

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ  
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

**42.04.02 Журналистика**

Профиль подготовки  
**Политическая журналистика**

Уровень высшего образования  
**Магистратура**

Форма обучения  
**Очная**

Статус дисциплины вариативная (по выбору)

Махачкала, 2017

Рабочая программа дисциплины «Проблемы информационной безопасности» составлена в 2017 году в соответствии с требованиями ФГОС ВО по направлению подготовки

**42.04.02 Журналистика**

(уровень **магистратура**)

от « 3 » ноября 2015 г. № 1295.

Разработчик: **кафедра печатных СМИ, Магомедов Г.А., к.и.н., доцент**  
(кафедра, ФИО, ученая степень, ученое звание)

Рабочая программа дисциплины одобрена:

на заседании кафедры печатных СМИ от « 17 » 03 2017 г., протокол № 5

Зав. кафедрой Г.А. Магомедов Магомедов Г.А.  
(подпись)

на заседании Методической комиссии филологического факультета от « \_\_\_ »  
\_\_\_\_\_ 2017 г., протокол № \_\_\_\_.

Председатель К.Э. Джамалов Джамалов К.Э.  
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим  
управлением « \_\_\_ » \_\_\_\_\_ 2017 г. \_\_\_\_\_

(подпись)

## Аннотация рабочей программы дисциплины

Дисциплина «Проблемы информационной безопасности» входит в вариативную часть образовательной программы магистратуры по направлению 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 магистранта: общекультурных – ОК-1, ОК-2, общепрофессиональных ОПК-2, профессиональных – ПК-3, ПК-7.

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

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме: контрольных работ, презентаций.

Объем дисциплины – 4 зачетные единицы, в том числе в академических часах по видам учебных занятий – 144 часа.

Семестр	Учебные занятия, в том числе контактная работа учащихся с преподавателем							Форма промежуточной аттестации (зачет, дифференц. зачет, экзамен)
	Из них							
	Всего	Лекции	Лаб.	Практич.	Конс.	СРС, в том числе экзамен		
А	144	6		12		126	зачет	

### 1.Цели освоения дисциплины

Цель курса «Проблемы информационной безопасности» - является ознакомление студентов с современными системами информационной безопасности, технологическими защиты информации, организационными мерами по информационной защите, экономическими и правовыми принципами их функционирования, а также

возможностями использования защиты в работе с информационными ресурсами в различных областях.

## 2. Место дисциплины в структуре ООП магистратуры.

Дисциплина «Проблемы информационной безопасности» относится к вариативной части(по выбору) образовательной программы магистратуры по направлению 42.04.01 – 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» магистранты используют знания навыки, полученные в результате освоения этих дисциплин.

## 3. Требования к результатам освоения дисциплины.

В результате изучения дисциплины студент должен:

- знать понятие информационных систем безопасности;
- знать роль мировых информационных систем безопасность в стратегии развития организации;
- знать признаки классификации безопасности информационных систем;
- знать основные типы функциональных систем безопасности ;
- уметь применять информационные системы безопасности в учебной и трудовой деятельности;
- уметь пользоваться различные системы безопасности информации в различных видах деятельности.

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

Компетенции	Формулировка компетенции из ФГОС ВО	Планируемые результаты обучения (показатели достижения заданного уровня)
Общекультурные компетенции (ОК): ОК-1, ОК-2	- способность к абстрактному мышлению, анализу, синтезу; - готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения.	<u>Знать</u> : законы логического, абстрактного мышления. <u>Уметь</u> : использовать имеющиеся знания в своей профессиональной деятельности; действовать в нестандартных ситуациях. <u>Владеть</u> : способностью нести социальную и этическую ответственность за принятые решения.
Общепрофессиональные компетенции (ОПК): ОПК - 2	- способность планировать и осуществлять коммуникационные кампании	<u>Знать</u> : способы планирования и осуществления коммуникационных кампаний и мероприятий.

	и мероприятия	<p>Владеть: способностью планировать и осуществлять коммуникационные кампании и мероприятия.</p> <p>Уметь: планировать коммуникационные кампании и мероприятия.</p>
<p>Профессиональные компетенции (ПК):</p> <p>ПК-3</p> <p>ПК-7</p>	<p>- готовность осуществлять организационные, координационные, контролирующие обязанности, текущее планирование в соответствии со стратегией развития СМИ, медийных проектов;</p> <p>- способность осуществлять разработку концепции медиапроекта на базе знания современных принципов и методов медиапроектирования и медиамоделирования</p>	<p>Знать: организационные, координационные, контролирующие обязанности, текущее планирование в соответствии со стратегией развития СМИ, медийных проектов</p> <p>концепции медиапроекта на базе знания современных принципов и методов медиапроектирования и медиамоделирования</p> <p>Владеть: организационными и координационными контролирующими обязанностями.;</p> <p>концепцией медиапроекта на базе знания современных принципов и методов медиапроектирования и медиамоделирования</p> <p>Уметь: осуществлять контролирующие обязанности, текущее планирование в соответствии со стратегией развития СМИ, медийных проектов;</p> <p>осуществлять разработку концепции медиапроекта на базе знания современных принципов и методов медиапроектирования и медиамоделирования</p>

--	--	--

#### 4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 4 зачетные единицы, 144 часа.

#### 4.2. Структура дисциплины.

№	Разделы и темы дисциплины	Се м.	Неделя	Виды учебной работы, включая самост. раб. студентов и трудоемкость (в часах)	Сам. раб.	Формы текущего контроля успеваемости (по неделям сем.) Форма промежуточ. аттест. (по семест.)
				Лек. Пр. Лаб. Конт., сам.		
<b>Модуль 1. Международные механизмы защиты информации</b>						
1.	Международные стандарты информационного обмена. Понятие угрозы.	2		2	10	
2.	Информационная безопасность в условиях функционирования в России глобальных сетей	2		2	10	
3.	Виды возможных нарушений информационной системы.	2		2	10	
Итого по модулю 1		2		4 2	30	
<b>Модуль 2. Способы защиты информации</b>						
4.	Таксономия нарушений информационной безопасности компьютерной системы и причины, обуславливающие их существование.	2		2	16	
5.	Назначение и	2		2	16	

	задачи в сфере обеспечения информационной безопасности на уровне государства.					
	Итого по модулю 2			2 2	32	
<b>Модуль 3. Концепция в сфере защиты информации</b>						
6.	Концепция информационной безопасности.	2		4	32	
	Итого по модулю 3			4	32	
<b>Модуль 4. Защита экономической информации</b>						
7.	Место информационной безопасности экономических систем в национальной безопасности страны.	2		2	16	
8.	Анализ способов нарушений информационной безопасности. Методы криптографии. Криптографические методы защиты информации. Использование защищенных компьютерных систем.	2		2	16	
	Итого по модулю 4			4	32	
	Итого: 144			6 12	126	

#### 4.3. Содержание дисциплины, структурированное по темам (разделам)

##### **Модуль 1. Международные механизмы защиты информации**

##### **Тема 1. Международные стандарты информационного обмена. Понятие угрозы.**

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. Информационная безопасность в условиях функционирования в России глобальных сетей**

Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.).

Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности.

Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.

## **Модуль 2. Способы защиты информации**

**Тема 1.** Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

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.

## **Практические занятия**

### **Модуль 1. Международные механизмы защиты информации**

**Тема 1.** Виды возможных нарушений информационной системы.

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.

## **Модуль 2. Способы защиты информации**

**Тема 1.** Таксономия нарушений информационной безопасности компьютерной системы и причины, обуславливающие их существование.

Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации.

Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа совместно с другими программами). Использование криптографических средств для решения задач идентификация и аутентификация.

Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов информационной системы. Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.

## **Модуль 3. Концепция в сфере защиты информации**

**Тема 1.** Концепция информационной безопасности.

Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований предъявляемых к системе. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

## **Модуль 4. Защита экономической информации**

**Тема 1.** Место информационной безопасности экономических систем в национальной безопасности страны.

Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности. Критерии безопасности компьютерных систем министерства обороны США ("Оранжевая книга"). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности.

Руководящие документы Гостехкомиссии России. Структура требований безопасности. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации. Показатели защищенности средств вычислительной техники от НСД. Классы защищенности автоматизированных систем.

Международные стандарты информационной безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Единые критерии»). Основные положения Единых критериев. Функциональные требования и требования доверия. Понятие Профиля защиты и Проекта защиты.

**Тема 2.** Анализ способов нарушений информационной безопасности. Методы криптографии. Криптографические методы защиты информации. Использование защищенных компьютерных систем.

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

### **5. Образовательные технологии.**

Преподавание дисциплины сочетает лекции и семинарские занятия в виде разбора кейсов. Предполагается проведение деловых игр, разбор конкретных ситуаций, разные тренинги в сочетании с внеаудиторной работой и целью формирования и развития профессиональных навыков магистрантов. В рамках учебного курса предусмотрены встречи с журналистами республиканских СМИ, государственных и общественных организаций.

### **6. Учебно-методическое обеспечение самостоятельной работы студентов.**

В рамках самостоятельной работы магистранты изучают литературу, знакомятся с сайтами Министерства печати и информации, республиканских СМИ, публикациями в центральных СМИ, документальными фильмами по соответствующей тематике.

Текущий контроль складывается из контроля посещения лекций, качества выполнения заданий и письменных работ, активного участия в семинарских занятиях, а также тестирования по отдельным темам.

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

#### **7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.**

Перечень компетенций с указанием этапов их формирования приведен в описании образовательной программы.

<b>Компетенция</b>	<b>Знания, умения, навыки</b>	<b>Процедура освоения</b>
ОК-1 ОК -2	Знать: законы логического мышления;	Устный опрос, письменный опрос
ОПК-2	Уметь: планировать и осуществлять коммуникационные кампании и	Письменный опрос.

ПК-3	мероприятия; Уметь: абстрактно мыслить, анализировать; - планировать и осуществлять коммуникационные кампании и мероприятия; - действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения;  - общаться с экспертами, представителями различных областей деятельности.	
ПК -3 ПК-7	Владеть: Способностью осуществлять разработку концепции медиапроекта.	Устный опрос, письменный опрос

## 7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания.

ОК-1

Схема оценки уровня формирования компетенции «способность к абстрактному мышлению, анализу, синтезу».

Уровень	Показатель (что обуч. должен продемонстрир.)	Оценочная шкала		
		Удовлетвор.	Хорошо	Отлично
Пороговый	Способность к абстрактному мышлению	Знает основные законы логики	Умеет использовать логические законы в профессиональной деятельности	Использует основы логических знаний в контексте своей социальной и профессиональной деятельности.
Базовый	Умение абстрактно мыслить, анализировать	Знает логические законы	Умеет абстрактно мыслить, анализировать различные ситуации в своей профессиональной	Использует знания медиаэкономики в своей социальной и профессиональной деятельности

			ой деятельности	
Продвину тый	Навыки абстрактного мышления, анализа, синтеза	Обладает навыками абстрактного мышления	Хорошо мыслит, анализирует, синтезирует различные социальные ситуации	Использует навыки абстрактного мышления, анализа, синтеза в своей профессионально й деятельности

## ОК - 2

Схема оценки уровня формирования компетенции «готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения».

Уровень	Показатель (что обуч. должен продемонстр.)	Оценочная шкала		
		Удовлетвор.	Хорошо	Отлично
Пороговы й	Готовность действовать в нестандартных ситуациях	Готов действовать в нестандартных ситуациях	Хорошо действует в нестандартных ситуациях.	Отлично действует в нестандартных ситуациях.
Базовый	Умение действовать в нестандартных ситуациях, нести социальную и этическую ответственнос ть за принятые решения	Умеет действовать в нестандартных ситуациях	Хорошо умеет действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения	Отлично несет социальную и этическую ответственность за принятые решения в своей профессионально й деятельности.
Продвину тый	Профессионал ьное чувство социальной и этической ответственнос ти за принятые	Способен действовать в нестандартных ситуациях, чувствует свою ответственность.	Хорошо действует в нестандартных ситуациях, глубоко понимая свою	Отлично действует в нестандартных ситуациях, глубоко понимая свою социальную

	решения, умение действовать в нестандартных ситуациях.		социальную и этическую ответственность за принятые решения в своей профессиональной деятельности.	и этическую ответственность за принятые решения в своей профессиональной деятельности.
--	--	--	---	--

ОПК – 2

Схема оценки уровня формирования компетенции «способность планировать и осуществлять коммуникационные кампании, мероприятия».

Уровень	Показатели (что обуч. должен продем.)	Оценочная шкала		
		Удовлетворит.	Хорошо	Отлично
Пороговый	Знание способов планирования и осуществления коммуникационных программ и мероприятий	Знает способы планирования и осуществления коммуникационных программ и мероприятий	Хорошо знает способы планирования и осуществления коммуникационных программ и мероприятий	Отлично знает способы планирования и осуществления коммуникационных программ и мероприятий
Базовый	Готовность планировать и осуществлять коммуникационные кампании, мероприятия	Готов планировать и осуществлять коммуникационные кампании, мероприятия	Хорошо готов планировать и осуществлять коммуникационные кампании, мероприятия	Отлично готов планировать и осуществлять коммуникационные кампании, мероприятия
Продвинутый	Планирует и осуществляет коммуникационные кампании мероприятия	Умеет планировать и осуществлять коммуникационные кампании и	Хорошо планирует и осуществляет коммуникационные кампании	Отлично планирует и осуществляет коммуникационные кампании

		мероприятия	мероприятия	мероприятия
--	--	-------------	-------------	-------------

ПК – 3

Схема оценки уровня формирования компетенции «готовность осуществлять организационные, координационные, контролирующие обязанности, текущее планирование в соответствии со стратегией развития СМИ, медийных проектов».

Уровень	Показатель (что обуч. должен продемонстрир.)	Оценочная шкала		
		Удовлетвор.	Хорошо	Отлично
Пороговый	Готовность квалифицированно выполнять организационные обязанности	Готов квалифицированно выполнять организационные обязанности	Умеет квалифицированно выполнять организационные обязанности	Квалифицированно выполняет организационные обязанности
Базовый	Умение осуществлять организационные, координационные, контролирующие обязанности, текущее планирование в соответствии со стратегией развития СМИ, медийных проектов	Умеет осуществлять организационные, координационные, контролирующие обязанности, текущее планирование в соответствии со стратегией развития СМИ, медийных проектов	Хорошо осуществляет организационные, координационные, контролирующие обязанности, текущее планирование в соответствии со стратегией развития СМИ, медийных проектов	Готов самостоятельно осуществлять организационные, координационные, контролирующие обязанности, текущее планирование в соответствии со стратегией развития СМИ, медийных проектов
Продвинутой	Навыки выполнения организационных, координационных, контролирующих обязанностей, текущее	Умеет самостоятельно осуществлять организационные, координационные, контролирующие обязанности,	Хорошо умеет осуществлять организационные, координационные, контролирующие	Отлично осуществляет организационные, координационные, контролирующие обязанности, текущее

	планирование в соответствии со стратегией развития СМИ, медийных проектов	текущее планирование в соответствии со стратегией развития СМИ, медийных проектов	е обязанности, текущее планирование в соответствии со стратегией развития СМИ, медийных проектов	планирование в соответствии со стратегией развития СМИ, медийных проектов
--	---	---	--	---

ПК – 7

Схема оценки уровня формирования компетенции «способность осуществлять разработку концепции медиапроекта на базе знания современных принципов и методов медиапроектирования и медиамоделирования».

Уровень	Показатель (что обуч. должен продемонстр.)	Оценочная шкала		
		Удовлетвор.	Хорошо	Отлично
Пороговый	способность осуществлять разработку концепции медиапроекта	Готов осуществлять разработку концепции медиапроекта	Умеет осуществлять разработку концепции медиапроекта	Осуществляет разработку концепции медиапроекта
Базовый	Умение осуществлять разработку концепции медиапроекта на базе знания современных принципов и методов медиапроектирования и медиамоделирования	Умеет осуществлять разработку концепции медиапроекта на базе знания современных принципов и методов медиапроектирования и медиамоделирования	Хорошо осуществляет разработку концепции медиапроекта на базе знания современных принципов и методов медиапроектирования и медиамоделирования	Отлично осуществляет разработку концепции медиапроекта на базе знания современных принципов и методов медиапроектирования и медиамоделирования
Продвинутый	Навыки разработки концепции медиапроекта на базе знания	Умеет самостоятельно осуществлять разработку концепции	Хорошо умеет осуществлять разработку концепции	Отлично осуществляет разработку концепции медиапроекта на

	современных принципов и методов медиапроектирования и медиамоделирования	медиапроекта на базе знания современных принципов и методов медиапроектирования и медиамоделирования	медиапроекта на базе знания современных принципов и методов медиапроектирования и медиамоделирования	базе знания современных принципов и методов медиапроектирования и медиамоделирования
--	--	--	--	--

Если хотя бы одна из компетенций не сформирована, то положительной оценки по дисциплине быть не может.

### 7.3. Типовые контрольные задания

#### Тестовые задания

**Кто имеет доступ к информации всемирной глобальной сети?**

1. Информационные работники
2. Сотрудники спец служб

**3. Все**

**Регулируется ли деятельность в сети какими-либо законами?**

1. Да, полностью регулируется
2. Нет, таких законов не существует

**3. Да, но не охватывает всю деятельность**

**Кто является владельцем сети Интернет?**

1. Страна, в которой возник Интернет
2. Частная компания
3. Государственное ведомство

**4. Не имеет владельца**

**Может ли Интернет использоваться для незаконной деятельности?**

1. Да
2. Нет

**Какая наиболее распространенная сетевая уязвимость вам известна?**

1. ICQ («аська»)
2. Электронная почта
3. Файрвол

**Являются ли беспроводные сети безопасным решением?**

1. Да, полностью безопасно
2. Нет
3. Да, но при условии установки специального устройства

**Что такое Межсетевой экран?**

1. Аська
2. Брэндмауэр
3. Троян
4. Файрвол

**В каких целях может быть установлен межсетевой экран?**

1. Для обеспечения безопасности домашней сети
2. Для обеспечения безопасности сети организации

**3. Во всех перечисленных случаях**

**Как может называться межсетевой экран?**

4. Файрвол



## Вопросы для промежуточных контрольных работ

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

### **7.4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций.**

Общий результат выводится как интегральная оценка, складывающаяся из текущего контроля – 30% и промежуточного контроля- 70%.

Текущий контроль по дисциплине включает:

- участие на практических занятиях – 5 баллов;
- выполнение домашних (аудиторных) контрольных работ – 15 баллов.

Промежуточный контроль по дисциплине включает:

- устный опрос – 15 баллов;
- письменная контрольная работа – 70 баллов.

### **8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.**

#### **Основная литература:**

1. Мельников В.П. Информационная безопасность и защита информации. –М., 2011
2. Федоров А.В. Информационная безопасность в мировом политическом процессе. – М., 2006

3. Филин С.А. Информационная безопасность. Учебное пособие. –М., 2006.

#### **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. – Мн.: «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](http://www.shturmuy.ru).
9. <http://www.shturmuy.ru>

#### **10. Методические указания для обучающихся по освоению дисциплины.**

Магистрант должен обладать широкими профессиональными качествами, в том числе к способности к самообразованию и к саморазвитию.

Формирование этих качеств являются обязательными компонентами учебно-воспитательного процесса в университете. В решении этой задачи значительная роль отводится самостоятельной работе как одной из важнейших видов учебной деятельности студента. Наряду с лекциями и практическими занятиями самостоятельная работа составляет система университетского образования.

Самостоятельная работа заключается:

- в составлении текстов по отдельным темам;
- в подготовке к семинарским занятиям;
- в подготовке к тестированию как по отдельным темам, так и по итоговому по дисциплине;

- в подготовке бизнес планов.

Самостоятельная работа по теме должна помочь приобрести соответствующие знания и умения:

1. уметь определять факторы, оказывающие влияние на политические, экономические и иного рода процессы;
2. понимать значение и роль средств массовой информации для социально-экономического, политического, культурного развития нашей страны;
3. понимать последствия внешних факторов воздействия для политической и экономической ситуации в России, в том числе для консолидации нашего общества.

Написание реферата или доклада целесообразно начинать с изучения учебно-методической и научно-исследовательской литературы. Кроме того, необходимо познакомиться с материалами учебников и другими первоисточниками. При этом важно понимать суть изучаемой проблемы, ее внутренне содержание и характер. Весьма важно обратить внимание на последствия того или иного исторического события, на степень его влияние на последующие периоды, а также отражение его в российских СМИ. Реферат и другие виды самостоятельной работы студента должны представлять собой целостную, завершённую учебно-научную работу. Должны быть четко сформулированы: исследуемые вопросы, цели, задачи, проблемы. Работа студента должна быть написана научным языком; особо следует обращать внимание на точность и однозначность терминологии.

Любой вид самостоятельной работы студента имеет несколько этапов и приемов:

1. повторение всего пройденного теоретического материала и проработка лекций;
2. определение цели самостоятельной работы;
3. уяснение задачи поставленной проблемы;
4. разработка плана действия (выбор путей и средств для решения задачи) и определение входов к практическому занятию;
5. выбор литературы;
6. конспектирование первоисточников и литературы;
7. подведение итогов и детализация собственных выводов.

Важным моментом самостоятельной работы является умение работать с научной литературой, с газетными текстами, нормативными документами. Работа с литературой состоит из целого ряда приемов, в том числе: структурирование, анализ, сопоставление, запоминание, смысловое воспроизведение прочитанного в письменной и устной форме. Анализируя газетные текста, главная задача студента заключается в том, чтобы как можно четко определить жанровую специфику материала, его особенности.

В процессе самостоятельной работы и проработки курса «Проблемы информационной безопасности» студенту рекомендуется опираться на учебно-методические издания и методические материалы, выпущенных кафедрой печатных СМИ ДГУ. а также учебно-методические издания других вузов России по подготовке – журналистика.

Самостоятельная работа должна носить систематический характер, быть интересной и привлекательной для студента.

результаты самостоятельной работы контролируются преподавателем и учитываются при аттестации студента (промежуточный контроль, экзамен). При этом проводятся: тестирование, экспресс-опрос на семинарах и практических занятиях, заслушивание докладов, проверка письменных работ.

Осваивая курс «Проблемы информационной безопасности», студенту необходимо научиться работать на лекциях, на семинарских занятиях и организовывать самостоятельную внеаудиторную деятельность.

В начале лекции необходимо уяснить цель, которую лектор ставит перед собой и студентами. Важно внимательно слушать лектора, отмечать наиболее существенную информацию и кратко записывать ее в тетрадь. Сравнить то, что услышано на лекции с прочитанным и усвоенным ранее, укладывать новую информацию в собственную, уже имеющуюся, систему знаний. По ходу лекции важно подчеркивать новые термины, устанавливать их взаимосвязь с изученными ранее понятиями.

Необходимо очень тщательно вслед за лектором делать записи, таблицы. Если лектор приглашает к дискуссии, необходимо принять в ней участие.

Если на лекции студент не получил ответа на возникшие у него вопросы, необходимо в конце лекции задать их лектору.

В ходе самостоятельной подготовки к семинарскому занятию необходимо прочитать записанную лекцию, подчеркнуть наиболее важные моменты, составить словарь новых терминов, составить план ответа на каждый из предлагаемых для изучения вопросов. Для более глубокого усвоения темы необходимо прочесть рекомендованный преподавателем материал из учебной литературы.

При подготовке выступления по реферату необходимо не только воспользоваться литературой, рекомендованной преподавателем, но и проявить самостоятельность в отыскании новых источников, интересных фактов, статистических данных, связанных с обеспечением безопасности бизнеса.

В процессе подготовки к занятиям необходимо воспользоваться материалами учебно-методического комплекса дисциплины.

Важнейшей особенностью обучения в высшей школе является высокий уровень самостоятельности студентов в ходе образовательного процесса. Эффективность самостоятельной работы зависит от таких факторов как:

- уровень мотивации студентов к овладению конкретными знаниями и умениями;
- наличие навыка самостоятельной работы, сформированного на предыдущих этапах обучения;
- наличие четких ориентиров самостоятельной работы.

Приступая к самостоятельной работе, необходимо получить следующую информацию:

- цель изучения конкретного учебного материала;
- место изучаемого материала в системе знаний, необходимых для формирования специалиста;
- перечень знаний и умений, которыми должен овладеть студент;
- порядок изучения учебного материала;
- источники информации;
- наличие контрольных заданий;
- форма и способ фиксации результатов выполнения учебных заданий;
- сроки выполнения самостоятельной работы.

Эта информация представлена в учебно-методическом комплексе дисциплины.

При выполнении самостоятельной работы рекомендуется:

- записывать ключевые слова и основные термины,
- составлять словарь основных понятий,
- писать краткие рефераты по изучаемой теме.

Результатом самостоятельной работы должна быть систематизация и структурирование учебного материала по изучаемой теме, включение его в уже имеющуюся у студента систему знаний.

После изучения учебного материала необходимо проверить усвоение учебного материала с помощью предлагаемых тестов текущего контроля и при необходимости повторить учебный материал.

В процессе подготовки к экзамену необходимо систематизировать, запомнить учебный материал, научиться применять его при решении конкретных задач по обеспечению безопасности бизнеса.

Основными способами приобретения знаний, как известно, являются: чтение учебника и дополнительной литературы, рассказ и объяснение преподавателя, решение тестов, поиск ответа на контрольные вопросы.

Известно, приобретение новых знаний идет в несколько этапов:

знакомство;

понимание, уяснение основных закономерностей строения и функционирования изучаемого объекта, выявление связей между его элементами и другими подобными объектами;

фиксация новых знаний в системе имеющихся знаний;

запоминание и последующее воспроизведение;

использование полученных знаний для приобретения новых знаний, умений и навыков и т.д.

Для того, чтобы учащийся имел прочные знания на определенном уровне (уровень узнавания, уровень воспроизведения и т.д.), рекомендуют проводить обучение на более высоком уровне.

Приобретение новых знаний требует от учащегося определенных усилий и активной работы на каждом этапе формирования знаний. Знания, приобретенные учащимся в ходе активной самостоятельной работы, являются более глубокими и прочными.

В ходе обучения студент сталкивается с необходимостью понять и запомнить большой по объему учебный материал. Запомнить его очень важно, так как даже интеллектуальные и операционные умения и навыки для своей реализации требуют определенных теоретических знаний.

Важнейшим условием для успешного формирования прочных знаний является их упорядочивание, приведение их в единую систему. Это осуществляется в ходе выполнения учащимся следующих видов работ по самостоятельному структурированию учебного материала:

- запись ключевых слов,
- составление словаря терминов,
- составление классификаций по различным признакам,
- выявление причинно-следственных связей,
- составление коротких рефератов, учебных текстов,
- составление опорных схем и конспектов,
- составление плана рассказа.

Практическое занятие должно ориентировать магистранта на организацию самостоятельной работы. С этой целью на каждом занятии должна быть предусмотрена самостоятельная работа студентов под контролем преподавателя, во время выполнения которой студент может обратиться к преподавателю с вопросом, получить на него ответ. Сам процесс организации самостоятельной работы на занятии должен служить образцом организации самостоятельной деятельности магистранта. Очень полезна организация самостоятельной работы со взаимопроверкой магистрантами работ друг друга. Это развивает умение осуществлять контроль и коррекцию результатов своего собственного труда.

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

Для достижения поставленных образовательных целей применяются следующие информационные технологии:

- представление учебников и другого печатного материала;
- размещение изучаемых материалов на сайте кафедры;
- видеопленки;
- работа в электронной библиотеке;
- самостоятельная работа с использованием электронной почты;
- электронные образовательные ресурсы.

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

Компьютерное и мультимедийное оборудование:

- ноутбук;
- проектор;
- экран;
- флеш-накопитель.

Видео-аудиовизуальные средства:

- диктофон;
- магнитофон;
- видеокамера.