МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Филологический факультет

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Кафедра печатных СМИ филологического факультета

Образовательная программа магистратуры
42.04.02 Журналистика

Направленность (профиль) программы
Политическая журналистика

Форма обучения
Очная, заочная

Статус дисциплины:
Факультативная дисциплина

Махачкала, 2022

Рабочая программа дисциплины «Проблемы информационной безопасности» составлена в 2022 году в соответствии с требованиями ФГОС ВО – магистратура по направлению подготовки 42.04.02 Журналистика от 08.06.2017г. № 529.

Разработчик: к.ф.н., старший преподаватель кафедры печатных СМИ Керимова Д. Ф.

Рабочая программа дисциплины одобрена:
на заседании кафедры печатных СМИ от «5» 03 2022г., протокол № 7.
Зав. кафедрой _____ /Магомедов Г. А./
(подпись)

на заседании Методической комиссии филологического факультета от «23» 03 2022г., протокол № 6.
Председатель _____ /Горбанева А. Н./
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «31» 03 2022г. _____
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина «Проблемы информационной безопасности» входит в часть факультативных дисциплин магистратуры по направлению «Политическая журналистика» образовательной программы 42.04.02 Журналистика. Дисциплина реализуется на филологическом факультете кафедрой печатных СМИ.

Содержание дисциплины охватывает круг вопросов, связанных с изучением понятий «право», «свобода», «тайна», «законодательство», с изучением медиа в системе отношений «государство – СМИ – общество», правовых основ журналистики и международного гуманитарного права.

Дисциплина нацелена на формирование следующих компетенций выпускника: универсальных – УК-1, общепрофессиональных – ОПК-2, профессиональных – ПК-4.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, самостоятельная работа.

Рабочая программа дисциплины предусматривает проведение видов контроля успеваемости в форме контрольных работ и промежуточный контроль в форме зачета.

Объем дисциплины – 1 зачетная единица, в том числе в академических часах по видам учебных занятий – 36.

Объем дисциплины в очной форме

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	Консультации		
3	36	36	6	-	-	-	-	30	зачет

Объем дисциплины в заочной форме

Семестр	Учебные занятия			Форма промежуточной аттестации (зачет,
	в том числе:			
	в	Контактная работа обучающихся с преподавателем	СРС, в	

		всего	из них					том числе экзамен	дифференцированный зачет, экзамен)
			Лекции	Лабораторные занятия	Практические занятия	КСР, зачет	Консультации		
3	36	36	2	-	-	4	-	30	зачет

1. Цели освоения дисциплины

Целями освоения дисциплины «Проблемы информационной безопасности» являются:
- ознакомление студентов с современными системами информационной безопасности, технологическими защиты информации;
- определение организационных мер информационной защиты, экономических и правовых принципов их функционирования, а также возможностей использования защиты в работе с информационными ресурсами в различных областях.

2. Место дисциплины в структуре ОПОП магистратуры

Дисциплина «Проблемы информационной безопасности» входит в часть факультативных дисциплин магистратуры (ФТД.01) по направлению 42.04.02 Журналистика.
Данный курс системно встраивается в общую программу магистратуры по направлению «Политическая журналистика».
Входные знания, умения и компетенции, необходимые для изучения данного курса, формируются в процессе изучения дисциплин «Правовые основы СМИ», «Права человека и журналистика», «Журналист в горячих точках».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения)

Код и наименование компетенции из ФГОС ВО	**Код и наименование индикатора достижения компетенций**	**Планируемые результаты обучения**	**Процедура освоения**
УК-1. Способен осуществлять поиск, критический анализ и синтез	**УК-1.1.** Анализирует и сопоставляет источники информации с точки зрения временных и	**Знает:** источники информации с точки зрения временных и пространственных условий их возникновения.	Устный опрос

информации, применять системный подход для решения поставленных задач	пространственных условий их возникновения: аргументированно формирует оценку информации, принимает обоснованные решения. **УК-1.2.** Демонстрирует способность анализировать и синтезировать информацию, связанную с проблемами современного общества, а также природой и технологиями формирования основ личностного мировоззрения. **УК-1.3.** Демонстрирует знание основных методов изучения наиболее значимых фактов, явлений, процессов в социогуманитарной сфере.	**Умеет:** аргументированно формировать оценку информации, принимать обоснованные решения. **Владеет:** методикой поиска и критического анализа информации. **Знает:** информацию, связанную с проблемами современного общества. **Умеет:** анализировать информацию, связанную с проблемами современного общества. **Владеет:** способностями синтезировать информацию, а также методами формирования основ личностного мировоззрения. **Знает:** основные методы изучения	

		наиболее значимых фактов, явлений, процессов в социогуманитарной сфере. **Умеет:** использовать свои знания в социогуманитарной сфере. **Владеет:** навыками использования знаний профессиональной деятельности.	
ОПК-2. Способен учитывать тенденции развития общественных и государственных институтов для их разностороннего освещения в создаваемых медиатекстах и (или) медиапродуктах	**ОПК-2.1.** Знает систему общественных государственных институтов и институтов, механизмы их функционирования и тенденции развития. **ОПК-2.2.** Соблюдают принцип объективности в создаваемых журналистских текстах и (или) продуктах при освещении деятельности	**Знает:** систему общественных государственных институтов. **Умеет:** использовать знание общественных государственных институтов в своей профессиональной деятельности. **Владеет:** способностью учитывать различные тенденции развития социальных институтов в своей профессиональной деятельности. **Знает:** принцип объективности в создаваемых журналистских	Письменный опрос

	общественных государственных институтов	текстах. **Умеет:** соблюдать принцип объективности в создаваемых журналистских текстах и (или) продуктах. **Владеет:** умением быть объективным в создаваемых журналистских текстах и (или) продуктах при освещении деятельности общественных государственных институтов.	
ПК-4. Способен организовать работу и руководить предприятием (подразделением) в современной медиаиндустрии	**ПК-4.1.** Проводит многофакторный анализ перспектив запуска проекта в сфере журналистики. **ПК-4.2.** Разрабатывает все компоненты и концепции и выстраивает приоритеты решения творческих задач.	**Знает:** множество перспектив запуска проекта в сфере журналистики. **Умеет:** анализировать перспективы запуска проекта в сфере журналистики. **Владеет:** множеством методов многофакторного анализа перспектив запуска проекта в сфере журналистики. **Знает:** приоритеты	Устный опрос

	ПК-4.3. Составляет план действий по реализации проекта.	решения творческих задач. **Умеет:** разрабатывать компоненты решения творческих задач. **Владеет:** способностью использовать разработанные компоненты при решении творческих задач. **Знает:** как составить план действий по проекту. **Умеет:** составлять план действий по реализации проекта. **Владеет:** способностью реализовать план проекта.	

4. Объем, структура и содержание дисциплины

4.1. Объем дисциплины составляет 1 зачетную единицу, 36 академических часов.

4.2. Структура дисциплины

4.2.1. Структура дисциплины в очной форме

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные	…		
	Модуль 1. Международные механизмы защиты информации. Защита экономической информации								
1.	Международные стандарты информационного обмена. Понятие угрозы	3		2				4	Устный опрос
2.	Информационная безопасность в условиях функционирования в России глобальных сетей	3						4	Устный опрос
3.	Виды возможных нарушений информационной системы	3		2				4	Устный опрос
4.	Таксономия нарушений информационной безопасности компьютерной системы и причины, обуславливающие их существование	3						2	Письменный опрос
5.	Назначение и	3		2				4	Устный опрос

	задачи в сфере обеспечения информационной безопасности на уровне государства								
6.	Концепция информационной безопасности	3						4	Устный опрос
7.	Место информационной безопасности экономических систем в национальной безопасности страны	3						4	Устный опрос
8.	Анализ способов нарушений информационной безопасности. Методы криптографии. Криптографические методы защиты информации. Использование защищенных компьютерных систем	3						4	Письменный опрос
	Итого по мод. 1: **36 часов**			6				30	
	Зачет								
	ИТОГО: 36 часов			6				30	

4.2.3. Структура дисциплины в заочной форме

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные	Зачет		
	Раздел 1. Международные механизмы защиты информации. Защита экономической информации								
1.	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей	3		2				6	Устный опрос
2.	Виды возможных нарушений информационной системы. Таксономия нарушений информационной безопасности компьютерной системы и причины, обуславливающие их существование	3						8	Письменный опрос
3.	Назначение и задачи в сфере обеспечения	3						8	Устный опрос

	информационной безопасности на уровне государства. Концепция информационной безопасности								
4.	Место информационной безопасности экономических систем в национальной безопасности страны. Анализ способов нарушений информационной безопасности. Методы криптографии. Криптографические методы защиты информации. Использование защищенных компьютерных систем	3						8	Письменный опрос
	Итого по разд. 2: **32 часа**			2				30	
	Зачет						4		
	ИТОГО: 36 часов			2			4	30	

4.3. Содержание дисциплины, структурированное по темам (разделам)

4.3.1. Содержание лекционных занятий по дисциплине

Модуль 1. Международные механизмы защиты информации. Защита экономической информации.

Тема 1. Международные стандарты информационного обмена. Понятие угрозы.

Содержание темы

Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации. Основные методы и средства защиты информационных систем.

Тема 2. Виды возможных нарушений информационной системы.

Содержание темы

Основные положения теории информационной безопасности информационных систем. Формальные модели безопасности их значение для построения защищенных информационных систем. Понятие доступа к данным и монитора безопасности. Функции монитора безопасности. Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности. Управление доступом к данным. Основные типы политики безопасности управления доступом к данным: дискреционная и мандатная политика безопасности. Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Тема 3. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Содержание темы

Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы, влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности. Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей. Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом. Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита. Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах. Защита данных и сервисов от воздействия вредоносных программ.

Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.

5. **Образовательные технологии**

Образовательный процесс по дисциплине строится на основе применения следующей комбинации методов преподавания: модульно-рейтинговое проблемное обучение и развивающее обучение. В связи с этим организация познавательной деятельности включает в себя элементы пассивного, активного и интерактивного обучения. В процессе реализации образовательных технологий предусмотрено возможное использование информационных технологий: предоставление информации, выдача рекомендаций по электронной почте, использование мультимедийных средств на занятиях и т. д.

6. Учебно-методическое обеспечение самостоятельной работы студентов

В рамках самостоятельной работы студенты изучают рекомендованную литературу (см. Пункт 8 учебной программы), знакомятся с электронными образовательными ресурсами, изучают периодическую печать.

№	Название темы	Кол-во часов	Форма самостоятельной работы
Модуль 1. Международные механизмы защиты информации. Защита экономической информации			
1.	Международные стандарты информационного обмена. Понятие угрозы	4	Реферирование рекомендованной литературы (см. Пункт 8 учебной программы)
2.	Информационная безопасность в условиях функционирования в России глобальных сетей	4	Организация наблюдения за соблюдением информационной безопасности в сетях
3.	Виды возможных нарушений информационной системы	4	Поиск возможных нарушений информационной системы
4.	Таксономия нарушений информационной безопасности компьютерной системы и	2	Разработка самостоятельной классификации нарушений информационной безопасности компьютерной системы и поиск

	причины, обуславливающие их существование		их причины
5.	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	4	Подготовка докладов, сообщений, рефератов (см. примерные темы в Пункте 7.2. учебной программы)
6.	Концепция информационной безопасности	4	Написание эссе по изученной теме
7.	Место информационной безопасности экономических систем в национальной безопасности страны	4	Организация круглого стола по изученной теме
8.	Анализ способов нарушений информационной безопасности. Методы криптографии. Криптографические методы защиты информации. Использование защищенных компьютерных систем	4	Подготовка дискуссионных докладов по изученной теме
Итого по мод. 1: ***30 часов***			
ВСЕГО: 30 часов			

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Типовые контрольные задания

Примерные темы рефератов и курсовых работ

1. Классификация информации. Виды данных и носителей.
2. Ценность информации. Цена информации.

3. Количество и качество информации.
4. Виды защищаемой информации.
5. Демаскирующие признаки объектов защиты.
6. Классификация источников и носителей информации.
7. Мероприятия по управлению доступом к информации.
8. Функциональные источники сигналов. Опасный сигнал.
9. Основные средства и системы, содержащие потенциальные источники опасных сигналов.
10. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.
11. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.
12. Виды угроз безопасности информации.
13. Основные принципы добывания информации.
14. Процедура идентификации, как основа процесса обнаружения объекта.
15. Методы синтеза информации.
16. Методы несанкционированного доступа к информации.
17. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.
18. Способы наблюдения с использованием технических средств.
19. Каналы утечки информации. Технические каналы утечки
20. Классификация технических каналов утечки по физической природе носителя.
21. Классификация технических каналов утечки по информативности.
22. Классификация технических каналов утечки по времени функционирования.
23. Классификация технических каналов утечки по структуре.
24. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.
25. Перехват электромагнитных излучений.
26. Акустическое подслушивание. Эффекты, возникающие при подслушивании.
27. Понятия скрытия информации, виды скрытия. Информационный портрет.
28. Противодействие наблюдению. Способы маскировки.
29. Способы и средства противодействия подслушиванию.
30. Нейтрализация закладных устройств.
31. Состав инженерной защиты и технической охраны объектов.
32. Инженерные конструкции и сооружения для защиты информации. Их классификация.
33. Средства идентификации личности.
34. Классификация датчиков охранной сигнализации.
35. Классификация извещателей.
36. Телевизионные системы наблюдения.
37. Основные средства системы видеоконтроля.
38. Защита личности как носителя информации.

39. Системный подход к защите информации.
40. Параметры системы защиты информации.

Вопросы к зачету
1. Международные стандарты информационного обмена.
2. Понятие угрозы.
3. Информационная безопасность в условиях функционирования в России глобальных сетей.
4. Виды противников или «нарушителей».
5. Понятия о видах вирусов.
6. Три вида возможных нарушений информационной системы. Защита.
7. Основные нормативные руководящие документы. Стандарт шифрования данных ГОСТ 28147-89.
8. Системы с открытым ключом.
9. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
10. Основные положения теории информационной безопасности информационных систем.
11. Модели безопасности и их применение.
12. Методы защиты информации с использованием голографии являются актуальным и развивающимся направлением.
13. Анализ способов нарушений информационной безопасности.
14. Криптографические методы.
15. Использование защищенных компьютерных систем.
16. Методы криптографии.
17. Основные технологии построения защищенных ЭИС.
18. Концепция информационной безопасности.

Тестовые задания
1. Кто имеет доступ к информации всемирной глобальной сети?
а) информационные работники;
б) сотрудники спецслужб;
в) все.
2. Регулируется ли деятельность в сети какими-либо законами?
а) да, полностью регулируется;
б) нет, таких законов не существует;
в) да, но не охватывает всю деятельность.
3. Кто является владельцем сети Интернет?
а) страна, в которой возник Интернет;
б) частная компания;
в) государственное ведомство;
г) не имеет владельца.
4. Может ли Интернет использоваться для незаконной деятельности?
а) да;
б) нет.

5. Какая наиболее распространенная сетевая уязвимость Вам известна?
а) ICQ («аська»);
б) электронная почта;
в) файрвол.
6. Являются ли беспроводные сети безопасным решением?
а) да, полностью безопасно;
б) нет;
в) да, но при условии установки специального устройства.
7. Что такое межсетевой экран?
а) аська;
б) брэндмауэр;
в) троян;
г) файрвол.
8. В каких целях может быть установлен межсетевой экран?
а) для обеспечения безопасности домашней сети;
б) для обеспечения безопасности сети организации;
в) во всех перечисленных случаях.
9. Что такое IT (ИТ)?
а) Интернет-технологии;
б) интересные технологии;
в) информационные технологии;
г) источники тока.
10. Какой вид компьютера считается стационарным (выглядит как довольно большая «коробка», к которой подключается монитор, клавиатура и мышь)?
а) планшет (англ. Tablet computer);
б) нетбук (англ. Netbook);
в) настольный компьютер (англ. Desktop);
г) бумбокс (англ. Boombox).

7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.
Общий результат выводится как интегральная оценка, складывающая из текущего контроля – 50 % и промежуточного контроля – 50 %.
Текущий контроль по дисциплине включает:
- посещение занятий – 18 баллов,
- выполнение творческих заданий – 16 баллов,
- выполнение домашних (аудиторных) контрольных работ – 16 баллов.
Промежуточный контроль по дисциплине включает:
- устный опрос – 20 баллов,
- письменная контрольная работа – 30 баллов.
Максимальное количество баллов за промежуточный контроль по одному модулю – 100 баллов. Результаты всех видов учебной деятельности за каждый модульный период оцениваются рейтинговыми баллами.

Минимальное количество средних баллов по всем модулям, дающее студентам право на положительную отметку без итогового контроля знаний – 51.
Итоговый контроль по дисциплине осуществляется преимущественно в форме тестирования по балльно-рейтинговой системе, максимальное количество которых – 100 баллов.
Итоговая оценка по дисциплине выставляется в баллах. Удельный вес итогового контроля в итоговой оценке по дисциплине составляет 50 % от среднего балла по всем модулям.
Шкала диапазона для перевода рейтингового балла в 5-балльную систему:
0-50 баллов – неудовлетворительно;
51-65 баллов – удовлетворительно;
66-85 баллов – хорошо;
86-100 баллов – отлично.

8. Учебно-методическое обеспечение дисциплины

а) адрес сайта курса
www.gam.sitecity.ru;

б) основная литература:
1. Вирен Г. Современные медиа. Приемы информационных войн [Электронный ресурс]: учебное пособие для студентов вузов / Г. Вирен. – Электрон. текстовые данные. – М.: Аспект Пресс, 2016. – 128 с. – 978-5-7567-0824-0. – Режим доступа: http://www.iprbookshop.ru/56990.html
2. Вирен Г. Современные медиа. Приемы информационных войн [Электронный ресурс]: учебное пособие для студентов вузов / Г. Вирен. – Электрон. текстовые данные. – М.: Аспект Пресс, 2013. – 126 с. – 978-5-7567-0701-4. – Режим доступа: http://www.iprbookshop.ru/21071.html
3. Мельников В. П. Информационная безопасность и защита и информации. – М., 2011.
4. Федоров А. В. Информационная безопасность в мировом политическом процессе. – М., 2006.
5. Филин С. А. Информационная безопасность. Учебное пособие. – М., 2006;

в) дополнительная литература:
1. Доктрина информационной безопасности Российской Федерации. Издательство: Ось-89, 2007. – 48 с.
2. Емельянов Г. В., Стрельцов А. А. О Доктрине информационной безопасности Российской Федерации. – Информационное общество, 2007. – С. 22-24.
3. Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В. Информационная безопасность открытых систем. Том 1. Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая Линия-Телеком, 2006. – 536 с.
4. Лепехин А. Н. Расследование преступлений против информационной

безопасности. Теоретико-правовые и прикладные аспекты. – М.: Тесей, 2008. – 176 с.
5. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. – М.: 2007. – 428 с.
6. Петренко С. А., Курбатов В. А. Политики информационной безопасности. – М.: Компания АйТи, 2006. – 400 с.
7. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. – СПб.: Питер, 2008. – 272 с.
8. Трахименок С. А. Безопасность государства. Методолого-правовые аспекты. – М.: «Хата», 2007. – 192 с.
9. Чернов А. А. Становление глобального информационного общества: проблемы и перспективы. – М.: «Дашков и К», 2008. – 232 с.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://www.media-online.ru
2. http://www.sostav.ru
3. http://www.adindex.ru
4. http://advtime.ru
5. http://www.advi.ru
6. http://www.advesti.ru
7. http://www.rwr.ru
8. Shturmuy.ru
9. http://www.shturmuy.ru

10. Методические указания для обучающихся по освоению дисциплины

В процессе организации самостоятельной работы студентов на занятиях используются традиционные формы и методы (аннотирование, конспектирование, подготовка выступления, доклада) и инновационные, такие как работа в группах, деловые игры, «мозговой штурм», анализ кейсов, «круглый стол» и др.

Рекомендации студентам по оформлению рефератов

Рефераты оформляются в виде рукописи (печатного текста), излагающей постановку проблемы, содержание исследования и его основные результаты. Текст реферата должен демонстрировать: знакомство автора с основной литературой вопроса; умение выделить проблему и определить методы ее решения; умение последовательно изложить существо рассматриваемых вопросов; владение соответствующим понятийным и терминологическим аппаратом; приемлемый уровень языковой грамотности, включая владение функциональным стилем изложения.

Реферат должен иметь следующую структуру:

титульный лист,
оглавление,
введение,
главы,
параграфы,
заключение,
список используемой литературы.
Номера присваиваются всем страницам, начиная с титульного листа, нумерация страниц проставляется со второй страницы. Титульный лист реферата должен содержать название факультета, направления подготовки магистра или специальность аспиранта, название темы, фамилию, имя, отчество автора, фамилию, инициалы научного руководителя, год выполнения. Оглавление представляет собой составленный в последовательном порядке список всех заголовков разделов работы с указанием страниц, на которых соответствующий раздел начинается

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Компьютерный класс с соответствующим программным обеспечением:
Microsoft Word,
Adobe InDesign,
Adobe PhotoShop,
Adobe Illustrator,
Internet
Explorer.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Специализированная аудитория: компьютерный класс, подключенный к интернету.
Специализированная мебель и оргсредства: интерактивная доска, наглядные пособия.
Компьютерное и мультимедийное оборудование:
- ноутбук;
- проектор;
- экран;
- флеш-накопитель.

Видео-, аудиовизуальные средства:
- диктофон;
- магнитофон;
- видеокамера.