Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И ДИЗАЙНА»

УТВЕРЖДАЮ
Первый проректор, проректор по учебной работе

_____ А.Е. Рудин

«30» июня 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.28	Организационное и правовое обеспечение информационной безопасности
(Индекс дисциплины)	*(Наименование дисциплины)*

Кафедра: 20 Интеллектуальных систем и защиты информации
Код *Наименование кафедры*

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем (в коммерческих структурах)

Уровень образования: **Бакалавриат**

План учебного процесса

Составляющие учебного процесса		Очное обучение	Очно-заочное обучение	Заочное обучение
Контактная работа обучающихся с преподавателем по видам учебных занятий и самостоятельная работа обучающихся (часы)	Всего	108		
	Аудиторные занятия	40		
	Лекции	20		
	Лабораторные занятия			
	Практические занятия	20		
	Самостоятельная работа	68		
	Промежуточная аттестация			
Формы контроля по семестрам (номер семестра)	Экзамен			
	Зачет	8		
	Контрольная работа			
	Курсовой проект (работа)			
Общая трудоемкость дисциплины (зачетные единицы)		3		

Форма обучения:	Распределение зачетных единиц трудоемкости по семестрам											
	1	2	3	4	5	6	7	8	9	10	11	12
Очная								3				
Очно-заочная												
Заочная												

Санкт-Петербург
2020

Программа государственной итоговой аттестации составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по соответствующему направлению подготовки

и на основании учебного плана № 1/1/704

1. ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1. Место преподаваемой дисциплины в структуре образовательной программы

Блок 1:	Базовая	X	Обязательная	X	Дополнительно является факультативом
	Вариативная		По выбору		

1.2. Цель дисциплины

Целью изучения дисциплины является развитие делового и логического мышления студентов, ознакомление студентов с основами теории, необходимыми для решения прикладных задач создания документов и управления документооборотом организаций.

1.3. Задачи дисциплины

- изучение основных вопросов современной теории подготовки, обработки и документооборота;
- изучение основ документоведения;
- воспитание делового и логического мышления на примере решения задач создания и принципов организации документоведения.

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

Код компетенции	Формулировка компетенции	Этап формирования
ОК-4	способность использовать основы правовых знаний в различных сферах деятельности	Второй
Планируемые результаты обучения Знать: Структуру государственной системы обеспечения информационной безопасности Уметь: анализировать, толковать и правильно применять правовые нормы Владеть: навыками работы с правовыми актами, договорной документацией		
ОПК-5	Способность использовать нормативные правовые акты в профессиональной деятельности	Второй
Планируемые результаты обучения Знать: Основы организации защиты государственной тайны и конфиденциальной информации Уметь: использовать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации Владеть: Навыками работы с правовыми основами организации защиты государственной тайны и конфиденциальной информации		
ПК- 8	Способность оформлять рабочую документацию с учетом действующих нормативных и методических документов	Второй
Планируемые результаты обучения Знать : Нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации Уметь : применять методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов Владеть : Опытом работы с методиками проверки защищенности объектов информатизации на соответствие нормам информационной безопасности		

1.5. Дисциплины (практики) образовательной программы, в которых было начато формирование компетенций, указанных в п.1.4:

- Правоведение (ОК-4)
- Основы информационной безопасности (ОПК-5, ПК-8)
- Информационные системы (ПК-8)

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Общие понятия правовых основ ИБ			
Тема 1. Конституционные гарантии прав граждан на информацию и механизм их реализации. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации. Конституция Российской Федерации (статьи 24 и 29). Законодательное регулирование вопросов обеспечения информационной безопасности. Субъекты законодательной инициативы. Процесс превращения законопроекта в закон. Законы Российской Федерации «О безопасности», «О государственной тайне», «Об информации, информационных технологиях и о защите информации», «О персональных данных».	6		
Тема 2. Окинавская хартия глобального информационного общества от 22 июля 2000 года. Электронная торговля. Электронное образование, дистанционные образовательные технологии. Болонское соглашение от 19 сентября 2003 года (бакалавр, магистр, доктор философии). Электронное правительство. Рекомендации Совета Европы № 2 и № 3 от 28 февраля 2001 года (безвозмездный доступ к правовым актам, земельный кадастр и регистр населения, судебный процесс через Интернет). Информационная безопасность (информационное оружие, информационная война).	7		
Тема 3. Понятие и виды защищаемой информации по законодательству РФ. Конфиденциальная информация: персональные данные, служебная тайна, профессиональная тайна, коммерческая тайна, тайна следствия и другие виды тайн. Указы Президента Российской Федерации «О концепции национальной безопасности», «Перечень сведений, отнесенных к государственной тайне». «Вопросы Межведомственной комиссии по защите государственной тайны». Постановления Правительства Российской Федерации. Нормативные документы Межведомственной комиссии по защите государственной тайны в Российской Федерации, ФСТЭК, МВД, ФСБ и др.	7		
Тема 4. Правовой режим защиты государственной тайны. Государственная тайна как особый вид защищаемой информации. Система защиты государственной тайны. Отнесение сведений к государственной тайне, их засекречивание и рассекречивание, допуск к государственной тайне, контроль за состоянием ее защиты, юридическая ответственность за нарушение режимных требований. Нормативно-техническая документация по порядку учета, хранения и перемещения	7		
Тема 5. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации. Основы трудового права. Трудовой договор (контракт) как особый вид договорных отношений. Предмет и стороны контракта. Содержание и основания для прекращения трудовых договорных отношений. Регулирование вопросов обеспечения сохранности информации с ограниченным доступом.	6		
Тема 6. Основы организации работ по защите информации при сотрудничестве с зарубежными странами. Требования нормативных актов, регламентирующих посещение режимных предприятий иностранными специалистами; проведение международных мероприятий научно-технического и экономического сотрудничества.	6		

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Тема 7. Правовая регламентация лицензионной и сертификационной деятельности в области защиты информации, в том числе государственной тайны. Правовые основы и государственная система лицензирования и сертификации в области защиты информации. Порядок проведения экспертизы, аттестации и сертификации испытаний. Органы, уполномоченные на ведение лицензионной деятельности.	7		
Текущий контроль 1 (опрос)	3		
Учебный модуль 2. Правовые основы ИБ в Российской Федерации			
Тема 8. Уголовный кодекс Российской Федерации. Статья 146. Нарушение авторских и смежных прав. Статья 272. Неправомерный доступ к компьютерной информации. Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ. Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.	7		
Тема 9. Гражданский кодекс РФ (часть 4). Защита интеллектуальной собственности средствами авторского права. Экономические аспекты защиты информации и охраны интеллектуальной собственности. Критерии эффективности «затраты – надежность». Особенности страхования информационных рисков.	7		
Тема 10. Кодекс РФ об административных правонарушениях. Статья 7.12. Нарушение авторских и смежных прав, изобретательских и патентных прав. Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных). Статья 13.12. Нарушение правил защиты информации. Статья 13.13. Незаконная деятельность в области защиты информации	7		
Тема 11. Правовая регламентация охранной деятельности. Правовые основы деятельности служб безопасности. Основные положения закона «О частной детективной и охранной деятельности». Задачи и элементы структуры служб безопасности.	6		
Тема 12. Экспертиза преступлений в области компьютерной информации. Криминалистические аспекты проведения расследований. Информация как криминалистический объект. Криминалистическая характеристика преступлений в сфере компьютерной информации, методика расследования, механизмы следообразования.	6		
Тема 13. Правовые основы обеспечения информационно-психологической безопасности. Информационно-психологическая безопасность. Виды «вредной» информации. Спам, диффамация и клевета. Правовое регулирование в сфере информационно-психологической безопасности. Основы психологической устойчивости при работе в экстремальных условиях. Основы психофизиологического тестирования.	6		
Тема 14. Правовые основы электронного документооборота Порядок и механизмы его реализации. Федеральный закон РФ № 1 от 10.01.2002 «Об электронной цифровой подписи». Государственные автоматизированные системы «Выборы» и «Правосудие».	7		
Тема 15. Правовые основы функционирования электронных платежных систем. Правовое обеспечение информационной безопасности межбанковских расчетов юридических лиц и кредитных пластиковых карточек физических лиц.	7		
Текущий контроль 2 (опрос)	3		
Промежуточная аттестация по дисциплине (зачет с оценкой)	**3**		
ВСЕГО:	**108**		

3. ТЕМАТИЧЕСКИЙ ПЛАН

3.1. Лекции

Номера	Очное обучение	Очно-заочное обучение	Заочное обучение

изучаемых тем	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	8	2				
2	8	2				
3	8	1				
4	8	1				
5	8	2				
6	8	1				
7	8	1				
8	8	1				
9	8	1				
10	8	2				
11	8	1				
12	8	1				
13	8	1				
14	8	1				
15	8	2				
	ВСЕГО:	20				

3.2. Практические и семинарские занятия

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	Конституционные гарантии прав граждан на информацию и механизм их реализации. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации (семинар)	8	2				
2	Окинавская хартия глобального информационного общества от 22 июля 2000 года (семинар)	8	2				
3	Понятие и виды защищаемой информации по законодательству РФ (семинар)	8	1				
4	Правовой режим защиты государственной тайны (семинар)	8	1				
5	Правовое регулирование взаимоотношений администрации и персонала в области защиты информации (семинар)	8	2				
6	Основы организации работ по защите информации при сотрудничестве с зарубежными странами (семинар)	8	1				
7	Правовая регламентация лицензионной и сертификационной деятельности в области защиты информации, в том числе государственной	8	1				

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
	тайны (семинар)						
8	Уголовный кодекс Российской Федерации (семинар)	8	1				
9	Гражданский кодекс РФ (часть 4) (семинар)	8	1				
10	Кодекс РФ об административных правонарушениях (семинар)	8	2				
11	Правовая регламентация охранной деятельности (семинар)	8	1				
12	Экспертиза преступлений в области компьютерной информации (семинар)	8	1				
13	Правовые основы обеспечения информационно-психологической безопасности (семинар)	8	1				
14	Правовые основы электронного документооборота (семинар)	8	1				
15	Правовые основы функционирования электронных платежных систем (семинар)	8	2				
		ВСЕГО:	20				

3.3. Лабораторные занятия

Не предусмотрено

4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

НЕ ПРЕДУСМОТРЕНО

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ ОБУЧАЮЩЕГОСЯ

Номера учебных модулей, по которым проводится контроль	Форма контроля знаний	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Кол-во	Номер семестра	Кол-во	Номер семестра	Кол-во
1	Опрос	8	1				
2	Опрос	8	1				

6. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

Виды самостоятельной работы обучающегося	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
Усвоение теоретического материала	8	31				
Подготовка к практическим занятиям	8	34				
Подготовка к зачету	8	3				
	ВСЕГО:	68				

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

7.1. Характеристика видов и используемых инновационных форм учебных занятий

Наименование видов учебных занятий	Используемые инновационные формы	Объем занятий в инновационных формах (часы)		
		очное обучение	очно-заочное обучение	заочное обучение
Лекции	Проблемная лекция, разбор конкретных ситуаций, лекция-диалог	5		
Практические и семинарские занятия	Диспут, дискуссия	5		
	ВСЕГО:	10		

7.2. Балльно-рейтинговая система оценивания успеваемости и достижений обучающихся

Перечень и параметры оценивания видов деятельности обучающегося

№ п/п	Вид деятельности обучающегося	Весовой коэффициент значимости, %	Критерии (условия) начисления баллов
1	Аудиторная активность: посещение лекций и практических (семинарских) занятий, прохождение промежуточного опроса	50	• 3 балла за каждое занятие (всего 20 занятий в семестре), максимум 60 баллов • 2 балла за каждый правильный ответ на вопрос опроса текущего контроля (всего 10 вопросов в опросе, два опроса в семестр), максимум 40 баллов
2	Сдача зачета	50	• Ответ на теоретический вопрос (полнота, владение терминологией, затраченное время) – максимум 40 баллов; • Решение практической задачи – до 60 баллов
	Итого (%):	100	

Перевод балльной шкалы в традиционную систему оценивания

Баллы	Оценка по нормативной шкале	
86 - 100	5 (отлично)	Зачтено
75 – 85	4 (хорошо)	
61 – 74		
51 - 60	3 (удовлетворительно)	
40 – 50		
17 – 39	2 (неудовлетворительно)	Не зачтено
1 – 16		
0		

8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Учебная литература

а) основная учебная литература

1. Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс]: учебное пособие/ А.Н. Кубанков, Н.Н. Куняев— Электрон. текстовые данные.— М.: Всероссийский государственный университет

юстиции (РПА Минюста России), 2014.— 78 с.— Режим доступа: http://www.iprbookshop.ru/47262.html.— ЭБС «IPRbooks»
2. Дроботун Н. В. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебное пособие / Дроботун Н. В. — СПб.: СПГУТД, 2014.— 110 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=1631, по паролю.

б) дополнительная учебная литература

1. Кремер А.С. Нормативно-правовые аспекты обеспечения информационной безопасности инфокоммуникационных сетей [Электронный ресурс]: учебное пособие/ А.С. Кремер— Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2007.— 97 с.— Режим доступа: http://www.iprbookshop.ru/61745.html.— ЭБС «IPRbooks»
2. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 242 с.— Режим доступа: http://www.iprbookshop.ru/62945.html.— ЭБС «IPRbooks»
3. Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Электронный ресурс]/ Н.Н. Куняев— Электрон. текстовые данные.— М.: Логос, 2015.— 348 с.— Режим доступа: http://www.iprbookshop.ru/51638.html.— ЭБС «IPRbooks»
4. Босхамджиева Н.А. Административно-правовые основы обеспечения общественной безопасности в Российской Федерации [Электронный ресурс]: монография/ Н.А. Босхамджиева— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 248 с.— Режим доступа: http://www.iprbookshop.ru/66249.html.— ЭБС «IPRbooks»
5. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс]: монография/ А.А. Смирнов— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 159 с.— Режим доступа: http://www.iprbookshop.ru/52524.html.— ЭБС «IPRbooks»

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

1. Дроботун Н. В. Управление информационной безопасностью [Электронный ресурс]: учебное пособие / Дроботун Н. В., Серова Н. Е. — СПб.: СПГУТД, 2014.— 142 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=2018, по паролю.
2. Защита информации и информационная безопасность [Электронный ресурс]: методические указания / Сост. Бусыгин К. Н., Васильева Е. К., Дружкина Ю. Д. — СПб.: СПГУТД, 2016.— 32 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=3007, по паролю.
3. Штеренберг С. И. Информационная безопасность. Стеганография [Электронный ресурс]: учебное пособие / Штеренберг С. И. — СПб.: СПбГУПТД, 2017.— 76 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=201733, по паролю.
4. Спицкий, С. В. Эффективная аудиторная и самостоятельная работа обучающихся: методические указания / С. В. Спицкий. – СПб.: СПбГУПТД, 2015. – Режим доступа: http://publish.sutd.ru/tp_get_file.php?id=2015811, по паролю.
5. Караулова, И. Б. Организация самостоятельной работы обучающихся / И. Б. Караулова, Г. И. Мелешкова, Г. А. Новоселов. – СПб.: СПГУТД, 2014. – 26 с. – Режим доступа http://publish.sutd.ru/tp_get_file.php?id=2014550, по паролю

8.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины

1 http://www.iprbookshop.ru
2 http://publish.sutd.ru/

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем *(при необходимости)*

1. Microsoft Office Standart 2016 Russian Open No Level Academic)
2. Microsoft Windows 10 Home Russian Open No Level Academic Legalization Get Genuine (GGK) + Microsoft Windows 10 Professional (Pro – профессиональная) Russian Upgrade Open No Level Academic

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

1 стандартно оборудованная аудитория
2 компьютер

8.6. Иные сведения и (или) материалы

Компьютерные презентации, каталоги, модели

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
Лекции	• проработка рабочей программы в соответствии с целями и задачами, структурой и содержанием дисциплины; • конспект лекций: кратко, схематично, последовательно фиксировать основные положения, выводы и формулировки; помечать важные мысли, выделять ключевые слова, термины. • Проверка терминов, понятий: осуществлять с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь; • работа с теоретическим материалом (конспектирование источников): найти ответ на вопросы в рекомендуемой литературе.
Практические занятия	• подготовка ответов к контрольным вопросам, опросам; • решение задач по алгоритму, решение кейсов
Самостоятельная работа	Следует предварительно изучить методические указания по выполнению самостоятельной работы, курсовой работы (проекта), контрольной работы (можно указать реквизиты изданий и электронный ресурс, где они находятся). При подготовке к экзамену (зачету) необходимо ознакомиться с демонстрационным вариантом задания (теста, перечнем вопросов, пр.), проработать конспекты лекций и практических занятий, рекомендуемую литературу, получить консультацию у преподавателя, подготовить презентацию материалов.

10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

10.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

10.1.1. Показатели оценивания компетенций на этапах их формирования

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
ОК-4	Раскрывает основные элементы государственной системы обеспечения информационной безопасности, их сущность, принципы функционирования и взаимодействия принимает решения и совершать юридические действия в области защиты информации в точном соответствии с законом Осуществляет поиск информации с помощью правовых информационно-поисковых и информационно-справочных систем и баз данных, используемых в профессиональной деятельности	Вопросы для устного собеседования Практическое задание Практическое задание	Перечень вопросов для устного собеседования (30 вопросов) Перечень практических заданий (6 заданий)
ОПК-5	Описывает правовой режим защиты государственной тайны и информации конфиденциального характера Применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем Пользуется нормативными документами по защите информации	Вопросы для устного собеседования Практическое задание Практическое задание	Перечень вопросов для устного собеседования (30 вопросов) Перечень практических заданий (6 заданий)
ПК-8	Определяет задачи органов защиты государственной тайны и служб защиты информации на предприятиях Формирует правила, процедуры, комплекс мер по организационно-правовому обеспечению информационной безопасности	Вопросы для устного собеседования Практическое задание	Перечень вопросов для устного собеседования (30 вопросов) Перечень

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
	Применяет комплексный подход к правовому обеспечению информационной безопасности в различных сферах деятельности.	Практическое задание	практических заданий (6 заданий)

10.1.2. Описание шкал и критериев оценивания сформированности компетенций

Критерии оценивания сформированности компетенций

Баллы	Оценка по традиционной шкале	Критерии оценивания сформированности компетенций
		Устное собеседование
86 - 100	5 (отлично)	Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу. Качество исполнения всех элементов задания полностью соответствует всем требованиям. Учитываются баллы, накопленные в течение семестра.
75 – 85	4 (хорошо)	Ответ полный, основанный на проработке всех обязательных источников информации. Подход к материалу ответственный, но стандартный. Учитываются баллы, накопленные в течение семестра.
61 – 74		Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки. Учитываются баллы, накопленные в течение семестра.
51 - 60	3 (удовлетво-рительно)	Ответ воспроизводит в основном только лекционные материалы, без самостоятельной работы с рекомендованной литературой. Демонстрирует понимание предмета в целом, без углубления в детали. Присутствуют существенные ошибки или пробелы в знаниях по некоторым темам. Учитываются баллы, накопленные в течение семестра.
40 – 50		Ответ неполный, основанный только на лекционных материалах. При понимании сущности предмета в целом – существенные ошибки или пробелы в знаниях сразу по нескольким темам, незнание (путаница) важных терминов. Учитываются баллы, накопленные в течение семестра.
17 – 39	2 (неудовлетво-рительно)	Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки. Не учитываются баллы, накопленные в течение семестра.
1 – 16		Непонимание заданного вопроса. Неспособность сформулировать хотя бы отдельные концепции дисциплины. Не учитываются баллы, накопленные в течение семестра.
0		Попытка списывания, использования неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки). Не учитываются баллы, накопленные в течение семестра.

10.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

10.2.1. Перечень вопросов (тестовых заданий), разработанный в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировка вопросов	№ темы
1	Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации.	1
2	Субъекты законодательной инициативы. Процесс превращения законопроекта в закон. Законы Российской Федерации «О безопасности».	1
3	Окинавская хартия глобального информационного общества от 22 июля 2000 года.	2
4	Электронная торговля. Электронное образование, дистанционные образовательные технологии. Болонское соглашение от 19 сентября 2003 года (бакалавр, магистр, доктор философии). Электронное правительство.	2
5	Информационная безопасность (информационное оружие, информационная война).	3
6	Конфиденциальная информация: персональные данные, служебная тайна, профессиональная тайна, коммерческая тайна, тайна следствия и другие виды тайн.	3
7	Нормативные документы Межведомственной комиссии по защите государственной тайны в Российской Федерации, ФСТЭК, МВД, ФСБ и др.	4

8	Государственная тайна как особый вид защищаемой информации. Система защиты государственной тайны. Отнесение сведений к государственной тайне, их засекречивание и рассекречивание, допуск к государственной тайне, контроль за состоянием ее защиты, юридическая ответственность за нарушение режимных требований.	4
9	Нормативно-техническая документация по порядку учета, хранения и перемещения.	5
10	Правовое регулирование взаимоотношений администрации и персонала в области защиты информации	5
11	Понятие и виды защищаемой информации по законодательству РФ	6
12	Требования нормативных актов, регламентирующих посещение режимных предприятий иностранными специалистами; проведение международных мероприятий научно-технического и экономического сотрудничества.	6
13	Регулирование вопросов обеспечения сохранности информации с ограниченным доступом	7
14	Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни	7
15	Правовые основы и государственная система лицензирования и сертификации в области защиты информации.	8
16	Правовая регламентация лицензионной и сертификационной деятельности в области защиты информации, в том числе государственной тайны.	8
17	Неправомерный доступ к компьютерной информации.	9
18	Создание, использование и распространение вредоносных программ для ЭВМ.	9
19	Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.	10
20	Нарушение авторских и смежных прав.	10
21	Защита интеллектуальной собственности средствами авторского права.	11
22	Нарушение авторских и смежных прав, изобретательских и патентных прав.	11
23	Правовые основы деятельности служб безопасности. Основные положения закона «О частной детективной и охранной деятельности». Задачи и элементы структуры служб безопасности.	12
24	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).	12
25	Незаконная деятельность в области защиты информации.	13
26	Нарушение правил защиты информации.	13
27	Правовые основы электронного документооборота.	14
28	Правовая регламентация охранной деятельности	14
29	Правовые основы функционирования электронных платежных систем	15
30	Правовое обеспечение информационной безопасности межбанковских расчетов юридических лиц и кредитных пластиковых карточек физических лиц.	15

Вариант тестовых заданий, разработанных в соответствии с установленными этапами формирования компетенций

10.2.2. Перечень тем докладов *(рефератов, эссе, пр.)***, разработанных в соответствии с установленными этапами формирования компетенций**

Не предусмотрено

Вариант типовых заданий (задач, кейсов), разработанных в соответствии с установленными этапами формирования компетенций

№ п/п	Условия типовых задач (задач, кейсов)	Ответ
1	Желая помочь своим коллегам, программист Сальников и адвокат Сабуров - работники нотариальной конторы «ОКС» - внесли изменения в программу «Акты и документы о недвижимости». В результате этих действий была уничтожена информация, касающаяся опыта работы конторы в области регистрации недвижимости за последний год и нарушена работа ПК. Руководитель нотариальной конторы обратился к прокурору с заявлением о возбуждении уголовного дела против Сальникова и Сабурова. Есть ли в действиях Сальникова и Сабурова состав преступления?	Согласно норме п. 1 ст. 273 УК РФ , создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. Те же деяния, повлекшие по неосторожности тяжкие последствия, наказываются лишением свободы на срок до семи лет (п. 2 ст. 273 УК РФ).
2	Программист Голанов поступая в фирму «Сокол», формально отнесся к заполнению документов по типовым формам, предложенным руководством фирмы. В течение двух лет Голанов	Прав Валентинов. Согласно ст. 1296 ГК РФ, в случае, когда программа для ЭВМ или база данных создана по договору, предметом которого было ее создание (по заказу), исключительное право на такую программу или такую базу данных принадлежит заказчику, если

	создал ряд программных продуктов, реализация которых принесла фирме «Сокол» значительную прибыль и известность в республике. Видя это, Голанов обратился к руководству фирмы с просьбой выплатить ему денежное вознаграждение как автору программ, обеспечивших заметный успех коллективу. Однако генеральный директор фирмы Валентинов, ссылаясь на регулярную выплату заявителю высокого должностного оклада, отказался удовлетворить его просьбу. При этом он заявил, что свои программы Голанов создал в служебное время и, кроме того, программист не осуществил регистрацию программ в установленном законом порядке. Прав Голанов или Валентинов?	договором между подрядчиком (исполнителем) и заказчиком не предусмотрено иное. Автор созданных по заказу программы для ЭВМ или базы данных, которому не принадлежит исключительное право на такую программу или такую базу данных, имеет право на вознаграждение в соответствии с абзацем третьим пункта 2 статьи 1295 ГК РФ.
3	Администрация фирмы «Свет» поручила своему программисту Алексееву, работавшему по трудовому договору, создать базу данных для учета материальных ценностей предприятия. В целях быстрейшего выполнения поставленной задачи программист использовал некоторые типовые разработки своих знакомых коллег, работавших в других организациях. В результате установки данных программ на ПК в компьютер был внесен вирус. Помимо этого, по истечении некоторого времени на ПК был установлен факт уничтожения базы данных в результате действия вируса. В итоге фирме «Свет» пришлось закупать новую базу данных, в результате чего она понесла убытки. Администрация предприятия, рассмотрев сложившуюся ситуацию, наложила на Алексеева штраф в размере трёх месячных окладов и лишила его премии. Программист написал жалобу в прокуратуру, требуя отмены решения руководства фирмы и снятия с него всех обвинений. Имеются ли здесь нарушения законодательства об информации, информационных технологиях и защите информации?	Да, нарушения законодательства об информации, информационных технологиях и защите информации имеются. Администрация фирмы «Свет» права. Непосредственным объектом преступления, предусмотренного ст. 274 УК РФ , признаются общественные отношения, обеспечивающие правильную и безопасную эксплуатации ЭВМ, системы ЭВМ или их сети. Предмет преступления - охраняемая законом компьютерная информация. Объективная сторона характеризуется нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшим уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред. Под правилами эксплуатации ЭВМ, системы ЭВМ или их сети (компьютерной системы) понимаются правила, установленные компетентным государственным органом, или технические правила, установленные соответствующими лицами, которыми могут быть изготовители ЭВМ, разработчиками компьютерных программ, их законные владельцы и др., определяющие порядок работы с ЭВМ (нормативные акты, инструкции, правила, техническое описание, положение, приказы и т.д.). Существенный вред - понятие оценочное, зависит от конкретных значимых для дела обстоятельств, например, от важности и ценности информации для гражданина, общества, государства, размер материального ущерба в результате уничтожения информации, объем повреждения, блокирования, модификации ЭВМ, системы ЭВМ или их сети и т.д. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет. В части 2 ст. 274 УК РФ предусмотрен квалифицированный вид состава - совершение деяния, повлекшего по неосторожности тяжкие последствия. Данное понятие оценочное, но в любом случае вред должен быть выше существенного, указанного в ч. 1 ст. 274 УК РФ. Деяние, повлекшее по неосторожности тяжкие последствия, наказывается лишением свободы на срок до четырех лет.

10.3. Методические материалы,

определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности), характеризующих этапы формирования компетенций

10.3.1. Условия допуска обучающегося к сдаче *(экзамена, зачета и / или защите курсовой работы*) **и порядок ликвидации академической задолженности**

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся

10.3.2. Форма проведения промежуточной аттестации по дисциплине

устная	X	письменная		компьютерное тестирование		иная*	

**В случае указания формы «Иная» требуется дать подробное пояснение*

10.3.3. Особенности проведения зачета

Обучающийся тянет билет, в котором теоретический вопрос и задача. После этого готовится в течении как минимум 15 минут с использованием конспекта лекций и других материалов.

Обучающийся в устной форме доводит до преподавателя ответ на вопрос, при необходимости прямо во время ответа составляет необходимые схемы или диаграммы. Отвечает на сопутствующие вопросы преподавателя, которые могут выходить за рамки билетов, но в рамках изучаемого материала дисциплины. После ответа на теоретический вопрос обучающийся приступает к решению задачи, гарантированно на решение задачи времени дается 30 минут, решение формулируется с использованием конспекта лекций и иных материалов, при правильном решении задачи преподаватель задает вопросы по методам или технологиям решения, вопросы могут касаться всего материала изучаемой дисциплины.