МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
Государственное образовательное учреждение высшего образования Московской области
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ОБЛАСТНОЙ УНИВЕРСИТЕТ
(МГОУ)

Юридический факультет
Кафедра гражданского права

Согласовано управлением организации и контроля качества образовательной деятельности
«9» 07 2021 г.
Начальник управления _____
/ Г.Е. Суслин /

Одобрено учебно-методическим советом
Протокол «9» 7 2021 г.№ 6
Председатель _____
/ О.А. Шестакова /

Рабочая программа дисциплины

Информационная безопасность

Направление подготовки
40.03.01 Юриспруденция

Профиль:
Правозащитная деятельность с интенсивным изучением иностранного языка

Квалификация
Бакалавр

Форма обучения
Очная

Согласовано учебно-методической комиссией юридического факультета:
Протокол от «17» июня 2021 г. № 11
Председатель УМКом _____
/К.В. Чистяков/

Рекомендовано кафедрой гражданского права
Протокол от «15» июня 2021 г. № 11
И.о. зав. кафедрой _____
/Левушкин А.Н/

Мытищи
2021

Автор-составитель:
доцент кафедры гражданского права МГОУ,
кандидат технических наук, доцент Петрова В.Ю.

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 40.03.01 Юриспруденция, утвержденного приказом Минобрнауки России от 13.08.2020 г. № 1011.

Дисциплина входит в часть, формируемую участниками образовательных отношений, и является элективной дисциплиной.

\

Год начала подготовки 2021

Содержание

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

1.1. Цель и задачи дисциплины

Целями освоения дисциплины «Информационная безопасность» являются: формирование у студентов знаний содержания нормативных правовых актов, регулирующих общественные отношения в области получения, обработки, применения и распространения информации и ее защиты; формирование умений и навыков практического применения юридических знаний

Задачи, обусловливающие достижение цели освоения дисциплины:

- формирование у студентов умения анализировать правовые нормы и институты;
- формирование умения применять в деятельности органов государственной власти, норм информационного права;
- создание у студентов целостной системы знаний о методах, средствах, способах защиты информации;
- подготовить специалистов, способных осуществлять как правотворческую, так и правоприменительную деятельность.

1.2. Планируемые результаты обучения:

В результате освоения данной дисциплины у обучающихся формируются следующие компетенции:

УК-1- способность осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

СПК-2 – способность квалифицированно применять правовые нормы и принимать правоприменительные акты в конкретных сферах юридической деятельности

СПК-3 - способность принимать профессиональные решение в пределах своих полномочий, совершать иные действия, связанные с реализацией правовых норм

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в часть, формируемую участниками образовательных отношений, и является элективной дисциплиной.

Знания и навыки, приобретенные студентами при изучении дисциплины «Информационная безопасность» имеют тесные связи с такими дисциплинами как: «Теория государства и права», «Конституционное право», «Административное право», «Информационное право».

При изучении дисциплины «Информационная безопасность» студентам необходимо опираться на знания, полученные, прежде всего, при изучении теории права.

Приступая к изучению данной дисциплины, студенты должны понимать, уметь анализировать, правильно толковать правовые нормы конституционного и административного законодательства, владеть навыками работы с нормативными правовыми актами с целью последующего их практического применения при изучении дисциплины «Информационная безопасность».

Учебный курс «Информационная безопасность» является самостоятельным курсом, в рамках которого изучается правовое регулирование общественных отношений, возникающих в области сбора, обработки, накопления, распространения информации. Изучение данного курса, следует рассматривать как предшествующее и обеспечивающее правильное понимание и осмысление отдельных тем дисциплин «Юридическая ответственность в частном праве», «Исполнительное производство» и др., а также

успешное освоение программ учебной и производственных практик, научно-исследовательской работы.

3.ОБЪЕМ И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем дисциплины

Показатель объема дисциплины	Форма обучения: очная
Объем дисциплины в зачетных единицах	2
Объем дисциплины в часах	72
Контактная работа	**34,2**
Лекции	10
Практические занятия	24
Контактные часы на промежуточную аттестацию:	0,2
Зачет	0,2
Самостоятельная работа	30
Контроль	7,8

Формой промежуточной аттестации является зачет в 5 семестре

3.2. Содержание дисциплины

По очной форме обучения

Наименование разделов (тем) дисциплины с кратким содержанием	Кол-во часов	
	Лекции	**Практические занятия**
Тема 1. Введение. Основные понятия информационной безопасности	2	2
Тема 2. История защиты информации в России	2	2
Тема 3. Системный анализ проблем обеспечения информационной безопасности.	2	4
Тема 4. Нормативная основа и стандарты обеспечения информационной безопасности.	2	2
Тема 5. Теоретические и методологические основы оптимизации комплексной защиты информации .		2

Тема 6. Методы и средства защиты информации		
Тема 7. Организация защиты информации	2	2
Тема 8. Основы криптографии		2
Тема 9. Защита информации в IP-сетях		8
Итого	10	24

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

4.1.УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ (ДЛЯ ОЧНОЙ ФОРМЫ ОБУЧЕНИЯ)

Темы для самостоятельного изучения	Изучаемые вопросы	Кол-во часов	Формы самост-ой работы	Методические обеспечения	Формы отчетности
Тема 1. Информационная безопасность как составная часть государственной безопасности	Соотношение понятий государственная безопасность, национальная безопасность, информационная безопасность, правовая безопасность, экологическая безопасность и т.д.	2	Подготовка к практическим занятиям, изучение литературы	Нестеров С.А. Информационная безопасность. ЮРАЙТ. 2019. – 321 с. Баранова Е.К. Информационная безопасность и защита информации: учебное пособие. – М.: РИОР. 2018. – 400 с.	Опрос на практических занятиях, тестирование
Тема 2. Защита информации взарубежных	Изучение вопросов защиты информации в	2	Подготовка к практически	Нестеров С.А. Информ	Опрос на практичес ких

странах	странах Западной Европы и США. Сравнительный анализ с методами защиты информации в России		м занятиям, изучение литературы.	ационная безопасность. ЮРАЙТ. 2019. – 321 с. Баранова Е.К. Информационная безопасность и защита информации: учебное пособие. – М.: РИОР. 2018. – 400 с.	занятиях, тестирование
Тема 3. Риски в информационной среде	Анализ рисков в информационной среде. Причины утери, хищения информации. Методикаоценки рисков. Информационная война.	4	Подготовка к практическим занятиям, изучение литературы	Нестеров С.А. Информационная безопасность. ЮРАЙТ. 2019. – 321 с. Баранова Е.К. Информационная безопасность и защита информации: учебное пособие. – М.: РИОР. 2018. – 400 с.	Опрос на практических занятиях, тестирование
Тема 4. Классификация стандартов информационной безопасности	Основания классификации стандартов информационной безопасности: области	4	Подготовка к практическим занятиям, изучение литературы	Нестеров С.А. Информационная безопасность. ЮРАЙТ	Опрос на практических занятиях, тестирование

	регламентации, территории, доступности, по обязательности исполнения			. 2019. – 321 с. Баранов а Е.К. Информ ационна я безопасн ость и защита информа ции: учебное пособие. – М.: РИОР. 2018. – 400 с.	
Тема 5. Операции в системе управления информационной безопасностью	Принципы построения систем информационной безопасности. Операции в системе управления информационной безопасностью	4	Подготовка к практическим занятиям, изучение литературы	Нестеров С.А. Информ ационная безопасност ь. ЮРАЙТ . 2019. – 321 с. Баранов а Е.К. Информ ационна я безопасн ость и защита информа ции: учебное пособие. – М.: РИОР. 2018. – 400 с.	Опрос на практиче ских занятиях, тестирова ние
Тема 6. Методы защиты от компьютерных вирусов	Понятие компьютерного вируса. Направления воздействия компьютерных вирусов. Внешние проявления компьютерныхви	4	Подготовка к практическим занятиям, изучение литературы	Нестеров С.А. Информ ационная безопасност ь. ЮРАЙТ . 2019. – 321 с. Баранов а	Опрос на практиче ских занятиях, тестирова ние

	русов. Классификация компьютерных вирусов. Многоуровневая система защиты.			Е.К. Информационная безопасность и защита информации: учебное пособие. – М.: РИОР. 2018. – 400 с.	
Тема 7. Правонарушения в информационной сфере	Административная ответственность за правонарушения в сфере информации. Уголовная ответственность в сфере информации	2	Подготовка к практическим занятиям, изучение литературы	Нестеров С.А. Информационная безопасность. ЮРАЙТ. 2019. – 321 с. Баранова Е.К. Информационная безопасность и защита информации: учебное пособие. – М.: РИОР. 2018. – 400 с.	Опрос на практических занятиях, тестирование
Тема 8. Классификация шифров	Понятие шифра. Виды и основания классификации шифров.	4	Подготовка к практическим занятиям, изучение литературы	Нестеров С.А. Информационная безопасность. ЮРАЙТ. 2019. – 321 с. Баранова Е.К. Информационная	Опрос на практических занятиях, тестирование

				безопасность и защита информации: учебное пособие. – М.: РИОР. 2018. – 400 с.	
Тема 9. Управление криптографическими ключами	Совместное использование симметричных и асимметричных шрифтов	4	Подготовка к практическим занятиям, изучение литературы	Нестеров С.А. Информационная безопасность. ЮРАЙТ. 2019. – 321 с. Баранова Е.К. Информационная безопасность и защита информации: учебное пособие. – М.: РИОР. 2018. – 400 с.	Опрос на практических занятиях, тестирование
Всего		30			

Подтверждением сформированности у студента оцениваемых компетенций является промежуточная аттестация.
Допуск к промежуточной аттестации – от 60 баллов. Зачет – 10 баллов**.**

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

5.1 Перечень компетенций с указанием этапов их формирования в процессе освоение образовательной программы

Код и наименование компетенции	**Этапы формирования**
УК-1 – способность осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	1.Работа на учебных занятиях 2.Самостоятельная

СПК-2 – способность квалифицированно применять правовые нормы и принимать правоприменительные акты в конкретных сферах юридической деятельности	1.Работа на учебных занятиях 2.Самостоятельная работа
СПК-3 – способность квалифицированно применять правовые нормы и принимать правоприменительные акты в конкретных сферах юридической деятельности	1.Работа на учебных занятиях 2.Самостоятельная работа

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

Оцениваемые компетенции	**Уровень сформированности**	**Этап формирования**	**Описание показателей**	**Критерии оценивания**	**Шкала оценивания**
УК-1	Пороговый	1.Работа на учебных занятиях 2.Самостоятельная работа	***Знать:*** методики поиска, сбора и обработки информации, метод системного анализа ***Уметь:*** применять методики поиска, сбора, обработки информации, системный подход для решения поставленных задач и осуществлять критический анализ и синтез информации, полученной из актуальных российских и зарубежных источников	Текущий контроль: опрос, тест Промежуточная аттестация: зачет	41-60 баллов
	Продвинутый	1.Работа на учебных занятиях 2.Самостоятельная работа	***Знать:*** методики поиска, сбора и обработки информации, метод системного анализа ***Уметь:*** применять методики	Текущий контроль: опрос, тест Промежуточная аттестация: зачет	61-100 баллов

			поиска, сбора, обработки информации, системный подход для решения поставленных задач и осуществлять критический анализ и синтез информации, полученной из актуальных российских и зарубежных источников ***Владеть:*** методами поиска, сбора и обработки, критического анализа и синтеза информации, методикой системного подхода для решения поставленных задач.		
СПК- 2	Пороговый	1.Работа на учебных занятиях 2.Самостоятельная работа	***Знать:*** правоприменительную практику в целях решения профессиональных задач ***Уметь*:** понимать значимость и сущность правосудия, различает виды судопроизводства, сущность контрольно-надзорной деятельности, систему соответствующих органов, различает виды контрольно-надзорных полномочий и правоприменительных актов	Текущий контроль: опрос, тест Промежуточная аттестация: зачет	41-60 баллов

	Продвинутый	1.Работа на учебных занятиях 2.Самостоятельная работа	***Знать:*** методику анализа правоприменительной практики в целях решения профессиональных задач ***Уметь:*** понимать значимость и сущность правосудия, различать виды судопроизводства; сущность контрольно-надзорной деятельности, систему соответствующих органов, различать виды контрольно-надзорных полномочий и правоприменительных актов; ***Владеть***: спецификой правоприменения в системе государственной и муниципальной службы	Текущий контроль: опрос, тест Промежуточная аттестация: зачет	61-100 баллов
СПК-3	Пороговый	1. Работа на учебных занятиях 2. Самостоятельная работа	***Знать:*** возможности принятия профессиональных решений в пределах своих полномочий, совершать иные действия, связанные с реализацией правовых норм	Текущий контроль: опрос, тест Промежуточная аттестация: зачет	41-60 баллов
	Продвинутый	1.Работа на учебных занятиях 2.Самостоятель	***Знать:*** возможности принятия профессиональных	Текущий контроль: опрос, тест Промежуто	61-100 баллов

		ная работа	решений в пределах своих полномочий, совершать иные действия, связанные с реализацией правовых норм ***Уметь:*** выявлять источники информации, системно их анализировать в целях принятия профессиональных решений ***Владеть:*** способностью обосновывать принимаемые решения в пределах должностных обязанностей	чная аттестация: зачет	

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

Вопросы к опросу

1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Определение информационной безопасности.
4. Место информационной безопасности в системе национальной безопасности.

5. Интересы личности в информационной сфере.
6. Интересы общества в информационной сфере.
7. Интересы государства в информационной сфере.
8. Угрозы информационному обеспечению государственной политики Российской Федерации.
9. Виды угроз информационной безопасности.
10. Внешние источники угроз информационной безопасности.
11. Внутренние источники угроз информационной безопасности государства.
12. Информационное оружие, его классификация и возможности.
13. Доктрина информационной войны.
14. Методы и средства ведения информационной войны
15. Понятие информационного противоборства
16. Причины искажения информации,
17. Виды искажения информации
18. Каналы утечки информации
19. Естественные и искусственные каналы утечки информации
20. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
21. Критерии и классы защищенности средств ВТ
22. Компьютерная система как объект информационной безопасности.
23. Информационные процессы как объект информационной безопасности
24. Влияние человеческого фактора на обеспечение информационной безопасности
25. Программно-аппаратные средства обеспечения информационной безопасности.
26. Классификация программно-аппаратных средств обеспечения информационной безопасности
27. Защита от несанкционированного доступа
28. Антивирусная защита
29. Межсетевые экраны
30. Криптографические методы защиты информации

Тесты для проведения текущего контроля и промежуточной аттестации по итогамосвоения дисциплины «Информационная безопасность».

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

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

11) Принципом политики информационной безопасности является принцип:
- невозможности миновать защитные средства сети (системы)
- усиления основного звена сети, системы
- полного блокирования доступа при риск-ситуациях

12) 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

13) Принципом политики информационной безопасности является принцип:
- разделения доступа (обязанностей, привилегий) клиентам сети (системы)

- одноуровневой защиты сети, системы
- совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
- компьютерный сбой
- логические закладки («мины»)
- аварийное отключение питания

15) 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

16) Принцип Кирхгофа означает:
- секретность ключа определена секретностью открытого сообщения
- секретность информации определена скоростью передачи данных
- секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:
- электронно-цифровой преобразователь
- электронно-цифровая подпись
- электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- покупка нелицензионного ПО
- ошибки эксплуатации и неумышленного изменения режима работы системы
- сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:
- распределенный доступ клиент, отказ оборудования
-моральный износ сети, инсайдерство
- сбой (отказ) оборудования, нелегальное копирование данных

20) 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

21) Утечкой информации в системе называется ситуация, характеризуемая:
- потерей данных в системе
- изменением формы информации
- изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- целостность

- доступность
- актуальность

23) Угроза информационной системе (компьютерной сети) – это:
- вероятное событие
- детерминированное (всегда определенное) событие
- событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- регламентированной
- правовой
- защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
- программные, технические, организационные, технологические
- серверные, клиентские, спутниковые, наземные
- личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
- владелец сети
- администратор сети
- пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
- руководств, требований обеспечения необходимого уровня безопасности
- инструкций, алгоритмов поведения пользователя в сети
- норм информационного права, соблюдаемых в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:
- аудит, анализ затрат на проведение защитных мер
- аудит, анализ безопасности
- аудит, анализ уязвимостей, риск-ситуаций

Вопросы к зачету.

31. Понятие национальной безопасности.
32. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
33. Определение информационной безопасности.
34. Место информационной безопасности в системе национальной безопасности.

35. Интересы личности в информационной сфере.
36. Интересы общества в информационной сфере.
37. Интересы государства в информационной сфере.
38. Угрозы информационному обеспечению государственной политики РоссийскойФедерации.
39. Виды угроз информационной безопасности.
40. Внешние источники угроз информационной безопасности.
41. Внутренние источники угроз информационной безопасности государства.
42. Информационное оружие, его классификация и возможности.
43. Доктрина информационной войны.
44. Методы и средства ведения информационной войны
45. Понятие информационного противоборства
46. Причины искажения информации,
47. Виды искажения информации
48. Каналы утечки информации
49. Естественные и искусственные каналы утечки информации
50. Правовые, организационно-технические и экономические методы обеспеченияинформационной безопасности.
51. Критерии и классы защищенности средств ВТ
52. Компьютерная система как объект информационной безопасности.
53. Информационные процессы как объект информационной безопасности
54. Влияние человеческого фактора на обеспечение информационной безопасности
55. Программно-аппаратные средства обеспечения информационной безопасности.
56. Классификация программно-аппаратных средств обеспечения информационнойбезопасности
57. Защита от несанкционированного доступа
58. Антивирусная защита
59. Межсетевые экраны
60. Криптографические методы защиты информации

5.2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

В ходе преподавания дисциплины «Информационная безопасность» используютсяследующие *оценочные средства:*

Вид работы	Кол-во баллов (максимальное значение)
Опрос	до 40 баллов
Тест	до 40 баллов
зачет	до 20 баллов

Шкала оценивания опроса и собеседования

Уровень оценивания	Критерии оценивания	Баллы
Опрос и собеседование	Свободное владение материалом	40
	Достаточное усвоение материала	39-20
	Поверхностное усвоение материала	19-10
	Неудовлетворительное усвоение материала	9-1

Шкала оценивания тестового задания

Уровень оценивания	Критерии оценивания	Баллы
Тестирование	89-70 правильных ответа	40
	71-40 правильных ответа	39-20
	41-20 правильных ответа	19-10
	менее 12 правильных	9-1

Описание шкалы оценивания зачета

Шкала оценивания зачета

Уровень оценивания	Критерий оценивания	Баллы /конвертируемые баллы	Оценка
Зачет	**Полный и правильный ответ на теоретический вопрос.** Глубокое и прочное усвоение знаний программного материала (умение выделять главное, существенное); исчерпывающее, последовательное, грамотное и логически стройное изложение; правильность формулировки понятий; знание источников и авторов-исследователей по данной проблеме; умение сделать вывод по излагаемому материалу.	81-100 /8-10	Зачтено
	Теоретический вопрос изложен достаточно. Достаточно полное знание программного материала; грамотное изложение материала по существу; отсутствие не существенных неточностей в формулировке понятий; умение сделать вывод. Допускается недостаточно последовательное и логическое изложение материала.	61-80 /5-7	
	Теоретический вопрос изложен неполно. Общие знания основного материала без усвоения некоторых существенных положений; формулировка основных понятий, но – с	41-60 /2-4	

	некоторой неточностью; отсутствие знаний гражданско-правовых источников и авторов-исследователей по данной проблеме.		
	Теоретический вопрос изложен плохо или с грубыми ошибками. Незнание значительной части программного материала; существенные ошибки в процессе изложения; неумение выделить существенное и сделать выводы; незнание или ошибочные определения понятий.	0-40 /0-1	Не зачтено

Перевод баллов в шкалу оценок представлен в таблице.

Количество баллов	Зачет
81–100	Зачтено
61–80	
41–60	
0–40	Не зачтено

6. Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература

Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. О безопасности: Федеральный закон от 28.12.2010 N 390-ФЗ//Собрание законодательства РФ, 03.01.2011, N 1, ст. 2.
3. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. N 149-ФЗ (ред. от 02.12.219)// Собраниезаконодательства РФ, 31.07.2006, N 31 (1 ч.), ст. 3448.
4. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: Федеральный закон от 9 февраля 2009 г. N 8-ФЗ 28.12.2017)// Собрание законодательства РФ, 16.02.2009, N 7, ст. 776.
5. О персональных данных: Федеральный закон от 27 июля 2006 г. N 152-ФЗ // Собрание законодательства РФ, 31.07.2006, N 31 (1 ч.), ст. 3451.
6. О лицензировании отдельных видов деятельности: Федеральный закон от 4.05.2011 № 99-ФЗ (в ред. от 02.08.2019).// Собрание законодательства РФ", 09.05.2011, N19, ст. 2716.
7. Об электронной цифровой подписи: Федеральный закон от 06.04.2011 № 63-ФЗ

Учебники, учебные пособия

5. Нестеров С.А. Информационная безопасность. ЮРАЙТ. 2019. – 321 с.
6. Баранова Е.К. Информационная безопасность и защита информации: учебное пособие. – М.: РИОР. 2018. – 400 с.
7. Мельников В.П. Защита информации: учебник. – М.: Академия, 2019. - 320 с.

б) Дополнительная литература

1. Краковский Ю.М. Защита информации: ученое пособие. – РнД: Феникс. 2017. – 347 с.

2. Кураков Л. П. Информация как объект правовой защиты / Л.П. Кураков, С.Н. Смирнов. - М.: Гелиос, 2018. - 240 с.
3. Хорев П.Б. Программно-аппаратная защита информации: учебное п особие. – М.:Форум. 2018. – 352 с.
4. Кузнецова А.В. Искусственный интеллект и информационная безопасностьобщества. – М.: Русайнс. 2017. – 64 с.
5. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежныйопыт: монография. – М.: ЮНИТИ. 2015. - 239 с.

6.3 Ресурсы информационно-телекоммуникационной сети «Интернет»

Справочно-правовая система «Консультант Плюс». Справочно-правовая система «Гарант». http://www.cbr.ru/
http://www.asv.org.ru/

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Методические указания по планированию и организации самостоятельной работы бакалавров. Надысева Э.Х.

8. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ ОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Лицензионное программное обеспечение:Microsoft Windows
Microsoft Office
Kaspersky Endpoint Security

Информационные справочные системы:
Система ГАРАНТ
Система «КонсультантПлюс»
Профессиональные базы данных
fgosvo.ru

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины включает в себя:

- учебные аудитории для проведения занятий лекционного и семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные учебной мебелью, доской, демонстрационным оборудованием *(если в РПД предусмотренапрезентация).*
- помещения для самостоятельной работы, укомплектованные учебной мебелью, персональными компьютерами с подключением к сети Интернет и обеспечением доступа к электронным библиотекам и в электронную информационно-образовательную средуМГОУ;
- помещения для хранения и профилактического обслуживания учебного оборудования, укомплектованные мебелью (шкафы/стеллажи), наборами

демонстрационного оборудования и учебно-наглядными пособиями.