по направлению подготовки кадров высшей квалификации 10.06.01 Информационная безопасность.

Дисциплина «Методы и средства защиты информации» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Перечень планируемых результатов обучения по дисциплине
ПК-1	способность разрабатывать новые и исследовать существующие методы защиты информации при ее передаче и хранении	Знать: -программные средства в области защиты информации; -программные средства исследования эффективности системы защиты информации; - алгоритмы и математические модели объектов и процессов в устройствах и системах защиты информации. Уметь: - моделировать алгоритмы цифровой обработки сигналов систем связи; -исследовать эффективность системы защиты информации инфокоммуникационной системы; - проверять адекватность алгоритмов и математических моделей объектов и процессов в устройствах и системах защиты информации Владеть: - способностью компьютерного моделирования систем защиты информации; - методами анализа антивирусных программ; - методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений.
ПК-2	способность применять современные методы моделирования угроз информационной безопасности для решения профессиональных задач	Знать: - современные направления построения систем защиты информации в системах связи; - принципы построения систем связи в соответствии с требованиями по защите информации; - методы оценки эффективности систем защиты информации Уметь: - выбирать механизмы информационной безопасности и защиты информации в системах связи; - выбрать технологии и средства защиты информации в системах связи; - применять критерии оценки эффективности защиты информации.

		Владеть: - способностью выбирать направления построения систем защиты информации; - методами и средствами защиты систем и сетей связи; - способностью определения степени эффективности применяемых средств защиты информации.
ПК-3	способность оценивать эффективность применяемых средств защиты информации	Знать: - предметную область научных исследований; - историю развития исследуемой научной проблемы, становления её разработки, степень сложности; - роль и место научной проблемы в данной области науки. Уметь: - правильно формулировать задачи исследования в ходе выполнения научно- исследовательской работы в соответствии с её целью; - выбирать методы и методики исследования и обосновывать целесообразность и соответствие их применения целям исследований; - составлять план исследований и корректировать его в ходе выполнения. Владеть: - современной проблематикой и терминологией в данной отрасли знания; - навыками самостоятельного планирования и проведения научного исследования; -способностью разработки новых и модернизации известных технических решений в рамках выбранного направления исследований.

Этапы формирования компетенций

Код компетенции	Формулировка компетенции	Очная / заочная форма обучения	
		Учебная дисциплина	Курс
ПК-1	способность разрабатывать новые и исследовать существующие методы защиты информации при ее передаче и хранении	Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук	1-4
		Методы и системы защиты информации, информационная безопасность	2
		Методы и средства защиты информации	2
		Информационная безопасность инфокоммуникационных системы	2
		Представление научного доклада об основных результатах подготовленной научно-	3

		квалификационной работы (диссертации) Подготовка к сдаче и сдача государственного экзамена	 4
ПК-2	способность применять современные методы моделирования угроз информационной безопасности для решения профессиональных задач	Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Методы и системы защиты информации, информационная безопасность Методы и средства защиты информации Информационная безопасность инфокоммуникационных системы Подготовка к сдаче и сдача государственного экзамена	1-4 2 2 2 4
ПК-3	способность оценивать эффективность применяемых средств защиты информации	Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Методы и системы защиты информации, информационная безопасность Методы и средства защиты информации Информационная безопасность инфокоммуникационных системы Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации) Подготовка к сдаче и сдача государственного экзамена	1-4 2 2 2 3 4

Этапы формирования компетенций: в качестве этапов формирования компетенций в процессе освоения образовательной программы указываются курсы.

Формы текущего контроля успеваемости аспирантов: устный опрос, практические задания

Форма промежуточной аттестации: зачет.

2. Структура и содержания дисциплины

Трудоемкость 3 зачетные единицы, 108 часов, из них:

36 лекционных, 36 практических и 36 часов самостоятельной работы;

2.1. Тематический план учебной дисциплины

№ п/п	Наименование	Количество часов по

	разделов и тем	учебному плану				
		Всего	Виды учебной работы			
			Аудиторная работа			Самостоятельная работа
			Лекции	Практические (семинарские) занятия	Лабораторные занятия	
1	2	3	4	5	6	7
1	Тема 1. Объекты информационной защиты		6	6		6
2	Тема 2. Угрозы безопасности информации		8	8		8
3	Тема 3. Классификация видов, методов и средств защиты информации		6	6		6
4	Тема 4. Организация защиты информации		8	8		8
5	Тема 5. Технический аудит безопасности телекоммуникационных систем		8	8		8
	Итого по дисциплине	**108**	**36**	**36**	**-**	**36**

2.2. Тематический план лекционных занятий:

№ п/п раздела	Наименование разделов и тем	Количество часов
1	2	3
1	Тема 1. Объекты информационной защиты	6
2	Тема 2. Угрозы безопасности информации	8
3	Тема 3. Классификация видов, методов и средств защиты информации	6
4	Тема 4. Организация защиты информации	8
5	Тема 5. Технический аудит безопасности телекоммуникационных систем	8
	Итого по дисциплине	**36**

Содержание лекционных занятий

Тема 1. Объекты информационной защиты

1. Понятие объекта защиты.
2. Носители информации как конечные объекты защиты.
3. Особенности отдельных видов носителей как объектов защиты
4. Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации
5. Демаскирующие признаки объектов защиты

Тема 2. Угрозы безопасности информации

1. Понятие уязвимости информации.
2. Формы проявления уязвимости информации.
3. Виды уязвимости информации.
4. Понятие “утечка информации”.
5. Соотношение форм и видов уязвимости информации
6. Понятие угрозы защищаемой информации.

7. Связь угрозы защищаемой информации с уязвимостью информации.
8. Признаки и составляющие угрозы: явления, факторы, условия.
9. Понятие угрозы защищаемой информации

Тема 3. Классификация видов, методов и средств защиты информации

1. Виды защиты информации, сферы их действия
2. Понятие и классификация средств защиты информации.
3. Назначение программных, криптографических и технических средств защиты

Тема 4. Организация защиты информации

1. Подсистема обеспечения информационной безопасности ТКС.
2. Основное назначение.
3. Решаемые задачи

Раздел 5. Технический аудит безопасности телекоммуникационных систем

1. Методы технического аудита информационной безопасности ТКС
2. Средства технического аудита информационной безопасности ТКС

2.3. Тематический план практических (семинарских) занятий:

№ п/п раздела	Наименование разделов и тем	Количество часов
1	2	3
1	Тема 1. Объекты информационной защиты	6
2	Тема 2. Угрозы безопасности информации	8
3	Тема 3. Классификация видов, методов и средств защиты информации	6
4	Тема 4. Организация защиты информации	8
5	Тема 5. Технический аудит безопасности телекоммуникационных систем	8
	Итого по дисциплине	**36**

Содержание практических занятий

Тема 1. Объекты информационной защиты

Классификация защищаемых объектов информатизации

Выявление состава, подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации

Определение демаскирующих признаков объекта защиты

Тема 2. Угрозы безопасности информации

Изучение нормативно - правовых документов в области информационной безопасности

Признаки и составляющие угрозы: явления, факторы, условия

Тема 3. Классификация видов, методов и средств защиты информации

Исследование и выбор антивирусных программ

Классификация видов, методов и средств защиты информации

Тема 4. Организация защиты информации

Межсетевые экраны

Изучение процессов формирования и проверки ЭЦП

Тема 5. Технический аудит безопасности телекоммуникационных систем

Сетевые сканеры безопасности

Радиотехнический контроль, обнаружение и подавление сигналов от нелегальных радиопередатчиков.

Изучение функциональных возможностей универсального прибора для обнаружения закладных устройств скрытого съема информации СРМ –700

Литература

1. Бурькова, Е.В. Физическая защита объектов информатизации : учебное пособие / Е.В. Бурькова; Министерство образования и науки Российской Федерации, Оренбургский государственный университет, Кафедра вычислительной техники и защиты информации. - Оренбург: Оренбургский государственный университет, 2017. - 158 с.: табл., схем. - Библиогр. в кн. - ISBN 978-5-7410-1697-8; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=481730

2. Петренко, В.И. Защита персональных данных в информационных системах: учебное пособие / В.И. Петренко; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь: СКФУ, 2016. - 201 с. : схем.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=459205

3. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

4. Нестандартные методы защиты информации: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. В.П. Пашинцев, А.В. Ляхов. - Ставрополь : СКФУ, 2016. - 196 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458132

5. Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва: Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356

6. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва: Издательский дом Государственного университета Высшей школы экономики, 2015. - 574 с.: ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285

7. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429070

8. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. М.А. Лапина, Д.М. Марков и др. - Ставрополь : СКФУ, 2016. - 242 с. ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012

9. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 105 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895

10.Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. : ил.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428820

Интернет-ресурсы

1. Сайт журнала «Хакер» [Электронный ресурс] URL: http://xakep.ru/
2. Защита информации, управление информационной безопасностью и рисками – ISO27000.ru - [Электронный ресурс] URL: http://www.iso27000.ru/
3. Официальный сайт компании «КонсультантПлюс» [Электронный ресурс] URL: http://www.consultant.ru/
4. ФСТЭК России. Федеральная служба по техническому и экспортному контролю. Официальный сайт [Электронный ресурс] URL: http://fstec.ru/
5. ФСБ Российской Федерации. Официальный сайт [Электронный ресурс] URL: http://www.fsb.ru/
6. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] URL: http://rkn.gov.ru/
7. Защита от хакеров беспроводных сетей: пер. с англ. / К. Барнс, Т. Боутс, Д. Лойд и др. ; пер. А.В. Семенов. - М.: ДМК Пресс, б.г. - 478 с.: ил. - (Информационная безопасность). - ISBN 5-98453-012-0; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=85095

2.3. Тематический план для самостоятельной работы

№ п/п раздела	Наименование разделов и тем	Количество часов
1	2	3
1	Тема 1. Объекты информационной защиты	6
2	Тема 2. Угрозы безопасности информации	8
3	Тема 3. Классификация видов, методов и средств защиты информации	6
4	Тема 4. Организация защиты информации	8
5	Тема 5. Технический аудит безопасности телекоммуникационных систем	8
	Итого по дисциплине	**36**

Вопросы для самостоятельной работы

1. Система защиты персональных данных включает в себя?
2. Сколько лет составляет максимальный срок засекречивания сведений, составляющих государственную тайну?
3. Завершите фразу правильно: "Защита информации включает в себя..."
4. Выберите правильное завершение фразы: "В соответствии с общей классификацией защищаемые объекты информатизации подразделяются на..."
5. Принцип действия каких приборов основан на интегральном методе измерения уровня электромагнитного поля в точке их размещения и на этой основе – в определении точки абсолютного уровня излучения в помещении?
6. Какие показатели необходимо учитывать, при включении угроз безопасности в модель угроз безопасности информации, необходимую для выбора мер по защите информации не содержащей государственную тайну в государственных информационных системах?
7. К какому уровню представления нормативно -правовой базы государственной системы информационной безопасности относится Закон Российской Федерации "О персональных данных"?

8. Выберите, что из перечисленного относится к основным техническим средствам и системам (ОТСС).

9. К какому уровню представления нормативно -правовой базы государственной системы информационной безопасности относится Постановление Правительства Российской Федерации "О сертификации средств защиты информации"?

10. Для решения задач обеспечения безопасности на первом этапе необходимо?

11. Завершите фразу правильно: "Доступность – это..."

12. Что из перечисленного является важнейшим элементом дискреционной модели разграничения доступа?

13. Сколько классов защищенности СВТ от НСД к информации установлено нормативными документами?

14. В информационной системе реализуется мандатная модель контроля доступа. Определены три уровня меток секретности. Наивысший уровень 1 - й. Какие действия будут разрешены субъекту с 1-й степенью допуска?

15. В информационной системе реализуется мандатная модель контроля доступа. Определены три уровня меток секретности. Наивысший уровень 1 - й. Какие действия будут разрешены субъекту с 3-й степенью допуска?

16. Какие множества должны быть определены для мандатной модели контроля доступа?

17. Какая из перечисленных характеристик используется для оценки риска информационной безопасности?

18. К какому уровню представления нормативно -правовой базы государственной системы информационной безопасности относится Постановление Правительства Российской Федерации "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации о государственной тайне"?

19. Какие элементы необходимы для описания угрозы информационной безопасности?

20. Возможна ли реализация угрозы через несколько уязвимостей?

21. Продолжите фразу правильно "Принято выделять следующие источники угроз:..

22. Укажите правильные варианты продолжения фразы: "Инженерно - технические методы снижают отрицательное воздействие угроз безопасности через устранение (уменьшение)..."

23. Приведите пример реализации подсистемы защиты WEB -приложений.

24. Какие из перечисленных уязвимостей устраняются организационными и программно - аппаратными методами парирования угроз?

Литература

1. Бурькова, Е.В. Физическая защита объектов информатизации : учебное пособие / Е.В. Бурькова; Министерство образования и науки Российской Федерации, Оренбургский государственный университет, Кафедра вычислительной техники и защиты информации. - Оренбург: Оренбургский государственный университет, 2017. - 158 с.: табл., схем. - Библиогр. в кн. - ISBN 978-5-7410-1697-8; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=481730

2. Петренко, В.И. Защита персональных данных в информационных системах: учебное пособие / В.И. Петренко; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь: СКФУ, 2016. - 201 с. : схем.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=459205

3. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

4. Нестандартные методы защиты информации: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. В.П. Пашинцев, А.В. Ляхов. - Ставрополь : СКФУ, 2016. -

196 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458132

5. Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва: Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356

6. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва: Издательский дом Государственного университета Высшей школы экономики, 2015. - 574 с.: ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285

7. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429070

8. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. М.А. Лапина, Д.М. Марков и др. - Ставрополь : СКФУ, 2016. - 242 с. ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012

9. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 105 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895

10.Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. : ил.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428820

Интернет-ресурсы

1. Сайт журнала «Хакер» [Электронный ресурс] URL: http://xakep.ru/

2. Защита информации, управление информационной безопасностью и рисками – ISO27000.ru - [Электронный ресурс] URL: http://www.iso27000.ru/

3. Официальный сайт компании «КонсультантПлюс» [Электронный ресурс] URL: http://www.consultant.ru/

4. ФСТЭК России. Федеральная служба по техническому и экспортному контролю. Официальный сайт [Электронный ресурс] URL: http://fstec.ru/

5. ФСБ Российской Федерации. Официальный сайт [Электронный ресурс] URL: http://www.fsb.ru/

6. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] URL: http://rkn.gov.ru/

7. Защита от хакеров беспроводных сетей: пер. с англ. / К. Барнс, Т. Боутс, Д. Лойд и др. ; пер. А.В. Семенов. - М.: ДМК Пресс, б.г. - 478 с.: ил. - (Информационная безопасность). - ISBN 5-98453-012-0; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=85095

3. Оценочные средств и методические рекомендации по проведению промежуточной аттестации

При проведении зачета по дисциплине «Методы и средства защиты информации» может использоваться устная или письменная форма проведения.

Примерная структура зачета по дисциплине «Методы и средства защиты информации»

1. устный ответ на вопросы

Аспиранту на зачете дается время на подготовку вопросов теоретического характера

2. выполнение практических заданий

Практических задания выполняются в течение 30 минут. Бланки с задачами готовит и выдает преподаватель.

Устный ответ аспиранта на зачете должен отвечать следующим требованиям:

- научность, знание и умение пользоваться понятийным аппаратом;
- изложение вопросов в методологическом аспектах, аргументация основных положений ответа примерами из современной практики, а также из личного опыта работы;
- осведомленность в важнейших современных проблемах современной науки.

Выполнение практического задания должно отвечать следующим требованиям:

- Владение профессиональной терминологией;
- Последовательное и аргументированное изложение решения.

Критерии оценивания ответов

	Устный ответ	**Практическое задание**
зачтено	знание учебного материала в пределах программы; логическое, последовательное изложение вопроса; определение своей позиции в раскрытии различных подходов к рассматриваемой проблеме;	свободное владение профессиональной терминологией; умение высказывать и обосновать свои суждения; аспирант дает четкий, полный анализ ситуации.
не зачтено	пробелы в знаниях основного учебно-программного материала, принципиальные ошибки в изложении материала	допущены ошибки в определении понятий, искажен их смысл; аспирант не может применять знания для решения практического задания.

Критерии и шкала оценивания уровней освоения компетенций

Шкала оценивания	Шкала оценивания	Шкала оценивания
отлично	высокий	аспирант, овладел элементами компетенции «знать», «уметь» и «владеть», проявил всесторонние и глубокие знания программного материала по дисциплине, освоил основную и дополнительную литературу, обнаружил творческие способности в понимании, изложении и практическом использовании усвоенных знаний.
хорошо	продвинутый	аспирант овладел элементами компетенции «знать» и «уметь», проявил полное знание программного материала по дисциплине, освоил основную рекомендованную литературу, обнаружил стабильный характер знаний и умений и проявил способности к их самостоятельному применению и обновлению в ходе последующего обучения и практической деятельности.
удовлетворительно	базовый	аспирант овладел элементами компетенции «знать», проявил знания основного программного материала по дисциплине в объеме, необходимом для последующего обучения и предстоящей практической деятельности, изучил основную рекомендованную литературу, допустил неточности в ответе на экзамене, но в основном обладает необходимыми знаниями для их устранения при

		корректировке со стороны экзаменатора.
неудовлетворительно	компетенции не сформированы	аспирант не овладел ни одним из элементов компетенции, обнаружил существенные пробелы в знании основного программного материала по дисциплине, допустил принципиальные ошибки при применении теоретических знаний, которые не позволяют ему продолжить обучение или приступить к практической деятельности без дополнительной подготовки по данной дисциплине.

Оценка «зачтено» соответствует критериям оценок от «отлично» до «удовлетворительно».

Оценка «не зачтено» соответствует критерию оценки «неудовлетворительно»

Итоговая отметка за зачет по предмету выставляется с учетом полученных отметок в соответствии с правилами математического округления.

Рекомендации по проведению зачета

1. Аспиранты должны быть заранее ознакомлены с требованиями к зачету, критериями оценивания.

2. Необходимо выяснить на зачете, формально или нет владеет аспирант знаниями по данному предмету. Вопросы при ответе по билету помогут выяснить степень понимания студентом материала, знание им связей излагаемого вопроса с другими изучавшими им понятиями, а практические задания – умения применять знания на практике.

3. На зачете следует выяснить, как аспирант знает программный материал, как он им овладел к моменту зачета, как он продумал его в процессе обучения и подготовки к зачету.

4. При устном опросе целесообразно начинать с легких, простых вопросов, ответы на которые помогут подготовить аспиранта к спокойному размышлению над дальнейшими более трудными вопросами и практическими заданиями.

5. Выполнение практических заданий осуществляется в учебной аудитории. Результат каждого обучающегося оценивается в соответствии с оценочной шкалой, приведённой в пункте 3.

Перечень вопросов к зачету

1 Что такое Методы и средства защиты информации: информационная безопасность.

2 Актуальность проблемы информационной безопасности.

3 Понятия и определения в информационной безопасности.

4 Основные составляющие информационной безопасности

5 Анализ способов нарушений информационной безопасности.

6 Использование защищенных компьютерных систем.

7 Основные определения и критерии классификации угроз.

8 Основные закономерности возникновения и классификация угроз информационной безопасности.

9 Пути и каналы утечки информации и их обобщенная модель.

10 Классификация каналов утечки информации.

11 Угрозы доступности.

12 Угрозы целостности.

13 Угрозы конфиденциальности.

14 Методы сбора сведений для вторжения в сеть.

15 Обобщенная модель нарушителя безопасности информации.

16 Распределенные атаки на отказ от обслуживания.

17 Вирусы и механизмы их работы.

18 Классификации вирусов. Среда обитания. Способ заражения среды обитания. Деструктивная возможность.

Особенности алгоритма вируса.

19 Методы обнаружения и удаления вирусов.

20 Антивирусная стратегия. Антивирусная защита.

21 Основные функции современных антивирусов.

22 Типовая структура корпоративной сети.

23 Способы НСД к каналам передачи данных.

24 Основные пути обеспечения безопасности информации.

25 Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт.

26 Механизмы безопасности.
27 Операционная и технологическая гарантированность.
28 Классы безопасности
29 Руководящие документы Гостехкомиссии России.
30 Административный уровень информационной безопасности.
31 Политика безопасности.
32 Уровни политики безопасности.
33 Программа безопасности.
34 Управление рисками.
35 Подготовительные этапы управления рисками.
36 Основные этапы управления рисками.
37 Анализ угроз.
38 Основные классы мер процедурного уровня.
39 Физическое управление доступом.
40 Поддержание работоспособности информационной системы.
41 Основные понятия программно-технического уровня информационной безопасности.
42 Сервисы безопасности. Классификация.
43 Особенности современных информационных систем, существенные с точки зрения безопасности.
44 Архитектурная безопасность. Основные принципы.
45 Протоколирование и аудит событий информационной системы.
46 Активный аудит.
47 Шифрование.
48 Симметричный и асимметричный методы шифрования.
49 Контроль целостности информационных сообщений.
50 Цифровые сертификаты.
51 Типичные задачи обеспечения информационной безопасности сети. УП: ФиИ44.03.05-2017-1-2595.plm.xml стр. 6
52 Сканеры портов. Обзор. Возможности.
53 Применение сканеров портов.
54 Криптографические протоколы. Применение, характеристики.
55 Причины существования дыр в системе безопасности.
56 Сканеры уязвимостей. Возможности, ограничения.
57 Сетевые анализаторы. Выбор расположения.
58 Практическое применение сетевых анализаторов.
59 Системы обнаружения вторжений. Выбор расположения системы обнаружения.
60 Классификация firewall'ов и определение политики firewall'а.
61 Политика безопасности современных операционных систем.
62 Электронная цифровая подпись.

4.Учебно-методическое и информационное обеспечение

Литература

1. Бурькова, Е.В. Физическая защита объектов информатизации : учебное пособие / Е.В. Бурькова; Министерство образования и науки Российской Федерации, Оренбургский государственный университет, Кафедра вычислительной техники и защиты информации. - Оренбург: Оренбургский государственный университет, 2017. - 158 с.: табл., схем. - Библиогр. в кн. - ISBN 978-5-7410-1697-8; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=481730

2. Петренко, В.И. Защита персональных данных в информационных системах: учебное пособие / В.И. Петренко; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь: СКФУ, 2016. - 201 с. : схем.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=459205

3. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

4. Нестандартные методы защиты информации: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. В.П. Пашинцев, А.В. Ляхов. - Ставрополь : СКФУ, 2016. - 196 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458132

5. Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва: Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356

6. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва: Издательский дом Государственного университета Высшей школы экономики, 2015. - 574 с.: ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285

7. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429070

8. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. М.А. Лапина, Д.М. Марков и др. - Ставрополь : СКФУ, 2016. - 242 с. ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012

9. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 105 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895

10.Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. : ил.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428820

Интернет-ресурсы

1. Сайт журнала «Хакер» [Электронный ресурс] URL: http://xakep.ru/

2. Защита информации, управление информационной безопасностью и рисками – ISO27000.ru - [Электронный ресурс] URL: http://www.iso27000.ru/

3. Официальный сайт компании «КонсультантПлюс» [Электронный ресурс] URL: http://www.consultant.ru/

4. ФСТЭК России. Федеральная служба по техническому и экспортному контролю. Официальный сайт [Электронный ресурс] URL: http://fstec.ru/

5. ФСБ Российской Федерации. Официальный сайт [Электронный ресурс] URL: http://www.fsb.ru/

6. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] URL: http://rkn.gov.ru/

7. Защита от хакеров беспроводных сетей: пер. с англ. / К. Барнс, Т. Боутс, Д. Лойд и др. ; пер. А.В. Семенов. - М.: ДМК Пресс, б.г. - 478 с.: ил. - (Информационная безопасность). - ISBN 5-98453-012-0; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=85095

Перечень программного обеспечения и информационных справочных систем

«Консультант Плюс», «Гарант» (договор о сотрудничестве от 23.09.2013 г. с ЗАО «Компьютерные технологии» (ПС Гарант)), регистрационный лист зарегистрированного пользователя ЭПС «Система ГАРАНТ» от 16.02.2012 г. №12-40272-000944; договора с ООО «КонсультантПлюс Марий Эл» №2017-СВ-4 от 28.12.2016 г., Windows 10 Education (Средства для разработки и проектирования, доступные по подписке Microsoft Imagine Premium), Windows 7 Professional (Средства для разработки и проектирования, доступные по подписке Microsoft Imagine Premium), Office Standart 2007, 2010 (Microsoft Open License), Office Professional Plus 2016 (Microsoft Open License)

5.Материально-техническое обеспечение дисциплины

Материально-техническую базу для проведения лекционных и практических занятий по дисциплине составляют:

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**
Аудитория для проведения лекционных и практических занятий, индивидуальных и групповых консультаций, промежуточной аттестации (в соответствии с расписанием)	ноутбук, мультимедийный проектор, экран
Помещение для самостоятельной работы, каб. 408, 409	9 рабочих мест ПЭВМ; Операционная система Ubuntu; Программное обеспечение: Open Office; доступ к сети Internet.
Библиотека	15 рабочих мест ПЭВМ, (15 компьютеров Asus P7H57D-VEVO Intel Core i3 540@3066 МГц), с доступом к базам данных и сети Интернет, копировальная техника.
Лаборатория программно-аппаратных средств обеспечения информационной безопасности, каб. 310.	ST-CE010MF Считыватель настольный для ввода идентификаторов Mifare; Считыватель смарт-карт ACR1252U-M1 (5шт); Программно-аппаратный комплекс Соболь 3.0; - 5шт. Программа для ЭВМ Индентификатор Rutoken S – 10 шт. Сетевой адаптер WiFi TP-Link TL-WN823N USB 2.0 (10шт); Коммутатор D-LINK DES-1016C/A1A; -1 шт. Сетевой экран Zyxel USG 40W (USG40W-RU0101F) – 1шт. Контроллер SIGUR E900I; ББП-20 Pro Tantos Источник вторичного электропитания резервированный 12В 2А (макс 3.5А) под акб.12В/7А•ч. Защита от глубокого разряда АКБ, Защита от КЗ; Аккумулятор Delta DT 1207; Извещатель, ИО 102-6, магнито-контактный, врезной на металическую дверь; Дверной замок; Считыватель PROX 13 - Reader карт формата MIFARE Classic 1k, Classic 4k, UltraLight, DESFire, с возможностью чтения кода из защищённой области карты (mad 3.0) (2шт); ПО Sigur Модуль базовый до 50 идентификаторов; Комплект Ezviz для управления Умным домом в составе: Ezviz Центр управления Умным домом (A1); Пульт дистанционного управления (K2); Ezviz Датчик движения (T1); Ezviz Датчик открытия-закрытия (T6); Ezviz Беспроводная сирена T9; Ezviz Беспроводной датчик протечки.
Лаборатория технической защиты информации, каб. 310.	Персональные компьютеры – 12 шт. Аппаратура акустической и виброакустической защиты SEL SP-55.

	Генератор шума переносной "Штора-1". Аппаратура акустической и виброакустической защиты SEL SP-55. Виброакустический электромагнитный излучатель (универсальный) SEL SP-55/V. Виброакустический электромагнитный излучатель SEL SP-55/VG. Многофункциональный прибор STO 31 "Пиранья". Нелинейный локатор "Лорнет». Осциллограф цифровой (БИТ). Алмаз обнаружитель видеокамер (БИТ). Беспроводная камера JMK. Monster 16CH. Уничтожитель информации Стек-НС1в.
Лаборатория сетей и систем передачи информации, каб. 310.	Cisco Catalist 2960. Cisco Catalist 3560. Cisco 2811. Cisco 2800. Системный блок. Монитор. Проектор и экран. Стабилизатор напряжения. Кондиционер. USB-Serial Port. Программное обеспечение: Notepad++. Cisco Packet Tracer. Bitvise SSH Client 7.39 (remove only). CCleaner. FileZilla Client. FreeCommander XE. GIMP 2.8.22. Google Chrome. HS 10.0 Express. LibreOffice 5.4 Help Pack. LibreOffice 5.4.3.2. Mozilla Firefox. MS Office 2010. NetBeans IDE. Nmap 7.60. Npcap 0.93. Oracle VM VirtualBox. Paint 3D. PuTTY. Pythol 3.6.2 (64-bit). SQL Server Browser for SQL Server 2014. VMware vSphere Client 5.1. Wireshark 2.4.2. 7-zip. Adobe Acrobat Reader DC. Adobe Flash Player.

6.Методические указания для обучающихся по освоению дисциплины

Методические указания для подготовки к практическим (семинарским) занятиям

Начиная подготовку к семинарскому занятию, необходимо, прежде всего, обратить внимание на конспект лекций, разделы учебников и учебных пособий, которые способствуют общему представлению о месте и значении темы в изучаемом курсе. Затем следует поработать с дополнительной литературой, сделать записи по рекомендованным источникам. Подготовка к семинарскому занятию включает 2 этапа:

- 1й этап - организационный;
- 2й этап - закрепление и углубление теоретических знаний. На первом этапе студент планирует свою самостоятельную работу, которая включает:
- уяснение задания, выданного на самостоятельную работу:
- подбор рекомендованной литературы;
- составление плана работы, в котором определяются основные пункты предстоящей подготовки.

Составление плана дисциплинирует и повышает организованность в работе. Второй этап включает непосредственную подготовку студента к занятию. Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная её часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам. В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь. При необходимости следует обращаться за консультацией к преподавателю. Готовясь к консультации, необходимо хорошо продумать вопросы, которые требуют разъяснения.

В начале занятия студенты под руководством преподавателя более глубоко осмысливают теоретические положения по теме занятия, раскрывают и объясняют основные положения выступления.

Записи имеют первостепенное значение для самостоятельной работы обучающихся. Они помогают понять построение изучаемого материала, выделить основные положения и проследить их логику. Ведение записей способствует превращению чтения в активный процесс, мобилизует, наряду со зрительной, и моторную память, Следует помнить: у студента, систематически ведущего записи, создается свой индивидуальный фонд подсобных материалов для быстрого повторения прочитанного, для мобилизации накопленных знаний. Особенно важны и полезны записи тогда, когда в них находят отражение мысли, возникшие при самостоятельной работе. Важно развивать умение сопоставлять источники, продумывать изучаемый материал.

Большое значение имеет совершенствование навыков конспектирования. Преподаватель может рекомендовать студентам следующие основные формы записи план (простой и развернутый), выписки, тезисы. Результаты конспектирования могут быть представлены в различных формах.

План - это схема прочитанного материала, краткий (или подробный) перечень вопросов, отражающих структуру и последовательность материала. Подробно составленный план вполне заменяет конспект.

Конспект - это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов.

План-конспект - это развернутый детализированный план, в котором достаточно подробные записи приводятся по тем пунктам плана, которые нуждаются в пояснении.

Текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника.

Свободный конспект - это четко и кратко сформулированные (изложенные) основные положения в результате глубокого осмысливания материала. В нем могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом.

Тематический конспект составляется на основе изучения ряда источников и дает более или менее исчерпывающий ответ по какой-то схеме (вопросу).

Ввиду трудоемкости подготовки к семинару следует продумать алгоритм действий, еще раз внимательно прочитать записи лекций и уже готовый конспект по теме семинара, тщательно продумать свое устное выступление.

На семинаре каждый его участник должен быть готовым к выступлению по всем поставленным в плане вопросам, проявлять максимальную активность при их рассмотрении Выступление должно строиться свободно, убедительно и аргументировано Необходимо следить, чтобы выступление не сводилось к репродуктивному уровню (простому воспроизведению текста), не допускать и простое чтение конспекта. Необходимо, чтобы выступающий проявлял собственное отношение к тому, о чем он говорит, высказывал свое личное мнение, понимание, обосновывал его и мог сделать правильные выводы из сказанного.

Выступления других обучающихся необходимо внимательно и критически слушать, подмечать особенное в суждениях обучающихся, улавливать недостатки и ошибки. При этом обратить внимание на то, что еще не было сказано, или поддержать и развить интересную мысль, высказанную выступающим студентом. Изучение студентами фактического материала по теме практического занятия должно осуществляться заблаговременно. Под фактическим материалом следует понимать специальную литературу по теме занятия, систему нормативных правовых актов, а также арбитражную практику по рассматриваемым проблемам. Особое внимание следует обратить на дискуссионные теоретические вопросы в системе изучаемого вопроса: изучить различные точки зрения ведущих ученых, обозначить противоречия современного законодательства. Для систематизации основных положений по теме занятия рекомендуется составление конспектов.

Обратить внимание на:

- составление списка нормативных правовых актов и учебной и научной литературы по изучаемой теме;
- изучение и анализ выбранных источников;
- изучение и анализ арбитражной практики по данной теме, представленной в информационно-справочных правовых электронных системах и др.;
- выполнение предусмотренных программой заданий в соответствии с тематическим планом;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;

- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов и эссе по отдельным вопросам изучаемой темы;

Семинарские занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности обучающихся по изучаемой дисциплине.

Методические указания для обучающихся по освоению дисциплины дли самостоятельной работы

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных особенностей студентов и условий учебной деятельности.

При этом преподаватель назначает студентам варианты выполнения самостоятельной работы, осуществляет систематический контроль выполнения студентами графика самостоятельной работы, проводит анализ и дает оценку выполненной работы.

Самостоятельная работа обучающихся осуществляется в аудиторной и внеаудиторной формах.

Самостоятельная работа обучающихся в аудиторное время может включать:

- конспектирование (составление тезисов) лекций, выполнение контрольных работ;
- решение задач;
- работу со справочной и методической литературой;
- работу с нормативными правовыми актами;
- выступления с докладами, сообщениями на семинарских занятиях;
- защиту выполненных работ;
- участие в оперативном (текущем) опросе по отдельным темам изучаемой дисциплины;
- участие в собеседованиях, деловых (ролевых) играх, дискуссиях, круглых столах, конференциях;
- участие в тестировании и др.

Самостоятельная работа обучающихся во внеаудиторное время может состоять из:

- повторение лекционного материала;
- подготовки к семинарам (практическим занятиям);
- изучения учебной и научной литературы;
- изучения нормативных правовых актов (в т.ч. в электронных базах данных);
- решения задач, выданных на практических занятиях;
- подготовки к контрольным работам, тестированию и т.д.;
- подготовки к семинарам устных докладов (сообщений);
- подготовки рефератов, эссе и иных индивидуальных письменных работ по заданию преподавателя;
- выполнения курсовых работ, предусмотренных учебным планом;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов;
- написания рефератов и эссе по отдельным вопросам изучаемой темы.
- подготовки к семинарам устных докладов (сообщений);
- подготовки рефератов, эссе и иных индивидуальных письменных работ по заданию преподавателя;
- выполнения курсовых работ, предусмотренных учебным планом;
- выполнения выпускных квалификационных работ и др.
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов;
- написания рефератов и эссе по отдельным вопросам изучаемой темы.