

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
образования
«Кубанский государственный университет»
Факультет управления и психологии

УТВЕРЖДАЮ
Проректор по учебной работе
качеству образования – первый
проректор
Хагуров Т.А.
подпись
« 31 » мая 2019 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.Б.16 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА
ИНФОРМАЦИИ

Направление подготовки: *46.03.02 Документоведение и архивоведение*

Направленность (профиль): *Организационное проектирование
документационного обеспечения управления в
организации*

Программа подготовки: *академическая*

Форма обучения: *заочная*

Квалификация (степень) выпускника: *бакалавр*

Краснодар, 2019

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 46.03.02 Документоведение и архивоведение (профиль: Организационное проектирование систем документационного обеспечения управления в организации)

Программу составили:

Савченко А.П., доцент кафедры, кандидат физ.-мат. наук, доцент



Мирошниченко М.А., доцент кафедры, канд. экон. наук, доцент



Рабочая программа обсуждена на заседании кафедры общего стратегического, информационного менеджмента и бизнес-процессов протокол № 9 от «02» апреля 2019 г.

Заведующий кафедрой Ермоленко В.В.



Рабочая программа обсуждена на заседании кафедры (выпускающей)

протокол № 9 от «02» апреля 2019 г.

Заведующий кафедрой (выпускающей) Ермоленко В.В.



Утверждена на заседании учебно-методической комиссии факультета управления и психологии

протокол № 7 от «22» апреля 2019 г.

Председатель УМК факультета Шлюбуль Е.Ю.



Рецензенты:

Маслак Светлана Ивановна, заместитель генерального директора ООО «Комплексный инжиниринг»

Бондарева Марина Ивановна, начальник отдела служебной переписки администрации Краснодарского края

1. Цели и задачи изучения дисциплины

1.1 Цели дисциплины

Основной целью дисциплины является формирование у студентов комплекса знаний в области организации системы защиты информации, освоение основных методов обеспечения информационной безопасности.

Цели изучения дисциплины:

- формирование понятийного аппарата в области информационной безопасности (ИБ), усвоение сущности, целей, задач и значения ИБ;
- установление критериев, условий и принципов отнесения информации к защищаемой и классификация ее по собственникам, видам тайн и материальным носителям;
- классификация угроз безопасности информации, их причины, условий проявления, методов реализации;
- определение и классификация объектов, видов, методов и средств ИБ и обоснование необходимости системного обеспечения ИБ в организациях и на предприятиях различных форм собственности;
- развитие у обучаемых организаторских способностей, инициативы и творчества, умения обоснованно и правильно принимать решения по организации мероприятий по ИБ.

Дисциплина рассматривает основы методологии обеспечения информационной безопасности в организации. Изучаются теоретические основы защиты информации, функциональные возможности программных и аппаратных средств защиты информации.

1.2 Задачи дисциплины

Для достижения целей решаются следующие задачи изучения дисциплины:

Теоретическая компонента:

- 1) сформировать базовый понятийный аппарат в области ЗИ и ИБ, теоретические и концептуальные основы ЗИ и ИБ;
- 2) знать критерии, условия принципы отнесения информации к защищаемой;
- 3) изучить потенциально существующие угрозы безопасности информации;
- 4) знать классификацию видов, методов и средств ЗИ, состав кадрового и ресурсного обеспечения ЗИ, назначение и структуру систем ЗИ;

Познавательная компонента:

- 1) классифицировать угрозы безопасности информации по их источникам, оценивать степень их опасности;
- 2) классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности;

Практическая компонента:

- 1) владеть методикой определения объектов ЗИ, методикой отнесения сведений к государственной и коммерческой тайне;
- 2) уметь определять гриф секретности и составлять перечни конфиденциальных документов на предприятии, организации;
- 3) осуществлять обоснованный выбор инструментальных средств информационных технологий для решения задач в области работы защиты информации.

1.3 Место дисциплины в структуре ООП ВО

Дисциплина «Информационная безопасность и защита информации» принадлежит к базовым дисциплинам блока Б1 направления подготовки 46.03.02 «Документоведение и архивоведение» основной образовательной программы бакалавра и имеет индекс Б1.Б.16.

Объектом изучения курса являются современные инструменты и технологии обеспечения информационной безопасности организации.

Предметом изучения курса являются:

- теоретические и методические основы обеспечения ИБ на предприятиях различных форм собственности;
- основные виды информационных угроз и методы их профилактики

- программные и технические средства защиты информации;

Для успешного усвоения дисциплины необходимо, чтобы студент имел знания, умения, владение и опыт деятельности в объеме требований следующих дисциплин: Информационные технологии, Математика, Информационное право, изучаемых на I–III курсах обучения.

Предшествующие дисциплины: Информационные технологии, Математика, Информационное право, на которые опирается изучаемая дисциплина и являющиеся необходимым «входным» уровням освоения данной дисциплины. В свою очередь, изучение дисциплины обеспечивает возможность успешного прохождения студентами преддипломной практики и выполнения выпускной квалификационной работы бакалавра.

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В итоге изучения дисциплины студенты должны приобрести необходимые для фактического проявления заявленных компетенций представления, знания, умения и навыки. В таблице представлено содержание данных результатов с указанием компетенций, фактическое проявление которых они обеспечивают.

Изучение данной учебной дисциплины направлено на формирование у обучающихся общепрофессиональных компетенций

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	ОПК-6	Способностью решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать методы решения задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Методами и инструментам и защиты информации
2.	ПК-38	Владением навыками работы с документами, содержащими информацию ограниченного доступа	Знать приемы работы с документами, содержащими информацию ограниченного доступа	Уметь применять навыки работы с документами, содержащими информацию ограниченного доступа	Владеть навыками работы с документами, содержащими информацию ограниченного доступа

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 3 зач.ед. (108 ч), их распределение по видам работ представлено в таблице (для студентов ОФО и ЗФО).

Распределение трудоемкости по всем видам аудиторной и самостоятельной работы студента по семестрам

Виды работы		Очная форма обучения		
		Всего часов	Семестр	
			7 семестр	6 семестр
Аудиторная работа		54	54	
В том числе: Лекции (Л)		18	18	
Занятия семинарского типа (семинары, практические занятия, практикумы и иные аналогичные занятия) (ПЗ)		18	18	
Лабораторные занятия (ЛР)		18	18	
ИКР		0,2	0,2	
КСР		4	4	
Контактные часы		58,2		
Самостоятельная работа		49,8	49,8	
В том числе:				
<i>Курсовая работа</i>				
<i>Проработка учебного (теоретического) материала</i>		10	10	
<i>Выполнение индивидуальных заданий (подготовка сообщений, презентаций)</i>		10	10	
<i>Реферат (Эссе)</i>				
<i>Подготовка к текущему контролю</i>		29,8	29,8	
<i>Подготовка и сдача зачета (экзамена)</i>				
Промежуточная аттестации (зачет, экзамен)			зачет	
Общая трудоемкость	Час.	108		
	Зач.ед.	3		

Распределение трудоемкости по всем видам аудиторной и самостоятельной работы студента по семестрам

Виды работы		Заочная форма обучения		
		Всего часов	Семестр	
			3 курс	4 курс
Аудиторная работа		14	8	6
В том числе: Лекции (Л)		6	4	2
Занятия семинарского типа (семинары, практические занятия, практикумы и иные аналогичные занятия) (ПЗ)		4		4
Лабораторные занятия (ЛР)		4	4	
ИКР		0,2		0,2
КСР				
Контактные часы				
Самостоятельная работа		90	28	62
В том числе:				
<i>Курсовая работа</i>				
<i>Проработка учебного (теоретического) материала</i>				
<i>Выполнение индивидуальных заданий (подготовка сообщений, презентаций)</i>				
<i>Реферат (Эссе)</i>				
<i>Подготовка к текущему контролю</i>				

<i>Подготовка и сдача зачета (экзамена)</i>		3,8		3,8
Промежуточная аттестации (<i>зачет, экзамен</i>)				зачет
Общая трудоемкость	Час.	108		
	Зач.ед.	3		

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам и темам дисциплины.
Разделы дисциплины, изучаемые в 8 семестре.

№ темы	Наименование разделов и тем	ОФО					ЗФО						
		Количество часов						Количество часов					
		Всего	Аудиторная работа			СРС	Всего	Аудиторная работа			СРС		
Л	ПЗ		ЛР	Л	ПЗ			ЛР					
1	2	3	4	5	6	7							
I	Раздел №1. Введение. Концепция информационной безопасности												
1	Основные термины и положения системы защиты информации		1			2				4			
2	Концептуальная модель информационной безопасности		1	2						4			
3	Угрозы конфиденциальной информации		2	2		4		2		8			
4	Действия, приводящие к неправомерному овладению конфиденциальной информацией		2	2		4			2	4			
II	Раздел № 2. Направления обеспечения информационной безопасности												
5	Правовая защита конфиденциальной информации		2	2		2		1		4			
6	Организационная защита конфиденциальной информации		2		2	2		1		4			
7	Инженерно-техническая защита конфиденциальной информации				2	10				10			
III	Раздел 3. Способы защиты информации												
8	Характеристика основных способов защиты информации		2			2		2		4			
9	Проектирование системы защиты информации				2	4				4			
IV	Раздел 4. Пресечение разглашения												

	конфиденциальной информации										
10	Общие положения по пресечению разглашения конфиденциальной информации		2			2					4
11	Основные способы пресечения разглашения конфиденциальной информации			2		2			2		4
V	Раздел 5. Защита информации от утечки по техническим каналам										
12	Классификация технических каналов утечки конфиденциальной информации		2			4					6
13	Защита информации от утечки по визуально-оптическим каналам					2					4
14	Защита информации от утечки по акустическим каналам			2		2					4
15	Защита информации от утечки по каналам электронной связи				4	2					4
16	Защита информации от утечки по материально-вещественным каналам			2	2					2	4
VI	Раздел 6. Противодействие несанкционированному доступу к источникам конфиденциальной информации										
17	Способы несанкционированного доступа		2			3					6
18	Технические средства защиты от несанкционированного доступа к информации			2	4					2	6
19	Защита от подслушивания и перехвата			2		1					2
20	Противодействие незаконному подключению к линиям связи				2	1,8					2
21	Зачет						4				
	Итого по дисциплине	108	18	18	18	49,8	108	6	4	4	90

2.3. Содержание разделов и тем дисциплины

2.3.1. Занятия лекционного типа

№ Раздела и темы	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
------------------	-----------------------------	---------------------------	-------------------------

I	Раздел №1. Введение. Концепция информационной безопасности		
1	Основные термины и положения системы защиты информации	Концепция информационной безопасности. Система защиты информации.	Обсуждение темы
2	Концептуальная модель информационной безопасности	Модель информационной безопасности. Система безопасности информации.	Обсуждение темы
3	Угрозы конфиденциальной информации	Основные проявления угроз безопасности информации. Классификация угроз безопасности информации.	Обсуждение темы
4	Действия, приводящие к неправомерному овладению конфиденциальной информацией	Классификация действий, приводящих к неправомерному овладению конфиденциальной информацией. Анализ действий, приводящих к неправомерному овладению конфиденциальной информацией.	Обсуждение темы
II	Раздел № 2. Направления обеспечения информационной безопасности		
5	Правовая защита конфиденциальной информации	Характеристика защитных действий. Анализ международных и внутригосударственных правовых актов по защите конфиденциальной информации.	Обсуждение темы
6	Организационная защита конфиденциальной информации	Анализ организационной защиты конфиденциальной информации. Задачи службы безопасности предприятия.	Обсуждение темы
III	Раздел 3. Способы защиты информации		
8	Характеристика основных способов защиты информации	Анализ основных способов защиты информации. Мероприятия по защите информации.	Обсуждение темы
IV	Раздел 4. Пресечение разглашения конфиденциальной информации		
10	Общие положения по пресечению разглашения конфиденциальной информации	Классификация каналов распространения информации. Анализ каналов распространения информации.	Обсуждение темы
V	Раздел 5. Защита информации от утечки по техническим каналам		
12	Классификация технических каналов утечки конфиденциальной информации	Причины и условия возникновения технических каналов утечки конфиденциальной информации. Классификация технических каналов утечки конфиденциальной информации.	Обсуждение темы
VI	Раздел 6. Противодействие несанкционированному доступу к источникам конфиденциальной информации		

17	Способы несанкционированного доступа	Классификация несанкционированного Обобщенная несанкционированного доступа.	способ доступа. модель	Дискуссия
----	--------------------------------------	---	------------------------	-----------

2.3.2 Занятия семинарского типа

№ темы	Наименование раздела	Тематика практических работ	Форма текущего контроля
2	Концептуальная модель информационной безопасности	Основные положения концепции информационной безопасности	Ответ на семинаре
3	Угрозы конфиденциальной информации	Классификация угроз безопасности информации	Ответ на семинаре
4	Действия, приводящие к неправомерному овладению конфиденциальной информацией	Состав и классификация действий, приводящих к неправомерному овладению конфиденциальной информацией	Ответ на семинаре
5	Правовая защита конфиденциальной информации	Поиск и анализ правовых документов по защите конфиденциальной информации	Ответ на семинаре
11	Основные способы пресечения разглашения конфиденциальной информации	Организационные и технические средства пресечения разглашения информации.	Ответ на семинаре
14	Защита информации от утечки по каналам электронной связи	Основы криптографии. Шифрованные каналы связи	Ответ на семинаре
16	Защита информации от утечки по материально-вещественным каналам	Средства и способы защиты от материально-вещественного канала утечки конфиденциальной информации	Ответ на семинаре
18	Технические средства несанкционированного доступа к информации	Характеристика основных технических средств несанкционированного доступа к информации	Ответ на семинаре
19	Защита от подслушивания и перехвата	Способы противодействия подслушиванию конфиденциальной информации	Ответ на семинаре

2.3.3 Лабораторные занятия

№ темы	Тематика лабораторных работ	Форма текущего контроля
1	Структура и функции службы безопасности предприятия	Отчет по л/р
2	Методы программно-аппаратной защиты информации	Отчет по л/р
3	Комплексный проект системы информационной безопасности	Отчет по л/р
4	Работы с антивирусными программами.	Отчет по л/р
5	Анализ рисков утечки конфиденциальной информации	Отчет по л/р

6	Организация защиты информации с помощью пароля	Отчет по л/р
7	Защита компьютеров с помощью сетевых экранов при работе в Интернет	Отчет по л/р

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы учебным планом не предусмотрены

2.4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Самостоятельное изучение тем	Методические указания по организации самостоятельной работы студентов магистратуры и бакалавриата направления «Документоведение и архивоведение», утвержденные кафедрой общего, стратегического, информационного менеджмента и бизнес-процессов. 2017 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии, используемые на аудиторных занятиях

Образовательные технологии, используемые при реализации различных видов учебной деятельности:

- лекции: лекция-визуализация и проблемные с компьютерными презентациями;
- семинары: выполнение расчетно-графического задания, опрос, контрольная работа, тест и дискуссия;
- групповая работа: решение задач по разработке вариантов управленческих решений.

В ходе обучения применяются следующие формы учебного процесса: лекции и практические занятия, самостоятельная внеаудиторная работа. В качестве метода проверки знаний будет практиковаться устный опрос студентов, написание контрольных работ по предложенным темам, письменные ответы на предложенные задачи и ситуации.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Реализация активных, инновационных образовательных технологий, которые способствуют развитию компетенций, обучающихся приведены в таблице.

№ темы	Вид занятия (Л, ПР, ЛР), тема занятия	Используемые интерактивные образовательные технологии	Количество часов	
			ОФО	ЗФО
1	Л. Концептуальная модель информационной безопасности	Мультимедийные презентации	2	-
2	Л. Угрозы конфиденциальной информации	Интерактивная лекция	2	2
3	Л. Характеристика основных способов защиты информации	Интерактивная лекция	2	2
4	ПР. Основные способы пресечения разглашения конфиденциальной информации	Групповая дискуссия	2	2
5	ЛР. Структура и функции службы безопасности предприятия	Разбор конкретных ситуаций	2	-
6	ЛР. Комплексный проект системы информационной безопасности	Кейс-задача	2	
7	ЛР. Анализ рисков утечки конфиденциальной информации	Кейс-задача	2	
8	ЛР Анализ рисков утечки конфиденциальной информации	Кейс-задача	2	2
9	ЛР Организация защиты информации с помощью пароля	Кейс-задача	4	2
<i>Всего:</i>			20 час. (40 %)	10 час. (71%)

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

4.1 Фонд оценочных средств для проведения текущей аттестации

Темы для самостоятельного изучения

Наименование темы	Количество часов	
	ОФО	ЗФО
Защита информационных процессов в компьютерных системах	4	8
Основные угрозы информации в компьютерных системах	6	10
Анализ целей и возможностей злоумышленника в компьютерной сети	4	8
Специфика возникновения угроз в открытых сетях	6	10
Системные вопросы защиты программ и данных	6	10
Требования к защите автоматизированных информационных систем от НСД	4	8
Основные категории требований к программной и программно-аппаратной реализации средств защиты информации	4	8
Концепция защиты информации в государственных и коммерческих структурах	6	10
Методы информационной борьбы на международном уровне	4	8
Информационно-манипулятивные технологии	5	10
<i>Всего</i>	49	90

Темы рефератов

№ п/п	Темы
1.	Государственная политика в области информатизации и развития информационного общества в России.
2.	Правовые основы менеджмента информационной безопасности.
3.	Правовые основы лицензирования программного обеспечения.
4.	Правовое регулирование информационных услуг.
5.	Лицензионная деятельности в области защиты информации .
6.	Правовое регулирование государственной системы управления открытыми ключами.
7.	Правовое регулирование использования программно-аппаратных средств защиты информации.
8.	Правовое регулирование защиты информации с использованием инженерно-технических средств защиты информации .
9.	Технологии облачных вычислений: понятие и перспективы использования с точки зрения информационной безопасности.
10.	Правовые основы проведения аудита информационной безопасности.
11.	Правовые основы функционирования официальных сайтов государственных органов и организаций .
12.	Правовые регулирования работы с персональными данными граждан РФ.
13.	Правовые основы использования криптографических средств защиты информации \.
14.	Открытые данные («Open data»): понятие и перспективы использования.
15.	Большие данные («Big data»): понятие и перспективы использования.
16.	Правовые основы защиты объектов интеллектуальной собственности в сети Интернет.
17.	Правовые основы использования технических средств защиты авторского права и смежных прав.

Критерии оценки:

Рефераты оцениваются по пятибалльной шкале с использованием следующих критериев:

– оценка «отлично» ставится, если в докладе студент полностью раскрыл заявленную тему, содержание доклада отражает современный уровень науки и практики в предметной области; использовано не менее 10 разнообразных библиографических источников; причем среди них не менее половины опубликованы за последние 5 лет; среди источников обязательно присутствуют 3-4 статьи из рецензируемых научных журналов; в процессе доклада студент показал полное владение материалом, ответил на дополнительные и уточняющие вопросы;

– оценка «хорошо» ставится, если в докладе заявленная тема в целом раскрыта, но не отражены некоторые аспекты, содержание реферата отражает современный уровень науки и практики в предметной области доклада; студент использовал 7-10 разнообразных библиографических источников; причем среди них не менее половины опубликованы за последние 5 лет; среди источников присутствуют 1-2 статьи из рецензируемых научных журналов; в процессе доклада студент показал достаточно высокий уровень владения материалом, но затруднялся в ответах на некоторые дополнительные вопросы;

– оценка «удовлетворительно» ставится, если в докладе заявленная раскрыта не полностью, упущены некоторые важные аспекты; студент использовал более 5 библиографических источников, но среди них большая часть старше 5 лет; среди источников нет статей из рецензируемых научных журналов; при докладе студент показал неуверенное владение материалом, затруднялся в ответах на дополнительные вопросы;

– оценка «неудовлетворительно» ставится, если в докладе заявленная тема не раскрыта или раскрыта очень слабо; уровень научных и практических знаний, отраженный в тексте, существенно отстает от современного; студент использовал менее 5 библиографических источников или большая часть источников старше 5 лет; среди источников нет статей из рецензируемых научных журналов; в процессе доклада студент показал слабое владения материалом, не смог ответить на дополнительные или уточняющие вопросы.

4.2. Фонд оценочных средств для проведения промежуточной аттестации

Перечень вопросов, выносимых на зачет по учебной дисциплине

«Информационная безопасность и защита информации»

1. Теория и методология информационной безопасности, ее основные понятия.
2. Информационная безопасность в системе национальной безопасности России.
3. Национальные интересы РФ в информационной сфере.
4. Угрозы национальной безопасности в информационной сфере и их источники.
5. Понятие информации, ее виды и критерии оценки. Задачи, методы и средства защиты информации.
6. Понятие уязвимости и угрозы информации.
7. Источники утраты конфиденциальности и искажения информации.
8. Понятие и виды информационных ресурсов. Информационные ресурсы государственного значения.
9. Понятие конфиденциальности. Критерии выделения информации ограниченного распространения.
10. Особенности документирования конфиденциальной информации.
11. Понятие и методы информационно-аналитической работы. Цели, задачи и организация информационно-аналитической работы на объекте по обеспечению информационной безопасности.
12. Основы проведения аналитических исследований.
13. Легальные способы получения полезной информации.
14. Классификация противоправных способов получения конфиденциальной информации. Понятие шпионажа и его виды.
15. Понятие информационного противоборства, его формы и методы.
16. Понятие информационного права. Предмет, методы и принципы информационного права.

17. Система информационного права. Подотрасли и институты информационного права. Информационно-правовые отношения.
18. Законодательство РФ в области информационной безопасности и защиты информации.
19. Правовые способы обеспечения защиты информации.
20. Лицензионная и сертификационная деятельность в области защиты информации.
21. Юридическая ответственность в области информационных отношений и ее виды.
22. Понятие преступления в информационной сфере. Характеристика основных составов преступлений, связанных с информационными отношениями.
23. Правовой режим государственной тайны, служебной тайны.
24. Международное сотрудничество в области информационной безопасности и защиты информации.
25. Правовой режим коммерческой тайны.
26. Профессиональные тайны как вид информации ограниченного распространения, особенности их правового режима.
27. Особенности правового режима персональных данных, обеспечение тайны переписки, телефонных переговоров и иных сообщений.
28. Понятие и правовой режим персональных данных.
29. Понятие и виды организационных мер обеспечения информационной безопасности и защиты информации.
30. Анализ и оценка угроз информационной безопасности объекта.
31. Организация обеспечения режима конфиденциальности на объекте.
32. Регламентация допуска и доступа персонала к конфиденциальной информации.
33. Служба безопасности, её структура и задачи по обеспечению информационной безопасности.
34. Задачи и способы подбора персонала на работу, связанную с использованием конфиденциальной информации.
35. Организация работы с персоналом, допущенным к конфиденциальной информации.
36. Предупредительные и профилактические меры, направленные на предотвращение разглашения персоналом конфиденциальной информации.
37. Организация защиты информации при подготовке и проведении совещаний.
38. Организация защиты информации при проведении переговоров.
39. Защита информации в процессе научной, рекламной и выставочной деятельности.
40. Защита конфиденциальных сведений при работе с клиентами и посетителями.
41. Понятие и виды технических мер обеспечения информационной безопасности и защиты информации.
42. Виды угроз информационной безопасности, исходящих по техническим каналам.
43. Средства и методы технической защиты объектов и информации.
44. Правовое регулирование защиты информации с использованием технических средств. Регламентация использования технических средств защиты информации (вопросы лицензирования и сертификации).
45. Угрозы безопасности информации в процессе использования компьютеров, локальных сетей и средств связи.
46. Правовое регулирование информационных отношений в сети Интернет, обеспечение защиты информационных ресурсов в глобальной информационной сети.
47. Виды охраняемых объектов, категории защищаемых помещений. Задачи и направления охраны объектов.

Оценка ответа студента на проводится по 3 основным критериям:

Критерий	Оценка
В ответе раскрыта сущность основных категорий и понятий, содержащихся в вопросе, таким образом, чтобы в нем просматривался ответ на поставленный вопрос	
определены логические связи и отношения между основными категориями, обеспечивающие полное раскрытие смысла ответа на поставленный вопрос	
приведены примеры из практической деятельности, иллюстрирующие ответ на поставленный вопрос	

Каждый критерий оценивается по шкале от 0 до 2 баллов, где:

0 – содержание доклада не удовлетворяет данному критерию

1 – содержание доклада частично удовлетворяет данному критерию

2 – содержание доклада в полной мере удовлетворяет данному критерию

Оценки по всем критериям суммируются и определяется итоговая оценка за доклад:

- оценка «зачтено» выставляется студенту, если он набрал от 3 до 6 баллов;

- оценка «не зачтено» выставляется студенту, если он набрал менее 3 баллов;

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1 Основная литература

№ п.п.	Автор, название, место издания, издательство, год издания учебной литературы, к-во страниц, вид и характеристика иных информационных ресурсов	Кол-во экз. в библиотеке факультета	Электронный ресурс размещен на
1	Нестеров, С. А. Информационная безопасность [Электронный ресурс]: учебник и практикум для академического бакалавриата / С. А. Нестеров. - М.: Юрайт, 2017. - 321 с.		https://www.biblionline.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7
2	Баранова, Е.К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - М.: РИОР: ИНФРА-М, 2017. - 322 с.		http://znanium.com/catalog.php?bookinfo=763644
3	Бачило, И.Л. Информационное право: учебник для магистров: учебник для студентов вузов, обучающихся по юридическим направлениям и специальностям. - 3-е изд., перераб. и доп. - М.: Юрайт, 2012. - 564 с.	7	

5.2 Дополнительная литература

№ п.п.	Автор, название, место издания, издательство, год издания учебной литературы, к-во страниц, вид и характеристика иных информационных ресурсов	Кол-во экз. в библиотеке факультета	Электронный ресурс размещен на
1	Партыка, Т. Л. Информационная безопасность [Электронный ресурс]: учебное пособие / Т. Л. Партыка, И. И. Попов. - 5-е изд., перераб. и доп. - Москва: ФОРУМ: ИНФРА-М, 2016. - 432 с.		http://znanium.com/bookread2.php?book=516806
2	Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие для студентов / Ю. А. Родичев. - СПб. [и др.]: ПИТЕР, 2008. - 272 с.	14	
3	Мельников В.П. Информационная безопасность и защита информации: учебное пособие для студентов вузов / В.П. Мельников, С.А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 5-е изд., стер. М.: Академия, 2011.	26	
4	Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности. М.: Издательство "Горячая линия-Телеком", 2012.	–	https://e.lanbook.com/book/5163#book_name

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

6. Перечень ресурсов информационно-телекоммуникационной сети «интернет», необходимых для освоения дисциплины

Портал: Технологии корпоративного управления. URL: iteam.ru

КиберЛенинка - URL: <http://cyberleninka.ru>.

Научная электронная библиотека URL: <http://elibrary.ru>.

7. Методические указания для обучающихся по освоению дисциплины

Курс предусматривает занятия в компьютерном классе, подключенном к Интернету с установленным специализированным программным обеспечением. Предусмотрены лекции, практические занятия в виде выполнения практических заданий по работе со знаниями.

Для эффективного изучения практической части дисциплины настоятельно рекомендуется:

– систематически выполнять подготовку к практическим занятиям по предложенным преподавателем темам;

– своевременно выполнять и защищать практические задания.

Самостоятельная работа студента - один из важнейших этапов в подготовке специалистов. Она приобщает студентов к исследовательской работе, обогащает опытом и знаниями, необходимыми для дальнейшего их становления как специалистов, прививает навыки работы с литературой.

Цель самостоятельной работы - систематизация, закрепление и расширение теоретических и практических знаний с использованием современных информационных

технологий и литературных источников. Для развития навыков самостоятельной работы студентами во время самостоятельной работы выполняются:

- эссе по проблемам современных технологий информационной безопасности;
- домашние задания по поиску в Интернете информации на заданную научную тему и подготовке доклада.

- доклады, связанные с правовыми аспектами использования электронных документов, охраной интеллектуальной собственности;

Эссе или доклад готовится студентом самостоятельно, в нём обобщаются теоретические материалы по исследуемой теме с использованием материалов из общетехнической и специальной литературы, нормативно-правовых документов, стандартизирующих рассматриваемую сферу. В содержании доклада должен быть собственный анализ и критический подход к решению проблемы по выбранной теме исследования. Материалы должны быть изложены на высоком теоретическом уровне, с применением практических данных, примеров.

Студентам рекомендуется непрерывно проводить научные исследования под руководством преподавателя кафедры по избранной теме и готовить сообщения на научные конференции, статьи в Сборник молодых исследователей и научные журналы.

Обучение студентов с ограниченными возможностями организуется в соответствии с требованиями «Методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего профессионального образования» от «8» апреля 2014 г.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1 Перечень необходимого программного обеспечения

- Microsoft Word 2010 или более поздний;
- Операционная система Windows 7/8;
- Средство чтения PDF-файлов Adobe Acrobat или аналог.

8.2 Перечень необходимых информационных справочных систем

Справочно-правовая система «КонсультантПлюс».

Справочно-правовая система «Гарант»

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, ноутбук) и соответствующим программным обеспечением (ПО): 417А, 409, 415А
2.	Семинарские занятия	Учебная аудитория

3.	Лабораторные занятия	Компьютерный класс (ауд. 401Н, 402Н): 15 учебных мест с выходом в сеть Интернет и с программным обеспечением на сервере
4.	Групповые (индивидуальные) консультации	Аудитория 415А, 412, 413
5.	Текущий контроль, промежуточная аттестация	Аудитория 417А, 412, 413
6.	Самостоятельная работа	Читальный зал для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета