МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Юридический факультет имени А.А. Хмырова

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования –
первый проректор
_____ Хагуров Т.А.
подпись
«_30_» _05_ 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФТД.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки 40.03.01 Юриспруденция

Направленность (профиль) гражданско-правовой

Форма обучения очная, очно-заочная, заочная .

Квалификация бакалавр

Краснодар 2025

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 40.03.01 Юриспруденция, утвержденную приказом Министерства науки и высшего образования Российской Федерации от «13» августа 2020 г. №1011.

Программу составил:

Г.А. Маркосян, доцент кафедры криминалистики и правовой информатики, к.э.н.

подпись

В.Е. Пономарев, ст. преподаватель кафедры Криминалистики и правовой информатики

подпись

Рабочая программа дисциплины «Информационная безопасность» утверждена на заседании кафедры криминалистики и правовой информатики протокол № 10 от «28» апреля 2025 г.

А.В. Руденко, заведующий кафедрой криминалистики и правовой информатики, д-р юрид. наук, профессор

подпись

Утверждена на заседании учебно-методической комиссии юридического факультета имени А.А. Хмырова протокол № 9 от «22» мая 2025 г.

Председатель УМК факультета Прохорова М.Л.

подпись

Рецензенты:

Р.Г. Мартыненко, руководитель отдела криминалистики следственного управления Следственного комитета Российской Федерации по Краснодарскому краю, полковник юстиции, кандидат юридических наук.

Н.Н. Щелочков, заместитель председателя Первомайского районного суда г.Краснодара, кандидат юридических наук.

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является формирование у учащихся знаний в области электронного документооборота, правового регулирования сети Интернет и основ информационной безопасности.

1.2 Задачи дисциплины

- Знать нормативно-правовые акты в области цифрового права
- Знать основные правила ведения электронного документооборота
- Уметь применять на практике электронные документы, в том числе с использованием электронной подписи
- Знать особенности правового регулирования сети интернет
- Знать основы информационной безопасности

В результате освоения дисциплины у студентов должны сформироваться устойчивые знания и навыки владения основными методами, способами и средствами получения, хранения, переработки информации, обладание навыками работы с компьютером как средством управления информацией; способность работать с информацией в глобальных компьютерных сетях; способность добросовестно исполнять профессиональные обязанности, соблюдать принципы этики юриста; способность повышать уровень своей профессиональной компетентности; способность применять нормативные правовые акты, реализовывать нормы материального и процессуального права в профессиональной деятельности; способность давать квалифицированные юридические заключения и консультации в конкретных видах юридической деятельности.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к части, формируемой участниками образовательных отношений Блока «Факультативные дисциплины» учебного плана.

Освоение дисциплины базируется на знаниях школьной программы алгебры и начал анализа, а также на положениях теории государства и права, информационных технологиях в юридической деятельности, которые преподаются на первом курсе, а также правовой информатики, изучаемой на третьем курсе.

Знания, навыки и умения, полученные в ходе изучения дисциплины, должны всесторонне использоваться студентами в их последующей профессиональной деятельности или дальнейшего обучения по программам магистратуры, аспирантуры.

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

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора*	Результаты обучения по дисциплине
ОПК-9 Способен принимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	

Код и наименование индикатора*	Результаты обучения по дисциплине
ИОПК-9.1 Понимает принципы работы современных информационных технологий.	**ИОПК-9.1.З-1.** Знает и понимает принципы работы современных информационных технологий.
ИОПК-9.2 Реализует принципы работы современных информационных технологий для решения задач профессиональной деятельности.	**ИОПК-9.2.У-1.** Умеет реализовывать принципы работы современных информационных технологий для решения задач профессиональной деятельности
ИОПК-9.3 Знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации.	**ИОПК-9.3.З-1** Знает современные цифровые технологии и требования цифровой безопасности, потенциальные риски в сфере цифровой безопасности
	ИОПК-9.3.У-1 Умеет применять современные цифровые технологии для обеспечения цифровой безопасности и нейтрализации рисков в сфере цифровой безопасности
ИОПК-9.4 Знание основных методов разработки искусственного интеллекта и оригинальных алгоритмов для решения задач в рамках заданной проблемной области.	**ИОПК-9.4.З-1** Знает методов разработки искусственного интеллекта и оригинальных алгоритмов
	ИОПК-9.4.У-1 Умеет решать задачи профессиональной деятельности с использованием искусственного интеллекта и оригинальных алгоритмов

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет: для ОФО - 2 зачетные единицы (72 часа), для ОЗФО - 2 зачетные единицы (72 часа), для ЗФО – 2 зачетные единицы (72 часа) для их распределения по видам работ представлено в таблице:

Виды работ	Всего часов	Форма обучения		
		очная	очно-заочная	заочная
	ОФО/ОЗФО/ЗФО	7 семестр (часы)	7 семестр (часы)	4 курс (часы)
Контактная работа, в том числе:	**36,2/30,2/14,2**	**36,2**	**30,2**	**14,2**

Аудиторные занятия (всего):		**34/28/14**	**34**	**28**	**14**
занятия лекционного типа		16/8/6	16	8	6
занятия семинарского типа (практические занятия)		18/20/8	18	20	8
Иная контактная работа:		**2,2/2,2/0,2**	**2,2**	**2,2**	**0,2**
Контроль самостоятельной работы (КСР)		2/2/-	2	2	-
Промежуточная аттестация (ИКР)		0,2/0,2/0,2	0,2	0,2	0,2
Самостоятельная работа, в том числе:		**35,8/41,8/54**	**35,8**	**41,8**	**54**
Контрольная работа		-/-/-	-	-	-
Реферат/эссе (подготовка)		4/8/16	4	8	16
Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам и т.д.)		31,8/33,8/34,2	31,8	33,8	34,2
Подготовка к текущему контролю		-/-/-	-	-	-
Контроль:		**-/-/3,8**	**-**	**-**	**3,8**
Подготовка к экзамену		-/-/3,8	-	-	3,8
Общая трудоемкость	**час.**	**72/72/18**	**72**	**72**	**72**
	в том числе контактная работа	**36,2/30,2/14,2**	**36,2**	**30,2**	**14,2**
	зач. ед	**2/2/2**	**2**	**2**	**2**

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в 7 семестре 4 курса *(очная форма обучения)*

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Понятие и предмет цифрового права	16	4	4	-	8
2.	Электронный документооборот	16	4	4	-	8
3.	Правовое регулирование сети Интернет	16	4	4	-	8
4.	Обеспечение информационной безопасности	21,2	4	6	-	11,2
	ИТОГО по разделам дисциплины	69,8	16	18	-	35,8
	Контроль самостоятельной работы (КСР)	2	-	-	-	-
	Промежуточная аттестация (ИКР)	0,2	-	-	-	-
	Подготовка к текущему контролю	-	-	-	-	-
	Общая трудоемкость по дисциплине	72	-	-	-	-

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

Разделы (темы) дисциплины, изучаемые в 7 семестре 4 курса *(очно-заочная форма обучения)*

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
5.	Понятие и предмет цифрового права	16	2	4	-	10
6.	Электронный документооборот	16	2	4	-	10

7.	Правовое регулирование сети Интернет	18	2	6	-	10
8.	Обеспечение информационной безопасности	19,8	2	6	-	11,8
	ИТОГО по разделам дисциплины	69,8	8	20	-	41,8
	Контроль самостоятельной работы (КСР)	2	-	-	-	-
	Промежуточная аттестация (ИКР)	0,2	-	-	-	-
	Подготовка к текущему контролю	-	-	-	-	-
	Общая трудоемкость по дисциплине	72	-	-	-	-

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

Разделы (темы) дисциплины, изучаемые на 4 курсе (заочная форма обучения)

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Понятие и предмет цифрового права	16	2	2	-	12
2.	Электронный документооборот	16	-	2	-	14
3.	Правовое регулирование сети Интернет	18	2	2	-	14
4.	Обеспечение информационной безопасности	18	2	2	-	14
	ИТОГО по разделам дисциплины	68	6	8	-	54
	Контроль самостоятельной работы (КСР)	-	-	-	-	-
	Промежуточная аттестация (ИКР)	0,2	-	-	-	-
	Подготовка к текущему контролю	3,8	-	-	-	-
	Общая трудоемкость по дисциплине	72	-	-	-	-

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа (очная форма обучения)

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1.	Понятие и предмет цифрового права	Понятие цифрового права. Место цифрового права в системе права. Предмет цифрового права. Методы цифрового права. Источники цифрового права. Связь цифрового права с другими науками. Тенденции развития цифрового права на современном этапе.	Р, С, РП
2.	Электронный документооборот	Понятие и значение электронного документа. Классификация документов в цифровой сфере. Обеспечение юридической силы электронных документов. Электронная подпись: понятие, виды и порядок использования. Персональные данные в цифровой среде.	Р, С, РП
3.	Правовое регулирование сети Интернет	Понятие сети Интернет. Понятие интернет-страницы. Правовое регулирование в сфере регистрации доменных имен. Правовая природа сети Интернет. Международно-правовое регулирование отношений в сети Интернет.	Р, С, РП

		Особенности правоотношений в цифровом пространстве. Правовое регулирование сети Интернет. Перспективы развития цифрового пространства. Нотариальное заверение страниц сети Интернет.	
4.	Обеспечение информационной безопасности	Понятие информационной безопасности. Принципы информационной безопасности. Правонарушения в информационной сфере. Преступления, совершаемые в цифровой среде. Правовые способы защиты информации и информационных систем. Политика государства в сфере информационной безопасности.	Р, С, РП

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

При изучении дисциплины могут применяться электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

2.3.2 Занятия лекционного типа (очно-заочная форма обучения)

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
	Понятие и предмет цифрового права	Понятие цифрового права. Место цифрового права в системе права. Предмет цифрового права. Методы цифрового права. Источники цифрового права. Связь цифрового права с другими науками. Тенденции развития цифрового права на современном этапе.	Р, С, РП
2.	Электронный документооборот	Понятие и значение электронного документа. Классификация документов в цифровой сфере. Обеспечение юридической силы электронных документов. Электронная подпись: понятие, виды и порядок использования. Персональные данные в цифровой среде.	Р, С, РП
3.	Правовое регулирование сети Интернет	Понятие сети Интернет. Понятие интернет-страницы. Правовое регулирование в сфере регистрации доменных имен. Правовая природа сети Интернет. Международно-правовое регулирование отношений в сети Интернет. Особенности правоотношений в цифровом пространстве. Правовое регулирование сети Интернет. Перспективы развития цифрового пространства. Нотариальное заверение страниц сети Интернет.	Р, С, РП
4.	Обеспечение информационной безопасности	Понятие информационной безопасности. Принципы информационной безопасности. Правонарушения в информационной сфере. Преступления, совершаемые в цифровой среде. Правовые способы защиты информации и информационных систем. Политика государства в сфере информационной безопасности.	Р, С, РП

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

При изучении дисциплины могут применяться электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

2.3.3 Занятия лекционного типа (заочная форма обучения)

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
	Понятие и предмет цифрового права	Понятие цифрового права. Место цифрового права в системе права. Предмет цифрового права. Методы цифрового права. Источники цифрового права. Связь цифрового права с другими науками. Тенденции развития цифрового права на современном этапе.	Р, С, РП
2.	Правовое регулирование сети Интернет	Понятие сети Интернет. Понятие интернет-страницы. Правовое регулирование в сфере регистрации доменных имен. Правовая природа сети Интернет. Международно-правовое регулирование отношений в сети Интернет. Особенности правоотношений в цифровом пространстве. Правовое регулирование сети Интернет. Перспективы развития цифрового пространства. Нотариальное заверение страниц сети Интернет.	Р, С, РП
3.	Обеспечение информационной безопасности	Понятие информационной безопасности. Принципы информационной безопасности. Правонарушения в информационной сфере. Преступления, совершаемые в цифровой среде. Правовые способы защиты информации и информационных систем. Политика государства в сфере информационной безопасности.	Р, С, РП

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

При изучении дисциплины могут применяться электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

2.3.4 Занятия семинарского типа (практические занятия). Очная форма обучения

№	Наименование раздела (темы)	Тематика занятий/работ	Форма текущего контроля
1.	Понятие и предмет цифрового права	1. Понятие цифрового права. 2. Место цифрового права в системе права. 3. Предмет цифрового права. 4. Методы цифрового права. 5. Источники цифрового права.	Устный опрос по вопросам темы, реферат

		6. Связь цифрового права с другими науками. 7. Тенденции развития цифрового права на современном этапе.	
2.	Электронный документооборот	1. Понятие и значение электронного документа. 2. Классификация документов в цифровой сфере. 3. Обеспечение юридической силы электронных документов. 4. Электронная подпись: понятие, виды и порядок использования. 5. Персональные данные в цифровой среде.	Устный опрос по вопросам темы, реферат, тестирование, решение задач
3.	Правовое регулирование сети Интернет	1. Понятие сети Интернет. 2. Понятие интернет-страницы. 3. Правовое регулирование в сфере регистрации доменных имен. 4. Правовая природа сети Интернет. 5. Международно-правовое регулирование отношений в сети Интернет. 6. Особенности правоотношений в цифровом пространстве. 7. Правовое регулирование сети Интернет. 8. Перспективы развития цифрового пространства. 9. Нотариальное заверение страниц сети Интернет.	Устный опрос по вопросам темы, реферат, сообщение, решение задач
4.	Обеспечение информационной безопасности	1. Понятие информационной безопасности. 2. Принципы информационной безопасности. 3. Правонарушения в информационной сфере. 4. Преступления, совершаемые в цифровой среде. 5. Правовые способы защиты информации и информационных систем. 6. Политика государства в сфере информационной безопасности.	Устный опрос по вопросам темы, реферат, коллоквиум, решение задач

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

При изучении дисциплины могут применяться электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

2.3.5 Занятия семинарского типа (практические занятия). Очно-заочная форма обучения

№	Наименование раздела (темы)	Тематика занятий/работ	Форма текущего контроля
1.	Понятие и предмет цифрового права	1. Понятие цифрового права. 2. Место цифрового права в системе права. 3. Предмет цифрового права. 4. Методы цифрового права. 5. Источники цифрового права. 6. Связь цифрового права с другими науками.	Устный опрос по вопросам темы, реферат

		7. Тенденции развития цифрового права на современном этапе.	
2.	Электронный документооборот	1. Понятие и значение электронного документа. 2. Классификация документов в цифровой сфере. 3. Обеспечение юридической силы электронных документов. 4. Электронная подпись: понятие, виды и порядок использования. 5. Персональные данные в цифровой среде.	Устный опрос по вопросам темы, реферат, тестирование, решение задач
3.	Правовое регулирование сети Интернет	1. Понятие сети Интернет. 2. Понятие интернет-страницы. 3. Правовое регулирование в сфере регистрации доменных имен. 4. Правовая природа сети Интернет. 5. Международно-правовое регулирование отношений в сети Интернет. 6. Особенности правоотношений в цифровом пространстве. 7. Правовое регулирование сети Интернет. 8. Перспективы развития цифрового пространства. 9. Нотариальное заверение страниц сети Интернет.	Устный опрос по вопросам темы, реферат, сообщение, решение задач
4.	Обеспечение информационной безопасности	1. Понятие информационной безопасности. 2. Принципы информационной безопасности. 3. Правонарушения в информационной сфере. 4. Преступления, совершаемые в цифровой среде. 5. Правовые способы защиты информации и информационных систем. 6. Политика государства в сфере информационной безопасности.	Устный опрос по вопросам темы, реферат, коллоквиум, решение задач

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

При изучении дисциплины могут применяться электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

2.3.6 Занятия семинарского типа (практические занятия). Заочная форма обучения

№	Наименование раздела (темы)	Тематика занятий/работ	Форма текущего контроля
2.	Понятие и предмет цифрового права	1. Понятие цифрового права. 2. Место цифрового права в системе права. 3. Предмет цифрового права. 4. Методы цифрового права. 5. Источники цифрового права. 6. Связь цифрового права с другими науками. 7. Тенденции развития цифрового права на современном этапе.	Устный опрос по вопросам темы, реферат

2.	Электронный документооборот	1. Понятие и значение электронного документа. 2. Классификация документов в цифровой сфере. 3. Обеспечение юридической силы электронных документов. 4. Электронная подпись: понятие, виды и порядок использования. 5. Персональные данные в цифровой среде.	Устный опрос по вопросам темы, реферат, тестирование, решение задач
3.	Правовое регулирование сети Интернет	1. Понятие сети Интернет. 2. Понятие интернет-страницы. 3. Правовое регулирование в сфере регистрации доменных имен. 4. Правовая природа сети Интернет. 5. Международно-правовое регулирование отношений в сети Интернет. 6. Особенности правоотношений в цифровом пространстве. 7. Правовое регулирование сети Интернет. 8. Перспективы развития цифрового пространства. 9. Нотариальное заверение страниц сети Интернет.	Устный опрос по вопросам темы, реферат, сообщение, решение задач
4.	Обеспечение информационной безопасности	1. Понятие информационной безопасности. 2. Принципы информационной безопасности. 3. Правонарушения в информационной сфере. 4. Преступления, совершаемые в цифровой среде. 5. Правовые способы защиты информации и информационных систем. 6. Политика государства в сфере информационной безопасности.	Устный опрос по вопросам темы, реферат, коллоквиум, решение задач

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

При изучении дисциплины могут применяться электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

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

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка учебного (теоретического) материала	Методические указания для обучающихся по освоению дисциплин кафедры криминалистики и правовой информатики, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой криминалистики и правовой информатики, протокол № 9 от 15 мая 2024 г.

2	Подготовка реферата с презентацией	Методические указания для обучающихся по освоению дисциплин кафедры криминалистики и правовой информатики, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой криминалистики и правовой информатики, протокол № 9 от 15 мая 2024 г.
3	Выполнение реферата, сообщения	Методические указания для обучающихся по освоению дисциплин кафедры криминалистики и правовой информатики, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой криминалистики и правовой информатики, протокол № 9 от 15 мая 2024 г.
4	Подготовка и проведение коллоквиума	Методические указания для обучающихся по освоению дисциплин кафедры криминалистики и правовой информатики, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой криминалистики и правовой информатики, протокол № 9 от 15 мая 2024 г.
5	Подготовка к текущему контролю	Методические указания для обучающихся по освоению дисциплин кафедры криминалистики и правовой информатики, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой криминалистики и правовой информатики, протокол № 9 от 15 мая 2024 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,
– в форме аудиофайла,
– в печатной форме на языке Брайля.

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,
– в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии, применяемые при освоении дисциплины

При изучении дисциплины «Информационная безопасность», наряду с традиционной формой, применяются следующие формы проведения лекционных занятий: *лекция-визуализация* (основное содержание лекции представлено в образной форме: рисунках, графиках, схемах и т.д.), *проблемная лекция* (при изложении материала указывается на противоречия, заложенные в проблемных ситуациях, которые необходимо решить), *моделирование профессиональных ситуаций* (решение задач).

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты и электронной образовательной среды университета.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Информационная безопасность».

Оценочные средства включают контрольные материалы для проведения **текущего контроля** в форме рефератов, рефератов с презентацией, сообщений, коллоквиумов по теме и **промежуточной аттестации** в форме вопросов к зачету.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	**ИОПК-9.1** Понимает принципы работы современных информационных технологий.	**ИОПК-9.1.З-1.** Знает и понимает принципы работы современных информационных технологий.	Вопросы для устного (письменного) опроса по теме, коллоквиум, подготовка реферата, сообщения, тестирование	*Вопросы к зачету 1-5, 8-10*
2	**ИОПК-9.2** Реализует принципы работы современных информационных технологий для решения задач профессиональной деятельности.	**ИОПК-9.2.У-1.** Умеет реализовывать принципы работы современных информационных технологий для решения задач профессиональной деятельности	Вопросы для устного (письменного) опроса по теме, коллоквиум, подготовка реферата, сообщения, тестирование	*Вопросы к зачету 5-8, 15-19*
3	**ИОПК-9.3** Знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации.	**ИОПК-9.3.З-1** Знает современные цифровые технологии и требования цифровой безопасности, потенциальные риски в сфере цифровой безопасности **ИОПК-9.3.У-1** Умеет применять современные цифровые технологии для обеспечения цифровой безопасности и нейтрализации рисков в сфере цифровой безопасности	Вопросы для устного (письменного) опроса по теме, коллоквиум, подготовка реферата, сообщения, тестирование	*Вопросы к зачету 10-15, 21-27*
4	**ИОПК-9.4** Знание основных методов разработки искусственного интеллекта и	**ИОПК-9.4.З-1** Знает методов разработки искусственного интеллекта и оригинальных алгоритмов	Вопросы для устного (письменного) опроса по теме, коллоквиум,	*Вопросы к зачету 27-30*

	оригинальных алгоритмов для решения задач в рамках заданной проблемной области.	**ИОПК-9.4.У-1** Умеет решать задачи профессиональной деятельности с использованием искусственного интеллекта и оригинальных алгоритмов	подготовка реферата, сообщения, тестирование	

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Тема 1 «Понятие и предмет цифрового права»

1. Понятие цифрового права.
2. Место цифрового права в системе права.
3. Предмет цифрового права.
4. Методы цифрового права.
5. Источники цифрового права.
6. Связь цифрового права с другими науками.
7. Тенденции развития цифрового права на современном этапе.

Темы рефератов

1. Место цифрового права в системе юридических наук.
2. Перспективы развития цифрового права в России.
3. Юридическая сила электронного документа.
4. Международные источники цифрового права.

Тема 2 «Электронный документооборот»

1. Понятие и значение электронного документа.
2. Классификация документов в цифровой сфере.
3. Обеспечение юридической силы электронных документов.
4. Электронная подпись: понятие, виды и порядок использования.
5. Персональные данные в цифровой среде.

Темы рефератов

1. Принципы электронного документооборота.
2. Перспективы развития законодательства о персональных данных.
3. Принцип действия электронной подписи.
4. Преимущества электронного документооборота.

Тема 3 «Правовое регулирование сети Интернет»

1. Понятие сети Интернет.
2. Понятие интернет-страницы.
3. Правовое регулирование в сфере регистрации доменных имен.
4. Правовая природа сети Интернет.

5. Международно-правовое регулирование отношений в сети Интернет.
6. Особенности правоотношений в цифровом пространстве.
7. Правовое регулирование сети Интернет.
8. Перспективы развития цифрового пространства.
9. Нотариальное заверение страниц сети Интернет.

Темы рефератов

1. История сети Интернет.
2. Интернет и объекты интеллектуальных прав.
3. Ограничения сети Интернет.
4. Концепция Интернет-права.

Тема 4 «Обеспечение информационной безопасности»

1. Понятие информационной безопасности.
2. Принципы информационной безопасности.
3. Правонарушения в информационной сфере.
4. Преступления, совершаемые в цифровой среде.
5. Правовые способы защиты информации и информационных систем.
6. Политика государства в сфере информационной безопасности.

Темы рефератов

1. Современное состояние киберпреступности.
2. Перспективы развития правоохранительных органов в целях расследования киберпреступности.
3. Развитие политики государства в цифровой сфере.

Задачи

Задача № 1

При организации компании «Аист» учредители внесли свою долю в ее уставный капитал. Соучредитель Воронов в качестве вклада в имущество данной компании внес разработанную им ранее программу для ЭВМ, которую оценил в 220 тыс. рублей. Учредительное собрание согласилось принять долю учредителя Воронова в виде его интеллектуальной собственности — программного продукта для ЭВМ.

Дайте правовую оценку действий Воронова из учредительного собрания компании «Аист».

Задача № 2

По заявлению истца компании «Запад» к ответчику, акционерному обществу «Восток», арбитражным судом было вынесено решение о взыскании с ответчика суммы основного долга и процентов за пользование денежными средствами.

Однако в процессе совместной работы ответчик заключил договор на обслуживание своего расчетного счета с другим банком, реквизиты которого не сообщил партнеру по коммерческим соображениям, а отношения с банком, указанным в договоре с компанией «Запад», прекратил. Кредитор истца обратился с заявлением в арбитражный суд, в котором просил направить в адрес налоговой инспекции по месту нахождения ответчика информацию о расчетных счетах партнера по коммерческим отношениям.

В ответ на запрос арбитражного суда налоговая инспекция сообщила, что, исходя из учредительных документов акционерного общества «Восток», информация о

нахождении и состоянии расчетных счетов ответчика является коммерческой тайной и поэтому она не может быть передана истцу».

Дайте правовую оценку действиям налоговой инспекции на запрос арбитражного суда.

Задача № 3

Фирма «Локон» купила в магазине за наличный расчет (по чеку) программный продукт, который потребовался этой фирме для разработки собственных электронных игр. Программное обеспечение было установлено на 25 компьютеров, составляющих локальную вычислительную сеть, с целью ее использования в автоматизированной информационно-правовой системе.

Нарушила ли в этом случае фирма «Локон» цифровое законодательство?

Задача № 4

Акционерное общество «Росинка» купила у холдинга «Сабина» (по чеку) программный продукт без заключения соответствующего договора. Впоследствии данный программный продукт был установлен на нескольких ЭВМ (на станциях), образующих локальную вычислительную сеть, и успешно функционировал.

Нарушен ли здесь закон?

Задача № 5

Оператор Суманеева стала обсуждать с коллегами в лаборатории перспективного программирования, откуда у инженера Петровой появились машина и норковая шуба. Кто-то из сотрудников бросил: «А она нелегально торгует программами и персональными данными». Суманеева пошутила, сказав, что Петрова настоящая компьютерная пиратка.

О разговоре тут же стало известно Петровой, и она обратилась в суд с просьбой привлечь Суманееву к ответственности за клевету и оскорбление.

Проанализируйте ситуацию с позиции цифрового права.

Задача № 6

Федеральное архивное агентство России (Росархив) с разрешения руководителя аппарата Правительства РФ передала Государственному архиву одной из республик бывшего СССР в постоянное пользование документы о личной жизни и деятельности руководителей бывшего СССР — уроженцев этой республики.

Дочь одного из указанных руководителей обжаловала в суд действия Росархива и руководителя аппарата Правительства РФ, ссылаясь на Федеральный закон от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации», и просила немедленно вернуть все документы в Москву.

Проведите юридический анализ сложившейся ситуации.

Критерии оценки коллоквиума, реферата, сообщения, реферата с презентацией, задач

Оценка «отлично» выставляется студенту, если студентом дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по теме, доказательно раскрыты основные положения вопросов; в ответе прослеживается структура и логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений.

Оценка «хорошо» выставляется студенту, если студентом дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ структурирован и логичен, изложен научным языком с использованием профессиональной терминологии.

Могут быть допущены 2–3 неточности или незначительные ошибки, исправленные обучающимся с помощью преподавателя.

Оценка «удовлетворительно» выставляется при недостаточно полном и недостаточно развернутом ответе. Логика и последовательность изложения нарушены. Допущены ошибки в раскрытии понятий, употреблении терминов. Обучающийся не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано.

Оценка «неудовлетворительно» выставляется при несоответствии ответа заданному вопросу, использовании при ответе ненадлежащих нормативных и иных источников, когда ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа обучающегося.

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен/зачет)

Перечень вопросов (для зачета)

1. Понятие цифрового права.
2. Предмет цифрового права.
3. Цель и задачи цифрового права.
4. Методы цифрового права.
5. Место цифрового права в системе юридических наук.
6. Связь цифрового права с иными науками.
7. Перспективы развития цифрового права в России.
8. Цифровое право в зарубежных странах.
9. Международное регулирование цифрового права.
10. Понятие электронного документа.
11. Юридическая сила электронного документа.
12. Понятие электронной подписи.
13. Виды электронной подписи.
14. Порядок применения электронной подписи.
15. Понятие и правовой режим персональных данных.
16. Защита персональных данных в цифровой среде.
17. Понятие сети Интернет.
18. Понятие и правовой статус страницы сети Интернет.
19. Понятие и правовой статус провайдера сети Интернет.
20. Правовое регулирование регистрации доменных имен.
21. Развитие правового регулирования сети Интернет.
22. Нотариальное заверение страниц сети Интернет.
23. Понятие информационной безопасности.
24. Методы обеспечения информационной безопасности.
25. Принципы информационной безопасности.
26. Правонарушения в цифровой сфере.
27. Способы пресечения преступлений, совершаемых в цифровой среде.
28. Правовые способы защиты информации.
29. Организационно-технические способы защиты информации.
30. Государственная политика в сфере информационной безопасности.

Критерии оценивания результатов обучения

Критерии оценивания результатов обучения

Ответ на зачете оценивается одной из следующих оценок: «зачтено», «не зачтено», которые выставляются по следующим критериям.

«Зачтено»:

- знание основных понятий предмета;
- умение использовать и применять полученные знания на практике;
- работа на занятиях семинарского типа;
- знание основных научных теорий, изучаемых предметом;
- ответы на вопросы.

«Не зачтено»:

- демонстрирует частичные знания по темам дисциплины;
- незнание основных понятий предмета;
- неумение использовать и применять полученные знания на практике.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации 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.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1. Нормативные правовые акты и акты судебного толкования:

1. Конституция Российской Федерации 1993 г. (в ред. от 21.07.2014 г. № 11-ФЗ) http://pravo.gov.ru/proxy/ips/?docbody=&nd=102027595&intelsearch=%CA%EE%ED%F1%F2%
E8%F2%F3%F6%E8%FF+%D0%EE%F1%F1%E8%E9%F1%EA%EE%E9+%D4%E5%E4%E5 %F0%E0%F6%E8%E8

2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 г. № 149-ФЗ (в ред. от 19.12.2016 г.) http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108264&intelsearch=%CE%E1+%E8%ED%F

4%
EE%F0%EC%E0%F6%E8%E8+%E8+%E8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%E D%FB%F5+%F2%E5%F5%ED%EE%EB%EE%E3%E8%FF%F5

3. Об электронной подписи: Федеральный закон от 06.04.2011 г. № 63-ФЗ (в ред. от 23.06.2016г.)
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102146610&intelsearch=%CE%E1+%FD%EB%E5% EA%F2%F0%EE%ED%ED%EE%E9+%EF%EE%E4%EF%E8%F1%E8

4. О Стратегии развития информационного общества в Российской Федерации 2017 – 2030 годы: Указ Президента Российской Федерации от 09.05.2017 г. № 203. http://pravo.gov.ru/proxy/ips/?docbody=&nd=102431687&intelsearch=%CE+%D1%F2%F0%E0%F
2%E5%E3%E8%E8+%F0%E0%E7%E2%E8%F2%E8%FF+%E8%ED%F4%EE%F0%EC%E0% F6%E8%EE%ED%ED%EE%E3%EE+%EE%E1%F9%E5%F1%F2%E2%E0

5. О Концепции правовой информатизации России: указ Президента Российской Федерации от 28.06.1993 г. № 966 (в ред. от 22.03.2005 г. № 329) http://pravo.gov.ru/proxy/ips/?docbody=&nd=102024537&intelsearch=%CE+%EA%EE%EE%F0
%E4%E8%ED%E0%F6%E8%E8+%E8%ED%F4%EE%F0%EC%E0%F2%E8%E7%E0%F6%E8 %E8

6. Об утверждении Правил обмена документами в электронном виде при организации электронного взаимодействия: постановление Правительства Российской Федерации от 25.12.2014 г. № 1494 (в ред. от. 24.01.2017 г.) http://pravo.gov.ru/proxy/ips/?docbody=&nd=102365639&intelsearch=%CF%F0%E0%E2%E8%EB
%E0+%EE%E1%EC%E5%ED%E0+%E4%EE%EA%F3%EC%E5%ED%F2%E0%EC%E8+%EF
%F0%E8+%FD%EB%E5%EA%F2%F0%EE%ED%ED%EE%EC+%E2%E7%E0%E8%EC%EE %E4%E5%E9%F1%F2%E2%E8%E8

7. Об утверждении государственной программы «Информационное общество (2011-2020 гг.)»: постановление Правительства Российской Федерации от 15.04.2014 г. № 313.
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102349623&intelsearch=%CF%F0%EE%E3%F0%E0
%EC%EC%E0+%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%EE%E5+%EE%E1 %F9%E5%F1%F2%E2%EE

8. О федеральной государственной информационной системе координации информатизации: постановление Правительства Российской Федерации от 14.11.2015 г. № 1235.
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102382687&intelsearch=%CE+%EA%EE%EE%F0
%E4%E8%ED%E0%F6%E8%E8+%E8%ED%F4%EE%F0%EC%E0%F2%E8%E7%E0%F6%E8 %E8

5.2 Учебная литература

1. Правовая информатика: учебник и практикум для вузов / С. Г. Чубукова, Т. М. Беляева, А. Т. Кудинов, Н. В. Пальянова; под редакцией С. Г. Чубуковой. 3-е изд., перераб. и доп. Москва: Издательство Юрайт, 2024. 314 с. ISBN 978-5-534-03900-9. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/449895

2. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под редакцией Т. А. Поляковой, А. А. Стрельцова. Москва: Издательство Юрайт,

2023. 325 с. ISBN 978-5-534-03600-8. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/450371

3. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. Москва: Издательство Юрайт, 2020. 312 с. ISBN 978-5-9916-9043-0. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/452368

4. Внуков А. А. Защита информации: учебное пособие для вузов / А. А. Внуков. 3-е изд., перераб. и доп. Москва: Издательство Юрайт, 2020. 161 с. ISBN 978-5-534-07248-8. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/422772 5. Горелов Н. А. Развитие информационного общества: цифровая экономика: учебное пособие для вузов / Н. А. Горелов, О. Н. Кораблева. Москва: Издательство Юрайт, 2023. 241 с. ISBN 978-5-534-10039-6. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/429156

5. Фомин В. И. Информационный бизнес: учебник и практикум для вузов / В. И. Фомин. 3-е изд., испр. и доп. Москва: Издательство Юрайт, 2020. ISBN 978-5-534-06654-8. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/454444

6. Нетёсова О. Ю. Информационные системы и технологии в экономике: учебное пособие для вузов / О. Ю. Нетёсова. 3-е изд., испр. и доп. Москва: Издательство Юрайт, 2024. 178 с. ISBN 978-5-534-08223-4. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/452595

7. Внуков А. А. Защита информации в банковских системах: учебное пособие для бакалавриата и магистратуры / А. А. Внуков. 2-е изд., испр. и доп. Москва: Издательство Юрайт, 2023. 246 с. ISBN 978-5-534-01679-6. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/414083

8. Информационные технологии в юридической деятельности: учебник для вузов / П. У. Кузнецов [и др.]; под общей редакцией П. У. Кузнецова. 3-е изд., перераб. и доп. Москва: Издательство Юрайт, 2020. 325 с. ISBN 978-5-534-02598-9. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/449842

9. Гасумова С. Е. Социальная информатика: учебник и практикум для вузов / С. Е. Гасумова. 6-е изд., испр. и доп. Москва: Издательство Юрайт, 2020. 284 с. ISBN 978- 5-534-11993-0. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/451997

10. Информационные технологии в юридической деятельности: учебник и практикум для академического бакалавриата / В. Д. Элькин [и др.]; под редакцией В. Д. Элькина. 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2022. 403 с. ISBN 978-5-9916-5283-4. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/431764

11. Плахотникова М. А. Информационные технологии в менеджменте: учебник и практикум для вузов / М. А. Плахотникова, Ю. В. Вертакова. 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2020. 326 с. ISBN 978-5-534-07333-1. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/44985031

12. Информационное право: учебник для бакалавриата, специалитета и магистратуры / М. А. Федотов [и др.]; под редакцией М. А. Федотова. Москва: Издательство Юрайт, 2023. 497 с. ISBN 978-5-534-10593-3. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/430915

13. Малашенко А. В. Становление постиндустриальной цивилизации: от цифровизации до варварства: монография / А. В. Малашенко, Ю. А. Нисневич, А. В. Рябов. Москва: Издательство Юрайт, 2024. 212 с. ISBN 978-5-534-11581-9. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/457073

14. Сологубова Г. С. Составляющие цифровой трансформации: монография / Г. С. Сологубова. Москва: Издательство Юрайт, 2021. 147 с. ISBN 978-5-534-11335-8. // ЭБС Юрайт [Электронный ресурс]. URL: https://urait.ru/bcode/445006

5.3. Периодическая литература

1. Юридический вестник Кубанского государственного университета // http://urv.kubsu.ru/
2. Базы данных компании «Ист Вью» http://dlib.eastview.com (Контракт № 50-АЭФ/44-ФЗ/2020 от 28.12.2020 г. с ООО «ИВИС»), срок доступа с 01.01.2021 по 31.12.2021 гг.
3. Электронная библиотека GREBENNIKON.RU https://grebennikon.ru/ (Договор № 2812/2020/4 от 28.12.2020 г. с ООО «Издательский дом «Гребенников»), срок доступа с 01.01.2021 по 31.12.2021 гг.

5.4. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «Лань» **https://e.lanbook.com** ООО «ЭБС ЛАНЬ» Контракт № 0712/2023 от 19 декабря 2023 г.
2. ЭБС «Университетская библиотека онлайн» **http://www.biblioclub.ru/** ООО «Директ-Медиа» Контракт № 0712/2023/3 от 19 декабря 2023 г.
3. ОП «Юрайт **https://urait.ru/** ООО «Электронное издательство Юрайт» Лиц. договор № 0712/2023/1 от 19 декабря 2023 г.
4. ЭБС «BOOK.ru» **https://www.book.ru** ООО «КноРус медиа» Договор № 450-еп/223-ФЗ/2023 от 29 ноября 2023 г.
5. ЭБС «ZNANIUM» **https://znanium.ru/** ООО «ЗНАНИУМ» Контракт № 0712/2023/2 от 19 декабря 2023 г.

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины

При освоении дисциплины «Информационная безопасность» необходимо руководствоваться действующим федеральным и иным законодательством и разработанными на его основе подзаконными нормативными актами.

Изучение курса осуществляется в тесном взаимодействии с другими юридическими и общественными дисциплинами. Форма и способы изучения материала определяются с учетом специфики изучаемой темы. Однако во всех случаях необходимо обеспечить сочетание изучения теоретического материала, научного толкования того или иного понятия, даваемого в учебниках и лекциях, с самостоятельной работой студентов, выполнением практических заданий, подготовкой сообщений и докладов.

Методические указания по лекционным занятиям

В ходе лекции студентам рекомендуется конспектировать ее основные положения, не стоит пытаться дословно записать всю лекцию, поскольку скорость лекции не рассчитана на аутентичное воспроизведение выступления лектора в конспекте. Тем не менее, она является достаточной для того, чтобы студент смог не только усвоить, но и

зафиксировать на бумаге сущность затронутых лектором проблем, выводы, а также узловые моменты, на которые обращается особое внимание в ходе лекции. Основным средством работы на лекционном занятии является конспектирование. Конспектирование – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста. Результат конспектирования – запись, позволяющая студенту немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других. Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей концепции лекции (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую сущность сообщения, понять систему изложения информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т.е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Определения, которые дает лектор, стоит по возможности записать дословно и выделить другим цветом или же подчеркнуть. В случае изложения лектором хода научной дискуссии желательно кратко законспектировать существо вопроса, основные позиции и фамилии ученых, их отстаивающих. Если в обоснование своих выводов лектор приводит ссылки на справочники, статистические данные, нормативные акты и другие официально опубликованные сведения, имеет смысл лишь кратко отразить их существо и указать источник, в котором можно полностью почерпнуть излагаемую информацию.

Во время лекции студенту рекомендуется иметь на столах помимо конспектов также программу спецкурса, которая будет способствовать развитию мнемонической памяти, возникновению ассоциаций между выступлением лектора и программными вопросами, необходимые законы и подзаконные акты, поскольку гораздо эффективнее следить за ссылками лектора на нормативный акт по его тексту, нежели пытаться воспринять всю эту информацию на слух.

В случае возникновения у студента по ходу лекции вопросов, их следует записать и задать в конце лекции в специально отведенное для этого время.

По окончании лекции (в тот же или на следующий день, пока еще в памяти сохранилась информация) студентам рекомендуется доработать свои конспекты, привести их в порядок, дополнить сведениями с учетом дополнительно изученного нормативного, справочного и научного материала. Крайне желательно на полях конспекта отмечать не только изученные точки зрения ученых по рассматриваемой проблеме, но и выражать согласие или несогласие самого студента с законспектированными положениями, материалами судебной практики и т.п.

Лекционное занятие предназначено для изложения особенно важных, проблемных, актуальных в современной науке вопросов. Лекция, также как и семинарское, практическое занятие, требует от студентов определенной подготовки. Студент обязательно должен знать тему предстоящего лекционного занятия и обеспечить себе необходимый уровень активного участия: подобрать и ознакомиться, а при необходимости иметь с собой рекомендуемый преподавателем нормативный материал, повторить ранее пройденные темы по вопросам, которые будут затрагиваться в предстоящей лекции, вспомнить материал иных дисциплин. Применение отдельных образовательных технологий требует специальной подготовки не только от

преподавателя, но и участвующих в занятиях студентов. Так, при проведении лекции-дискуссии, которая предполагает разделение присутствующих студентов на группы, студент должен быть способен высказать свою позицию относительно выдвинутых преподавателем точек зрения.

Методические указания для подготовки к занятиям семинарского типа (практическим занятиям)

Для практических (семинарских) занятий по дисциплине «Информационная безопасность» характерно сочетание теории с обсуждением этических проблем.

Практические (семинарские) занятия представляют собой одну из важных форм самостоятельной работы студентов над нормативными актами, материалами практики дисциплинарных комиссий, научной и учебной литературой непосредственно в учебной аудитории под руководством преподавателя.

В зависимости от изучаемой темы и ее специфики преподаватель выбирает или сочетает следующие формы проведения семинарских (практических) занятий: обсуждение теоретических вопросов, подготовка рефератов и т.п. Проверка усвоения отдельных (ключевых) тем может осуществляться посредством проведения коллоквиума.

Коллоквиум представляет собой предметную дискуссию по тематике занятия, в котором принимают участие все студенты учебной группы. Во время коллоквиума студенты совместно с преподавателем рассматривают проблемные вопросы дисциплины и приходят к обоснованным выводам относительно каждого исследуемого вопроса, включенного в тематику занятия.

Подготовка к практическому занятию заключается в подробном изучении конспекта лекции, нормативных актов и материалов судебной практики, рекомендованных к ним, учебной и научной литературы, основные положения которых студенту рекомендуется конспектировать.

Активное участие в работе на практических и семинарских занятиях предполагает выступления на них, дополнение ответов однокурсников, коллективное обсуждение спорных вопросов и проблем, что способствует формированию у студентов навыков формулирования, аргументации и отстаивания выработанного решения, умения его защитить в дискуссии и представить дополнительные аргументы в его пользу. Активная работа на семинарском (практическом) занятии способствует также формированию у студентов навыков публичного выступления, умения ясно, последовательно, логично и аргументировано излагать свои мысли.

При выступлении на семинарских или практических занятиях студентам разрешается пользоваться конспектами для цитирования нормативных актов, судебной практики или позиций ученых. По окончании ответа другие студенты могут дополнить выступление товарища, отметить его спорные или недостаточно аргументированные стороны, проанализировать позиции ученых, о которых не сказал предыдущий выступающий.

В конце занятия после подведения его итогов преподавателем студентам рекомендуется внести изменения в свои конспекты, отметить информацию, прозвучавшую в выступлениях других студентов, дополнения, сделанные преподавателем и не отраженные в конспекте.

Практические занятия требуют предварительной теоретической подготовки по соответствующей теме: изучения учебной и дополнительной литературы, ознакомления с нормативным материалом, актами толкования. Рекомендуется при этом вначале изучить вопросы темы по учебной литературе. Если по теме прочитана лекция, то непременно надо использовать материал лекции, так как учебники часто устаревают уже в момент выхода в свет.

Применение отдельных образовательных технологий требуют предварительного ознакомления студентов с содержанием применяемых на занятиях приемов. Так, при

практических занятиях студент должен представлять как его общую структуру, так и особенности отдельных методических приемов: дискуссии, контрольные работы, использование правовых документов и др.

Примерные этапы практического занятия и методические приемы их осуществления:

– постановка целей занятия: обучающей, развивающей, воспитывающей;

– планируемые результаты обучения: что должны студенты знать и уметь;

– проверка знаний: устный опрос, фронтальный опрос, программированный опрос, блиц-опрос, письменный опрос, комментирование ответов, оценка знаний, обобщение по опросу;

– изучение нового материала по теме;

– закрепление материала предназначено для того, чтобы студенты запомнили материал и научились использовать полученные знания (активное мышление).

Формы закрепления:

– решение задач;

– работа с приговорами судов;

– групповая работа (коллективная мыслительная деятельность).

Домашнее задание:

– работа над текстом учебника;

– решение задач.

В рамках семинарского занятия студент должен быть готов к изучению предлагаемых правовых документов и их анализу.

Важнейшим этапом курса является *самостоятельная работа* по дисциплине «П Информационная безопасность», включающая в себя проработку учебного (теоретического) материала, выполнение индивидуальных заданий (подготовка сообщений, презентаций), выполнение рефератов, подготовку к текущему контролю.

Самостоятельна работа осуществляется на протяжении всего времени изучения дисциплины «Информационная безопасность», по итогам которой студенты предоставляют сообщения, рефераты, презентации, конспекты, показывают свои знания на практических занятиях при устном ответе.

Методические рекомендации по подготовке рефератов, сообщений, рефератов с презентацией

Первичные навыки научно-исследовательской работы должны приобретаться обучающимися при написании рефератов по специальной тематике.

Цель: научить студентов связывать теорию с практикой, пользоваться литературой, статистическими данными, привить умение популярно излагать сложные вопросы.

Рефераты составляются в соответствии с указанными темами. Выполнение рефератов предусмотрено на листах формата А4. Они сдаются на проверку преподавателю в соответствии с указанным графиком.

Требования к работе. Реферативная работа должна выявить углубленные знания студентов по той или иной теме дисциплины «Информационная безопасность». В работе должно проявиться умение работать с литературой. Студент обязан изучить и использовать в своей работе не менее 2–3 учебных пособий.

Оформление реферата:

1. Реферат должен иметь следующую структуру: а) план; б) изложение основного содержания темы; с) список использованной литературы.

2. Общий объём – 12-15 страниц основного текста.

3. Перед написанием должен быть составлен план работы, который обычно включает 2–3 вопроса. План не следует излишне детализировать, в нём перечисляются основные, центральные вопросы темы.

4. В процессе написания работы студент имеет право обратиться за консультацией к преподавателю кафедры.

5. В основной части работы большое внимание следует уделить глубокому теоретическому освещению основных вопросов темы, правильно увязать теоретические положения с практикой, конкретным фактическим и цифровым материалом.

6. В реферате обязательно отражается использованная литература, которая является завершающей частью работы.

7. Особое внимание следует уделить оформлению. На титульном листе необходимо указать название вуза, название кафедры, тему, группу, свою фамилию и инициалы, фамилию научного руководителя. На следующем листе приводится план работы.

8. При защите реферата выставляется дифференцированная оценка.

9. Реферат, не соответствующий требованиям, предъявляемым к данному виду работы, возвращается на доработку.

Качество реферата оценивается по тому, насколько полно раскрыто содержание темы, использованы первоисточники, логичное и последовательное изложение. Оценивается и правильность подбора основной и дополнительной литературы (ссылки по правилам: фамилии и инициалы авторов, название источника, место издания, издательство, год издания, страница).

Реферат обязательно должен отражать точку зрения автора на данную проблему.

Составление презентаций к реферату — это вид самостоятельной работы студентов по созданию наглядных информационных пособий, выполненных с помощью мультимедийной компьютерной программы «Power Point» или ее аналогов. Этот вид работы требует навыков студента по сбору, систематизации, переработке информации, оформления ее в виде подборки материалов, кратко отражающих основные вопросы изучаемой темы, в электронном виде. Материалы презентации готовятся студентом в виде слайдов.

Одной из форм задания может быть реферат-презентация. Данная форма выполнения самостоятельной работы отличается от написания реферата и доклада тем, что студент результаты своего исследования представляет в виде презентации. Серией слайдов он передаёт содержание темы своего исследования, её главную проблему и социальную значимость. Слайды позволяют значительно структурировать содержание материала и одновременно заостряют внимание на логике его изложения.

Слайды презентации должны содержать логические схемы реферируемого материала. Студент при выполнении работы может использовать картографический материал, диаграммы, графики, звуковое сопровождение, фотографии, рисунки и другое. Каждый слайд должен быть аннотирован, то есть он должен сопровождаться краткими пояснениями того, что он иллюстрирует.

Во время презентации студент имеет возможность делать комментарии, устно дополнять материал слайдов.

Подготовка сообщения представляет собой разработку и представление небольшого по объему устного сообщения для озвучивания на практическом занятии. Сообщаемая информация носит характер уточнения или обобщения, несет новизну, отражает современный взгляд по определенным проблемам.

Сообщение отличается от реферата не только объемом информации, но и ее характером – сообщения дополняют изучаемый вопрос фактическими или статистическими материалами. Возможно письменное оформление задания, оно может включать элементы наглядности (иллюстрации, демонстрацию).

Регламент времени на озвучивание сообщения – до 5 минут.

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.

7. Материально-техническое обеспечение по дисциплине

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Ауд.7 Интерактивная мультимедийная трибуна, проектор, магнитно- маркерная доска, проектор, учебная мебель, портреты известных ученых-юристов (6), учебно-наглядные пособия (2) Ауд. 9 Интерактивный проектор, магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (6), ноутбук Ауд. 10 Интерактивная мультимедийная трибуна, проектор, система усиления и обработки звука, магнитно-маркерная доска, учебная мебель, портреты известных ученых- юристов (8), учебно-наглядные пособия (3), флаги (2) Ауд. 17 Интерактивный проектор, магнитно-маркерная доска, учебная мебель, портреты известных ученых-юристов (8), учебно-наглядные пособия (10), гербы (2), ноутбук Ауд. 18 Интерактивный проектор, система усиления и обработки звука, магнитно-маркерная доска, учебная мебель, портреты известных ученых-юристов (12), учебно-наглядные пособия (5), ноутбук	КонсультантПлюс – Справочная Правовая Система (КонсультантПлюс). Артикул правообладателя КонсультантПлюс. (Дог. №ГК/479/ЕП/223/ФЗ/2023). ГАРАНТ – Справочная Правовая Система (ГАРАНТ). «Компания АПИ «ГАРАНТ»» Артикул правообладателя ГАРАНТ. (Дог. №4920/НК/14). Антиплагиат-ВУЗ Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ» версии 3.3. (интернет-версия) (Дог. №19/АЭФ/44/ФЗ/2023). Р7-Офис - Десктопные редакторы текстовых документов, таблиц и презентаций. Лицензии на офисное программное обеспечение для рабочих мест с целью обеспечения образовательного процесса Р7-Офис. Профессиональный (Десктоп + Сервер оптимальный). (Дог. №30-АЭФ/44-ФЗ/2022)

	Ауд. 208 Магнитно-маркерная доска, учебная мебель, проектор, учебно-наглядные пособия (3), портреты ученых-юристов (5), система обработки и усиления звука, ноутбук. Ауд. 305 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (11), портрет ученного-юриста (1), переносной экран на штативе, переносной проектор, ноутбук. Ауд. 404 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (4), портреты ученых-юристов (11), переносной экран на штативе, переносной проектор, ноутбук. Ауд. 406 Интерактивный проектор с экраном, учебная мебель, учебно-наглядные пособия (5), ноутбук. Ауд. 002 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (5), переносной экран на штативе, переносной проектор, ноутбук. Ауд. 005 Магнитно-маркерная доска, учебная мебель, переносной экран на штативе, переносной проектор, ноутбук. Ауд. 01 Интерактивная мультимедийная трибуна, проектор, проекционный экран, портреты известных ученых-юристов (10), учебно-наглядные пособия (5) Ауд. 02 Интерактивный проектор, **м**агнитно-маркерная доска, учебная мебель,	

	портреты известных ученых-юристов (10), учебно-наглядные пособия (16), ноутбук Ауд. 03 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (4), переносной экран на штативе, переносной проектор, ноутбук	
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Ауд. 3 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (3), переносной экран на штативе, переносной проектор, ноутбук Ауд. 5 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (4), переносной экран на штативе, переносной проектор, ноутбук Ауд. 7 Интерактивная мультимедийная трибуна, проектор, магнитно- маркерная доска, проектор, учебная мебель, портреты известных ученых-юристов (6), учебно-наглядные пособия (2) Ауд. 9 Интерактивный проектор, магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (6), ноутбук Ауд. 18 Интерактивный проектор, система усиления и обработки звука, магнитно-маркерная доска, учебная мебель, портреты известных ученых-юристов (12), учебно-наглядные пособия (5), ноутбук Ауд. 104 Магнитно-маркерная доска, учебная мебель, портреты ученых-юристов (15), специализированная мебель, технические средства обучения, DVD плеер, ж/к телевизор,	КонсультантПлюс – Справочная Правовая Система (КонсультантПлюс). Артикул правообладателя КонсультантПлюс. (Дог. №ГК/479/ЕП/223/ФЗ/2023). ГАРАНТ – Справочная Правовая Система (ГАРАНТ). «Компания АПИ «ГАРАНТ»» Артикул правообладателя ГАРАНТ. (Дог. №4920/НК/14). Антиплагиат-ВУЗ Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ» версии 3.3. (интернет-версия) (Дог. №19/АЭФ/44/ФЗ/2023). Р7-Офис - Десктопные редакторы текстовых документов, таблиц и презентаций. Лицензии на офисное программное обеспечение для рабочих мест с целью обеспечения образовательного процесса Р7-Офис. Профессиональный (Десктоп + Сервер оптимальный). (Дог. №30-АЭФ/44-ФЗ/2022)

	стенд с научными журналами, музей криминалистического оборудования, переносной экран на штативе, переносной проектор, ноутбук. Ауд. 108 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (8), цифровой фотоаппарат, комплект криминалистического оборудования, манекен, переносной экран на штативе, переносной проектор, ноутбук. Ауд. 204 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (7), переносной экран на штативе, переносной проектор, ноутбук. Ауд. 208 Магнитно-маркерная доска, учебная мебель, проектор, учебно-наглядные пособия (3), портреты ученых-юристов (5), система обработки и усиления звука, ноутбук. Ауд. 209 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (7), переносной экран на штативе, переносной проектор, ноутбук. Ауд. 304 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (8), портреты ученых-юристов (6), переносной экран на штативе, переносной проектор, ноутбук. Ауд. 305 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (11), портрет ученного-юриста (1), переносной экран на штативе, переносной проектор, ноутбук.	

	Ауд. 306 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (10), портрет ученного-юриста (1), переносной экран на штативе, переносной проектор, ноутбук. Ауд. 307 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (3), переносной экран на штативе, переносной проектор, ноутбук. Ауд. 404 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (4), портреты ученых-юристов (11), переносной экран на штативе, переносной проектор, ноутбук. Ауд. 405 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (4), портреты ученых-юристов (3), переносной экран на штативе, переносной проектор, ноутбук. Ауд. 407 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (4), переносной экран на штативе, переносной проектор, ноутбук Ауд. 002 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (5), переносной экран на штативе, переносной проектор, ноутбук. Ауд. 004 Магнитно-маркерная доска, учебная мебель, переносной экран на штативе, переносной проектор, ноутбук. Ауд. 005 Магнитно-маркерная доска, учебная мебель, переносной экран на штативе, переносной проектор, ноутбук.	

	Ауд. 03 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (4), переносной экран на штативе, переносной проектор, ноутбук Ауд. 03-А Магнитно-маркерная доска, учебная мебель, портреты известных ученых-юристов (2), переносной экран на штативе, переносной проектор, ноутбук Ауд. 06 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (4), переносной экран на штативе, переносной проектор, ноутбук Ауд. 09 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (8), переносной экран на штативе, переносной проектор, ноутбук Ауд. 010 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (4), переносной экран на штативе, переносной проектор, ноутбук Ауд. 012 Магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия (6), переносной экран на штативе, переносной проектор, ноутбук	

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для	Мебель: учебная мебель	КонсультантПлюс –

самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	Справочная Правовая Система (КонсультантПлюс). Артикул правообладателя КонсультантПлюс. (Дог. №ГК/479/ЕП/223/ФЗ/2023). ГАРАНТ – Справочная Правовая Система (ГАРАНТ). «Компания АПИ «ГАРАНТ»» Артикул правообладателя ГАРАНТ. (Дог. №4920/НК/14). Антиплагиат-ВУЗ Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ» версии 3.3. (интернет-версия) (Дог. №19/АЭФ/44/ФЗ/2023). Р7-Офис - Десктопные редакторы текстовых документов, таблиц и презентаций. Лицензии на офисное программное обеспечение для рабочих мест с целью обеспечения образовательного процесса Р7-Офис. Профессиональный (Десктоп + Сервер оптимальный). (Дог. №30-АЭФ/44-ФЗ/2022)
Помещение для самостоятельной работы обучающихся	Библиотека. Учебная мебель, стенды с литературой, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС КубГУ, с техническими возможностями перевода основных библиотечных фондов в электронную форму Ауд.103 Учебная мебель, компьютерная техника с	КонсультантПлюс – Справочная Правовая Система (КонсультантПлюс). Артикул правообладателя КонсультантПлюс. (Дог. №ГК/479/ЕП/223/ФЗ/2023). ГАРАНТ – Справочная Правовая Система (ГАРАНТ). «Компания АПИ «ГАРАНТ»» Артикул правообладателя ГАРАНТ. (Дог. №4920/НК/14). Антиплагиат-ВУЗ Программная система для обнаружения текстовых

	возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС КубГУ Ауд. 201 Учебная мебель, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС КубГУ Ауд. 011 Магнитно-маркерная доска, учебная мебель, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС КубГУ	заимствований в учебных и научных работах «Антиплагиат.ВУЗ» версии 3.3. (интернет-версия) (Дог. №19/АЭФ/44/ФЗ/2023). Р7-Офис - Десктопные редакторы текстовых документов, таблиц и презентаций. Лицензии на офисное программное обеспечение для рабочих мест с целью обеспечения образовательного процесса Р7-Офис. Профессиональный (Десктоп + Сервер оптимальный). (Дог. №30-АЭФ/44-ФЗ/2022)

Приложение 1

ПРИМЕРНЫЙ ИТОГОВЫЙ ТЕСТ

по дисциплине «Информационная безопасность»

ВАРИАНТ 1

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных

- Разработка и установка во всех компьютерных правовых сетях журналов учета действий

+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство

+ Перехват данных, хищение данных, изменение архитектуры системы

- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная

- Клиентская, серверная, сетевая

- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети

- инсайдерства в организации

- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных

- Информационные системы, психологическое состояние пользователей

- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации

- Техническое вмешательство, выведение из строя оборудования сети

+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности

- Многоплатформенной реализации системы

- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний

+ органы права, государства, бизнеса

- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков

- Установка новых офисных приложений, смена хостинг-компании

- Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:

+ Неоправданных ограничений при работе в сети (системе)

- Рисков безопасности сети, системы

- Презумпции секретности

ВАРИАНТ 2

1) Принципом политики информационной безопасности является принцип:

+ Невозможности миновать защитные средства сети (системы)

- Усиления основного звена сети, системы

- Полного блокирования доступа при риск-ситуациях

2) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой

+ Логические закладки («мины»)

- Аварийное отключение питания

3) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить

- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

+ Удалить письмо с приложением, не раскрывая (не читая) его

4) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения

- Секретность информации определена скоростью передачи данных

+ Секретность закрытого сообщения определяется секретностью ключа

5) ЭЦП – это:

- Электронно-цифровой преобразователь

+ Электронно-цифровая подпись

- Электронно-цифровой процессор

6) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО

+ Ошибки эксплуатации и неумышленного изменения режима работы

системы

- Сознательного внедрения сетевых вирусов

7) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования

- Моральный износ сети, инсайдерство

+ Сбой (отказ) оборудования, нелегальное копирование данных

8) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет

+ Вирусы в сети, логические мины (закладки), информационный перехват

- Компьютерные сбои, изменение администрирования, топологии

9) Утечкой информации в системе называется ситуация, характеризуемая:

+ Потерей данных в системе

- Изменением формы информации

- Изменением содержания информации

10) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

+ Целостность

- Доступность

- Актуальность

ВАРИАНТ 3

1) Угроза информационной системе (компьютерной сети) – это:

+ Вероятное событие

- Детерминированное (всегда определенное) событие

- Событие, происходящее периодически

2) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной

- Правовой

+ Защищаемой

3) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

+ Программные, технические, организационные, технологические

- Серверные, клиентские, спутниковые, наземные

- Личные, корпоративные, социальные, национальные

4) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

+ Владелец сети

- Администратор сети

- Пользователь сети

5) Политика безопасности в системе (сети) – это комплекс:

+ Руководств, требований обеспечения необходимого уровня безопасности

- Инструкций, алгоритмов поведения пользователя в сети

- Нормы информационного права, соблюдаемые в сети

6) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер

- Аудит, анализ безопасности

+ Аудит, анализ уязвимостей, риск-ситуаций

7) Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)

- Перехода в безопасное состояние работы сети, системы

- Полного доступа пользователей ко всем ресурсам сети, системы

8) ЭЦП – это:

- Электронно-цифровой преобразователь

+ Электронно-цифровая подпись

- Электронно-цифровой процессор

9) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети

- инсайдерства в организации

- чрезвычайных ситуаций

10) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных

- Информационные системы, психологическое состояние пользователей

- Бизнес-ориентированные, коммерческие системы