Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Нижегородский институт управления – филиал РАНХиГС
(наименование института (факультета))
Кафедра правового обеспечения национальной безопасности
(наименование кафедры)

УТВЕРЖДЕНО
Директор Нижегородского института управления – филиала РАНХиГС

Парамонов Александр Васильевич
Подписано цифровой подписью: Парамонов Александр Васильевич
Дата: 2024.05.30 14:07:42 +03'00'

ПРОГРАММА МАГИСТРАТУРЫ

«Юридическое обеспечение национальной безопасности»
(наименование образовательной программы)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ, реализуемой с применением электронного (онлайн) курса

Б1.В.07 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
(индекс и наименование дисциплины, в соответствии с учебным планом)
40.04.01 ЮРИСПРУДЕНЦИЯ
(код и наименование направления подготовки)

заочная
(форма обучения)

Год набора - 2024

Нижний Новгород, 2024 г.

Автор(ы)–составитель(и):

Старший преподаватель кафедры правового обеспечения национальной безопасности — С.В. Кочеткова
(ученая степень и(или) ученое звание, должность, наименование кафедры) (Ф.И.О.)

Заведующий кафедрой правового обеспечения национальной безопасности, канд.юрид.наук, доцент — М.В. Балалаева
(ученая степень и(или) ученое звание, должность, наименование кафедры) (Ф.И.О.)

РПД Б1.В.07 Информационная безопасность одобрена на заседании кафедры правового обеспечения национальной безопасности
Протокол от 09 февраля 2024 г. № 7.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 4
2.Объем и место дисциплины в структуре образовательной программы 5
3.Содержание и структура дисциплины 5
4.Материалы текущего контроля успеваемости обучающихся по дисциплине 7
5.Оценочные материалы промежуточной аттестации по дисциплине 11
6.Методические материалы для освоения дисциплины 13
7.Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет" 16
7.1. Основная литература 16
7.2. Дополнительная литература 16
7.3. Учебно-методическое обеспечение 16
7.4. Нормативные правовые документы и иная правовая информация 17
7.5. Интернет-ресурсы 21
7.6. Иные источники 21
8.Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы 21

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

1.1. Дисциплина *Б1.В.07 «Информационная безопасность»* обеспечивает овладение следующими компетенциями:

Таблица 1

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
ПКс-2.1.	Способен устранять признаки нарушения требований законодательства в сфере безопасности Российской Федерации	ПКс-2.1.2	Способен выявлять и оценить признаки правонарушения в области требований законодательства в сфере безопасности Российской Федерации

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Таблица 2

ОТФ/ТФ/трудовые или профессиональные действия	Код компонента компетенции	Результаты обучения
Организация и осуществление криминалистической деятельности, связанной с проведением следственных и иных процессуальных действий с целью предварительного расследования преступлений (ОТФ (А) Выполнение отдельных функций процессуального контроля (ТФ (А/02.7)	Пкс-2.1.2	**на уровне знаний*:*** – национальные интересы Российской Федерации в информационной сфере; – основные угрозы информационной безопасности; – нормативную базу, регулирующую вопросы обеспечения информационной безопасности; – силы и средства, формы и методы обеспечения информационной безопасности;
		на уровне умений: – анализировать и правильно применять правовые нормы в сфере обеспечения информационной безопасности; – выявлять признаки нарушения требований законодательства в сфере обеспечения информационной безопасности Российской Федерации; – оценивать и квалифицировать выявленные правонарушения, посягающие на информационную безопасность;
		– выбирать правовые средства и методы противодействия, адекватные выявленным нарушениям законодательства в сфере обеспечения информационной безопасности Российской Федерации;

2. Объем и место дисциплины в структуре образовательной программы

Дисциплина *«Информационная безопасность»* является дисциплиной части, формируемой участниками образовательных отношений и в соответствии с учебным планом осваивается на 3 курсе при заочной форме обучения, общая трудоемкость дисциплины в зачетных единицах – 4 (144 академических часа /108 астрономических часов).

Для освоения дисциплины *«Информационная безопасность»* обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения дисциплин: *«Государственная и общественная безопасность», «Кибер*

преступления и национальная безопасность», «Национальная оборона и военная безопасность», «Техногенная безопасность», «Экологическая и природоресурсная безопасность», «Энергетическая безопасность», «Научно-исследовательская работа».

Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся:

Вид учебных занятий и самостоятельная работа		Всего
Заочная форма обучения		
Контактная работа обучающихся с преподавателем, в том числе:		*24*
лекционного типа (Л)		*8*
практического (семинарского) типа (ПЗ)		*14*
консультация		2
Самостоятельная работа обучающихся (СР)		111
Промежуточная аттестация	форма	*экзамен*
	час.	*9*
Общая трудоемкость (час. / з.е.)		*144/4*

Форма промежуточной аттестации в соответствии с учебным планом – экзамен.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Таблица 3

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости**, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ЭО, ДОТ*	ЛР/ЭО, ДОТ*	ПЗ/ЭО, ДОТ*	КСР		
Тема 1	Информационная безопасность как составляющая общественной безопасности	16	1		2		13	УО
Тема 2	Основы информационной безопасности и защиты информации	16	1		2		13	УО
Тема 3	Виды и особенности угроз информационным ресурсам	16	1		2		13	СЗ
Тема 4	Основные направления и этапы работ по созданию комплексной системы информационной безопасности организации	16	1		2		13	УО
Тема 5	Основные направления деятельности службы безопасности организации по защите информационных ресурсов	16	1		2		13	УО
Тема 6	Особенности работы с персоналом, владеющим конфиденциальной информацией	16	1		2		13	СЗ
Тема 7	Защищенный документооборот	15	1		1		13	Д
Тема 8	Инженерно-технические и программные методы защиты информации	22	1		1		20	Т
	Консультация	2						
Промежуточная аттестация		9						экзамен
Всего (в з.е., акад. часах, астр. часах):		**4/144/ 108**	**8/6**		**14/10.5**		**111/ 83,25**	**2/1,5 9/6,75**

Примечание:

** – при применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом*

*** – формы текущего контроля успеваемости: Т- тесты, УО – устный опрос, Д — доклады, СЗ — ситуационные задачи*

3.2 Содержание дисциплины

ТЕМА 1. *[Информационная безопасность как составляющая общественной* безопасности*]*.

1. Система национальной безопасности Российской Федерации.
2. Информационная безопасность как элемент национальной безопасности.
3. Международные договоры и программные документы Российской Федерации в области информационной безопасности.
4. Законодательство о безопасности и защите информации, его структура и содержание.

ТЕМА 2. *[Основы информационной безопасности и защиты информации]*.

1. Понятие и цели защиты информации. Соотношение понятий «информационная безопасность», «безопасность информации», «защита информации».
2. Цели, задачи, уровни обеспечения информационной безопасности.
3. Основные угрозы жизненно важным интересам личности, общества, государства в информационной сфере.
4. Формы и методы обеспечения информационной безопасности.
5. Информационная безопасность и компьютеризация информационной среды.

ТЕМА 3. *[Виды и особенности угроз информационным ресурсам]*.

1. Правовой режим информационных ресурсов.
2. Риски угроз информационным ресурсам.
3. Документирование информации как способ ее защиты.
4. Институт тайн в законодательстве Российской Федерации.
5. Понятие и виды правонарушений в информационной сфере.

ТЕМА 4. *[Основные направления и этапы работ по созданию комплексной системы информационной безопасности организации]*.

1. Аналитическая работа по выявлению угроз информационной безопасности.
2. Понятие, цели, задачи, принципы построения, элементы системы защиты конфиденциальной информации.
3. Компьютерные технологии и формирование основ системы защиты информации.
4. Формирование и актуализация системы в реальных обстоятельствах, изменения в соотношении элементов системы в соответствии с типом организации и видами угроз.
5. Сертификация систем и средств защиты информационных систем и информационных ресурсов.

ТЕМА 5. *[Основные направления деятельности службы безопасности организации по защите информационных ресурсов]*.

1. Службы безопасности в организациях различных типов.
2. Задачи и функции подразделений служб безопасности по защите информации.
3. Формы и методы деятельности службы безопасности организации по защите информации.
4. Взаимодействие службы безопасности и службы персонала по защите информации.
5. Назначение и взаимосвязь плановой и контрольной работы службы безопасности, их место в построении и функционировании комплексной системы защиты информации организации.

ТЕМА 6. *[Особенности работы с персоналом, владеющим конфиденциальной информацией]*.

1. Угрозы безопасности информации, исходящие от персонала и направления противодействия им.

2. Задачи и стадии работы с персоналом, обладающим конфиденциальными сведениями.

3. Организация доступа персонала к конфиденциальным сведениям, документам и базам данных.

4. Принципы, организационные формы и методика обучения сотрудников правилам обеспечения безопасности информации.

5. Методы контроля соблюдения персоналом правил работы с конфиденциальной информацией.

6. Правовая ответственность персонала за разглашение информации ограниченного доступа.

ТЕМА 7. *[Защищенный документооборот]*.

1. Понятие и задачи, основные требования к защищённому документообороту.

2. Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков.

3. Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации.

4. Технологические системы защиты и обработки документов, содержащих сведения ограниченного доступа.

5. Принципы учёта, технология обработки подготовленных документов, содержащих сведения ограниченного доступа.

ТЕМА 8. [*Инженерно-технические и программные методы защиты информации*].

1. Физические средства защиты информации.

2. Виды, назначение, задачи и организационные формы охраны объектов, функции персонала охраны, их значение для защиты информации.

3. Классификация и характеристика классификационных групп технических средств защиты информации.

4. Программно-технические методы обеспечения информационной безопасности.

5. Критерии оценки защищённости систем информационной безопасности компьютерной информации.

6. Основные виды компьютерных вирусов. Профилактика вирусного заражения.

7. Криптографические средства защиты информации.

4. Материалы текущего контроля успеваемости обучающихся по дисциплине

4.1.. В ходе реализации дисциплины «Информационная безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 4

Тема (раздел)	**Методы текущего контроля успеваемости**
Информационная безопасность как составляющая общественной безопасности	Устный опрос
Основы информационной безопасности и защиты информации	Устный опрос
Виды и особенности угроз информационным ресурсам	Ситуационные задачи
Основные направления и этапы работ по созданию комплексной системы информационной безопасности организации	Устный опрос
Основные направления деятельности службы безопасности организации по защите информационных ресурсов	Устный опрос
Особенности работы с персоналом, владеющим конфиденциальной информацией	Ситуационные задачи

Тема (раздел)	Методы текущего контроля успеваемости
Защищенный документооборот	Доклады
Инженерно-технические и программные методы защиты информации	Тестирование

4.2. Типовые материалы текущего контроля успеваемости.

Примерные оценочные материалы по теме 1. Информационная безопасность как составляющая общественной безопасности

Примерные вопросы для устного опроса:

1. Система национальной безопасности Российской Федерации.
2. Информационная безопасность как элемент национальной безопасности.
3. Международные договоры и программные документы Российской Федерации в области информационной безопасности.
4. Законодательство о безопасности и защите информации, его структура и содержание.

Примерные оценочные материалы по теме 2. Основы информационной безопасности и защиты информации

Примерные вопросы для устного опроса:

1. Понятие и цели защиты информации. Соотношение понятий «информационная безопасность», «безопасность информации», «защита информации».
2. Цели, задачи, уровни обеспечения информационной безопасности.
3. Основные угрозы жизненно важным интересам личности, общества, государства в информационной сфере.
4. Формы и методы обеспечения информационной безопасности.
5. Информационная безопасность и компьютеризация информационной среды.

Примерные оценочные материалы по теме 3. Виды и особенности угроз информационным ресурсам

Примерные ситуационные задачи:

Задача 1.

Комаров И.Н. приобрел лицензионный CD-диск с программами для ЭВМ и сделал с него резервную копию для личного пользования.

Дайте юридическую оценку действиям Комарова. Назовите нормативные акты, регулирующие описанные правоотношения.

Задача 2.

Семёнов И.К. приобрел в магазине лицензионный DWD-диск с электронной энциклопедией, сделал с него копию и подарил ее на день рождения своему другу Лаврентьеву К.В.

Дайте правовую оценку действиям Семёнова. Охарактеризуйте юридические полномочия Семёнова как собственника данного DWD-диска.

Задача 3.

Гаврилов Н.С. приобрёл у знакомого диск с нелицензионным программным продуктом, который не работал из-за встроенных в него модулей, защищающих от несанкционированной активации. Тогда Гаврилов скачал в сети «Интернет» специальную компьютерную программу, запуск которой обеспечил нейтрализацию средств защиты и работу программного продукта.

Квалифицируйте действия Гаврилова. Подлежит ли он юридической ответственности?

Примерные оценочные материалы по теме 4. Основные направления и этапы работ по созданию комплексной системы информационной безопасности организации

Примерные вопросы для устного опроса:

1. Аналитическая работа по выявлению угроз информационной безопасности.
2. Понятие, цели, задачи, принципы построения, элементы системы защиты конфиденциальной информации.
3. Компьютерные технологии и формирование основ системы защиты информации.
4. Формирование и актуализация системы в реальных обстоятельствах, изменения в соотношении элементов системы в соответствии с типом организации и видами угроз.
5. Сертификация систем и средств защиты информационных систем и информационных ресурсов.

Примерные оценочные материалы по теме 5. Основные направления деятельности службы безопасности организации по защите информационных ресурсов

Примерные вопросы для устного опроса:

1. Службы безопасности в организациях различных типов.
2. Задачи и функции подразделений служб безопасности по защите информации.
3. Формы и методы деятельности службы безопасности организации по защите информации.
4. Взаимодействие службы безопасности и службы персонала по защите информации.
5. Назначение и взаимосвязь плановой и контрольной работы службы безопасности, их место в построении и функционировании комплексной системы защиты информации организации.

Примерные оценочные материалы по теме 6. Особенности работы с персоналом, владеющим конфиденциальной информацией]

Примерные ситуационные задачи:

Задача 1.

В ООО «Фортуна» введён режим коммерческой тайны. Доступ к сведениям, составляющим коммерческую тайну данной организации, для выполнения своих функциональных обязанностей необходим начальнику производственного цеха Кузнецову С.О., переведённой с другой должности на должность старшего менеджера по работе с персоналом Игнатьевой Л.М. и поступающей на должность бухгалтера Соколовой Н.А.

Помимо этого, сведения, составляющие коммерческую тайну ООО «Фортуна», необходимы для выполнений обязательств по договору контрагенту ООО «Успех», контракт о сотрудничестве с которым находится в стадии разработки.

Каким образом следует организовать доступ указанных лиц к сведениям, составляющим коммерческую тайну ООО «Фортуна» с точки зрения обеспечения информационной безопасности? Составьте проекты необходимых документов.

Задача 2.

Служба безопасности ООО «Интеграл» выявила утечку конфиденциальной информации, содержащейся в документах ограниченного доступа, регулярно используемых несколькими сотрудниками организации.

Опишите порядок действий сотрудников службы безопасности при проведении проверки по данному факту.

Задача 3.

Государственный служащий при изменении должностных обязанностей, для выполнения которых ему далее необходимо будет работать с документами под грифом

«секретно», отказался проходить проверку на допуск к сведениям, составляющими государственную тайну.

Назовите, какие действия в данном случае должен предпринять представитель работодателя.

Примерные оценочные материалы по теме 7. Защищенный документооборот

Примерные темы докладов:

1. Понятие и задачи, основные требования к защищённому документообороту.
2. Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков.
3. Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации.
4. Технологические системы защиты и обработки документов, содержащих сведения ограниченного доступа.
5. Принципы учёта, технология обработки подготовленных документов, содержащих сведения ограниченного доступа.

Примерные оценочные материалы по теме 8. Инженерно-технические и программные методы защиты информации

Примерные варианты тестовых заданий:

1. Основная особенность компьютерных вирусов заключается:

а) в возможности их самопроизвольного внедрения в различные объекты операционной

системы;

б) в возможности наказания деструктивного влияния на информацию;

в) в возможности заражения окружающих;

г) в возможности их внедрения злоумышленниками.

2. Действие Закона «О лицензировании отдельных видов деятельности» не распространяется на:

а) образовательную деятельность в области защиты информации;

б) деятельность по технической защите конфиденциальной информации;

в) предоставление услуг в области шифрования информации;

г) деятельность по созданию компьютерных баз данных.

3. В число универсальных сервисов безопасности не входят:

а) экранирование;

б) протоколирование;

в) аудит;

г) средства построения виртуальных локальных сетей.

4. При анализе стоимости защитных мер следует учитывать:

а) расходы на закупку оборудования;

б) расходы на закупку программ;

в) расходы на обучение персонала;

г) расходы на премирование сотрудников организации выявивших или предотвративших

нарушение информационной безопасности.

5. Первый шаг в анализе угроз - это:

а) прогнозирование возможности возникновения угрозы;

б) идентификация угроз;

в) аутентификация угроз;

г) ликвидация угроз.

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1. Экзамен проводится с применением следующих методов (средств): проведение устного экзамена, включающего теоретическую часть и практико-ориентированное задание, требующее демонстрации уровня владения умениями/навыками.

5.2. Оценочные материалы промежуточной аттестации

Таблица 5

Код компонента освоения компетенции	Компонент освоения компетенции	Код промежуточного индикатора освоения компетенции	Промежуточный индикатор освоения компетенции	Критерий оценивания
ПКс -2.1.2	Способен выявлять и оценить признаки правонарушения в области требований законодательства в сфере безопасности Российской Федерации	ИПКс -2.1.2	Показывает способность выявлять и оценить признаки правонарушения в области требований законодательства в сфере безопасности Российской Федерации	Умеет формулировать правовую позицию, составлять и оформлять необходимые документы для реализации мероприятий по обеспечению информационной безопасности Российской Федерации.

Типовые оценочные материалы промежуточной аттестации

Вопросы для экзамена по дисциплине:

1. Система национальной безопасности Российской Федерации.
2. Информационная безопасность как элемент национальной безопасности.
3. Национальные интересы Российской Федерации в информационной сфере.
4. Международные договоры и программные документы Российской Федерации в области информационной безопасности.
5. Доктрина информационной безопасности РФ об основных угрозах в информационной сфере и их источниках.
6. Законодательство о безопасности и защите информации, его структура и содержание.
7. Понятие и цели защиты информации.
8. Соотношение понятий «информационная безопасность», «безопасность информации», «защита информации».
9. Цели, задачи, уровни обеспечения информационной безопасности.
10. Принципы, задачи, функции и стандарты обеспечения информационной безопасности.
11. Основные субъекты обеспечения информационной безопасности России.
12. Формы и методы обеспечения информационной безопасности.
13. Информационная безопасность и компьютеризация информационной среды.
14. Документированная информация как объект информационных правоотношений.
15. Электронный документ и электронный документооборот.
16. Документирование информации как способ ее защиты.
17. Информационные ресурсы: понятие, виды, правовой режим информационных ресурсов.

18. Риски угроз информационным ресурсам.
19. Информационные системы: понятие, назначение, признаки.
20. Программы для ЭВМ и базы данных как модули информационной системы.
21. Информационно-телекоммуникационные сети: понятие, значение.
22. Понятие и виды информационных технологий, порядок их создания и основные направления внедрения.
23. Правовые режимы информации: общая характеристика.
24. Режим свободного доступа к информации.
25. Институт тайны как правовой режим информации ограниченного доступа.
26. Виды тайн, их общая характеристика.
27. Правовое регулирование информационных отношений в области государственной тайны.
28. Правовое регулирование информационных отношений в области коммерческой тайны.
29. Особенности информационных правоотношений, возникающих при производстве, передаче и распространении персональных данных.
30. Основные угрозы жизненно важным интересам личности, общества, государства в информационной сфере.

Практико-ориентированные (практические) задания к экзамену:

ПКс-2.1.2 Способен выявлять и оценить признаки правонарушения в области требований законодательства в сфере безопасности Российской Федерации

Задание 1.

Журналист Петров О.А. при проведении журналистского расследования произвёл скрытую видеосъёмку встречи предпринимателя Иванова Ф.Л. и сотрудника областной администрации Сидорова Н.С. На видеозаписи был зафиксирован факт передачи Ивановым Сидорову небольшого свёртка, завёрнутого в непрозрачный полиэтиленовый пакет.

Допускается ли распространение в средствах массовой информации сообщений и материалов, подготовленных с использованием скрытой аудио- и видеозаписи, кино- и фотосъемки? Какой нормативно-правовой акт регламентирует действия журналиста в описанной ситуации?

Задание 2.

ООО «Фиеста», специализирующееся на электронных публикациях литературных произведений в сети Интернет, при размещении материалов использует специальный плагин, препятствующий копированию текста.

Назовите нормативный акт, описывающий применение технических средств защиты авторских прав. Для решения каких задач они могут применяться?

Задание 3.

Сотрудник НИИ «Гамма» Соколов Н.Ф. участвовал в НИОКР по разработке приборов для новых образцов военной техники, поставляемой в Вооружённые Силы Российской Федерации.

Назовите возможные временные ограничения прав Соколова Н.Ф. во время работы в НИИ «Гамма». Укажите, в каком нормативном акте приведён их перечень.

Шкала оценивания

Промежуточная аттестация проводится в форме экзамена без применения балльно-рейтинговой системы оценивания - посредством аттестационных испытаний в форме традиционного экзамена.

Результаты промежуточной аттестации оцениваются по традиционной балльной системе оценивания («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»).

Наряду с оцениванием учебных достижений обучающихся по принятой образовательной организации системе оценок и использованием ее при оформлении официальных дипломов Академии о высшем образовании, вводят повышенный («Excellent» и «Good») и базовый («Very good» и «Satisfactory») уровень оценок «отлично» и «хорошо» для использования при оформлении ЕПД, согласно Положению об оформлении и выдаче ЕПД.

Таблица 6.

Соответствие академической оценке

Академическая оценка		Оценка по шкале ESTS	
зачтено	отлично	Passed	A (Excellent)
			B (Very Good)
	хорошо		C (Good)
			D (Satisfactory)
	удовлетворительно		E (Sufficient)
не зачтено	неудовлетворительно	-	-

Оценивание результатов промежуточного контроля (экзамен)

Оценка «отлично» выставляется обучающемуся:

– если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно излагает его на экзамене, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение; учебные достижения и результаты текущего контроля успеваемости демонстрируют высокую степень сформированности соответствующих компетенций.

Оценка «хорошо» выставляется обучающемуся:

– если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения; учебные достижения и результаты текущего контроля успеваемости демонстрируют хорошую степень сформированности соответствующих компетенций.

Оценка «удовлетворительно» выставляется обучающемуся:

– если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ; учебные достижения и результаты текущего контроля успеваемости демонстрируют удовлетворительную степень сформированности соответствующих компетенций.

Оценка «неудовлетворительно» выставляется обучающемуся:

– если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы; учебные достижения и результатами текущего контроля успеваемости демонстрируют низкую степень сформированности соответствующих компетенций.

6. Методические материалы по освоению дисциплины

Обучение по дисциплине предполагает изучение курса на аудиторных занятиях (лекции, практические/семинарские) и самостоятельной работы студентов. Практические/семинарские занятия дисциплины предполагают их проведение в

различных формах с целью выявления полученных знаний, умений, навыков и компетенций.

Подготовка к лекции студентами заключается в следующем:

– повторить материал предыдущей лекции, прочитав его повторно;

– ознакомиться с темой предстоящей лекции (в рабочей программе учебной дисциплины);

– ознакомиться с учебными материалами по данной теме в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины или с электронными материалами, предложенными лектором;

– записать возможные вопросы, которые можно будет задать лектору.

Подготовка к практическим (семинарским) занятиям:

– внимательно прочитать материал лекций относящихся и к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы, предложенные в рабочей программе дисциплины для обсуждения;

– выполнить задания, если они предусмотрены в письменной форме;

– понять, что для вас осталось неясными и постараться получить на них ответ заранее;

– готовиться к практическим/семинарским занятиям можно как индивидуально, так и в составе малой группы;

– рабочую программу учебной дисциплины необходимо использовать в качестве основного ориентира в организации обучения;

– электронной версии рабочей программы по дисциплине размещена на сайте Нижегородского института управления и предоставлен авторизованный доступ.

Подготовка к промежуточной аттестации. К промежуточной аттестации необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно-методической документацией:

– программой дисциплины;

– перечнем знаний и умений, которыми студент должен владеть;

– тематическими планами лекций, семинарских занятий;

– учебником, учебными пособиями по дисциплине, а также электронными ресурсами;

– перечнем и тематикой письменных работ, а также методическими рекомендациями по их выполнению;

– перечнем экзаменационных вопросов.

Систематическое выполнение всех видов заданий на лекциях, практических/семинарских занятиях, а также самостоятельная работа позволит успешно освоить дисциплину и создать хорошую базу для прохождения промежуточной аттестации.

Вопросы для самостоятельной подготовки к практическим занятиям

Тема 1. Информационная безопасность как составляющая общественной безопасности

1. Система национальной безопасности Российской Федерации.

2. Информационная безопасность как элемент национальной безопасности.

3. Международные договоры и программные документы Российской Федерации в области информационной безопасности.

4. Законодательство о безопасности и защите информации, его структура и содержание.

Тема 2. Основы информационной безопасности и защиты информации

1. Понятие и цели защиты информации. Соотношение понятий «информационная безопасность», «безопасность информации», «защита информации».
2. Цели, задачи, уровни обеспечения информационной безопасности.
3. Основные угрозы жизненно важным интересам личности, общества, государства в информационной сфере.
4. Формы и методы обеспечения информационной безопасности.
5. Информационная безопасность и компьютеризация информационной среды.

Тема 3. Виды и особенности угроз информационным ресурсам

1. Правовой режим информационных ресурсов.
2. Риски угроз информационным ресурсам.
3. Документирование информации как способ ее защиты.
4. Институт тайн в законодательстве Российской Федерации.
5. Понятие и виды правонарушений в информационной сфере.

Тема 4. Основные направления и этапы работ по созданию комплексной системы информационной безопасности организации

1. Аналитическая работа по выявлению угроз информационной безопасности.
2. Понятие, цели, задачи, принципы построения, элементы системы защиты конфиденциальной информации.
3. Компьютерные технологии и формирование основ системы защиты информации.
4. Формирование и актуализация системы в реальных обстоятельствах, изменения в соотношении элементов системы в соответствии с типом организации и видами угроз.
5. Сертификация систем и средств защиты информационных систем и информационных ресурсов.

Тема 5. Основные направления деятельности службы безопасности организации по защите информационных ресурсов

1. Службы безопасности в организациях различных типов.
2. Задачи и функции подразделений служб безопасности по защите информации.
3. Формы и методы деятельности службы безопасности организации по защите информации.
4. Взаимодействие службы безопасности и службы персонала по защите информации.
5. Назначение и взаимосвязь плановой и контрольной работы службы безопасности, их место в построении и функционировании комплексной системы защиты информации организации.

Тема 6. Особенности работы с персоналом, владеющим конфиденциальной информацией

1. Угрозы безопасности информации, исходящие от персонала и направления противодействия им.
2. Задачи и стадии работы с персоналом, обладающим конфиденциальными сведениями.
3. Организация доступа персонала к конфиденциальным сведениям, документам и базам данных.
4. Принципы, организационные формы и методика обучения сотрудников правилам обеспечения безопасности информации.
5. Методы контроля соблюдения персоналом правил работы с конфиденциальной информацией.

6. Правовая ответственность персонала за разглашение информации ограниченного доступа.

Тема 7. Защищенный документооборот

1. Понятие и задачи, основные требования к защищённому документообороту.
2. Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков.
3. Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации.
4. Технологические системы защиты и обработки документов, содержащих сведения ограниченного доступа.
5. Принципы учёта, технология обработки подготовленных документов, содержащих сведения ограниченного доступа.

Тема 8. Инженерно-технические и программные методы защиты информации

1. Физические средства защиты информации.
2. Виды, назначение, задачи и организационные формы охраны объектов, функции персонала охраны, их значение для защиты информации.
3. Классификация и характеристика классификационных групп технических средств защиты информации.
4. Программно-технические методы обеспечения информационной безопасности.
5. Критерии оценки защищённости систем информационной безопасности компьютерной информации.
6. Основные виды компьютерных вирусов. Профилактика вирусного заражения.
7. Криптографические средства защиты информации.

7.Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет"

7.1. Основная литература.

1. Информационное право : учебник для вузов / Н.Н. Ковалева, И.И. Брянцев, О.В.Брянцева [и др.] ; под редакцией Н.Н. Ковалевой. - Москва : Юрайт, 2021. - 353 с. - (Высшее образование). - ISBN 978-5-534-13786-6. - Текст : электронный // ЭБС "Юрайт" : [сайт]. - URL: https://urait.ru/bcode/477219 (дата обращения: 27.08.2021). - Режим доступа: по подписке.

2. Кардашова, И.Б. Основы теории национальной безопасности : учебник для вузов / И.Б. Кардашова. - 2-е изд. ; перераб. и доп. - Москва : Юрайт, 2021. - 332 с. - (Высшее образование). - ISBN 978-5-534-12725-6. - Текст : электронный // ЭБС "Юрайт" : [сайт]. - URL: https://urait.ru/bcode/472932 (дата обращения: 27.08.2021). - Режим доступа: по подписке.

3. Рассолов, И.М. Информационное право : учебник и практикум для вузов / И.М.Рассолов. - 6-е изд. ; перераб. и доп. - Москва : Юрайт, 2021. - 415 с. - (Высшее образование). - ISBN 978-5-534-14327-0. - Текст : электронный // ЭБС "Юрайт" : [сайт]. - URL: https://urait.ru/bcode/479850 (дата обращения: 27.08.2021). - Режим доступа: по подписке.

7.2. Дополнительная литература.

1. Бачило, И.Л. Информационное право : учебник для вузов / И.Л. Бачило. - 5-е изд. ; перераб. и доп. - Москва : Юрайт, 2021. - 419 с. - (Высшее образование). - ISBN 978-5-534-00608-7. - Текст : электронный // ЭБС "Юрайт" : [сайт]. -

URL: https://urait.ru/bcode/468354 (дата обращения: 27.08.2021). - Режим доступа: по подписке.

2. Информация как правовая категория : учебное пособие для вузов / Ю.В. Волков. - 2-е изд. - Москва : Юрайт, 2021. - 109 с. - (Высшее образование). - ISBN 978-5-534-07052-1. - Текст : электронный // ЭБС "Юрайт" : [сайт]. - URL: https://urait.ru/bcode/474484 (дата обращения: 27.08.2021). - Режим доступа: по подписке.

3. Костенко, М.А. Права человека и национальная безопасность : учебное пособие / М.А. Костенко, О.А. Лупандина. - Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2019. - 107 с. - ISBN 978-5-9275-3403-6. - Текст : электронный // ЭБС "IPRBooks" : [сайт]. - URL: http://www.iprbookshop.ru/100188.html (дата обращения: 27.08.2021). - Режим доступа: по подписке.

7.3. Учебно-методическое обеспечение самостоятельной работы.

Электронные информационно-образовательные ресурсы Нижегородского института управления – филиала РАНХиГС URL: http://sdo.niu.ranepa.ru/

7.4. Нормативные правовые документы.

1. Всеобщая декларация прав человека (принята 10 декабря 1948 г. Генеральной Ассамблеей ООН) // Международное публичное право: Сборник документов. Т. 1. М.: БЕК, 1996.

2. Международный пакт о гражданских и политических правах от 19 декабря 1966 г.

3. Резолюция № 428 (1970) Консультативной ассамблеи Совета Европы «Относительно Декларации о средствах массовой информации и правах человека (принята 23 января 1970 г. на 21-й сессии Консультативной ассамблеи Совета Европы).

4. Заключительный акт Совещания по безопасности и сотрудничеству в Европе от 1 августа 1975 г.

5. Декларация об основных принципах, касающихся вклада средств массовой информации в укрепление мира и международного взаимопонимания, в развитие прав человека и борьбу против расизма и апартеида и подстрекательства к войне (принята 28 ноября 1978 г.).

6. Конвенция о защите физических лиц при автоматизированной обработке персональных данных ETS N 108 (Страсбург, 28 января 1981 г.).

7. Декларация основных принципов правосудия для жертв преступлений и злоупотреблений властью (принята 29 ноября 1985 г. Резолюцией 40/34 Генеральной Ассамблеи ООН).

8. Директива «О правовой охране компьютерных программ (91/250/ЕЭС) (Брюссель, 14 мая 1991 г.).

9. Декларация о правах и свободах человека и гражданина Российской Федерации от 22 декабря 1991 г.

10. Всеобщая декларация о геноме человека и правах человека (принята 11 ноября 1997 г. на 29-й сессии Генеральной конференции ЮНЕСКО) // Международное публичное право: Сборник документов. Т. 1. М.: БЕК, 1996.

11. Окинавская хартия глобального информационного общества от 22 июля 2000.

12. Типовой закон ЮНСИТРАЛ об электронных подписях (принят ЮНСИТРАЛ 5 июля 2001 г.)

13. Коммюнике глав государств и правительств «Группы восьми» (Генуя, 22 июля 2001 г.).

14. Конвенция о киберпреступности, принятая Советом Европы 23 ноября 2001 г.,

15. Декларация «Партнерство во имя будущего» (Бангкок, 21 октября 2003 г.)

16. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) // «Собрание законодательства РФ», 04.08.2014, N 31, ст. 4398.

17. Федеральный конституционный закон от 30 мая 2001 г. № 3-ФКЗ «О чрезвычайном положении» (с послед. изм. и доп.) // СЗ РФ. 2001. № 23. Ст. 2277.

18. Федеральный конституционный закон от 30 января 2002 года № 1-ФКЗ «О военном положении» // СЗ РФ. 2002. № 5. Ст. 375.

19. Гражданский кодекс Российской Федерации (с послед изм. и доп.) // СЗ РФ. 1994. № 32. Ст. 3301; 1996. N 5. Ст. 410; 2001. N 49. Ст. 4552; 2006. N 52. Ст. 5496.

20. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с послед. изм. и доп.) // СЗ РФ. 1996. № 25. Ст. 2954.

21. Налоговый кодекс РФ.Ч. 1. от 31 июля 1998 года № 146 (с послед. изм. и доп.) // СЗ РФ. 1998. № 31. Ст. 3824.

22. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (с послед. изм. и доп.) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1.

23. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (с послед. изм. и доп.) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 3.

24. Арбитражно-процессуальный кодекс РФ от 24 июля 2002 года № 95-ФЗ (с послед. изм. и доп.) // СЗ РФ. 2002. № 30. Ст. 3012.

25. Федеральный закон от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» (с послед. изм. и доп.) // СЗ РФ. 1994. № 35. Ст. 3648.

26. Федеральный закон от 29 декабря 1994 г. № 77-ФЗ «Об обязательном экземпляре документов» (с послед. изм. и доп.) // СЗ РФ. 1995. № 1. Ст. 1.

27. Федеральный закон от 29 декабря 1994 г. № 78-ФЗ «О библиотечном деле» (с послед. изм. и доп.) // СЗ РФ. 1995. № 1. Ст. 2.

28. Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «Об органах федеральной службы безопасности в Российской Федерации» (с послед. изм. и доп.) // СЗ РФ. 1995. № 15. Ст. 1269.

29. Федеральный закон от 19 мая 1995 г. № 82-ФЗ «Об общественных объединениях» (с послед. изм. и доп.) // СЗ РФ. 1995. № 21. Ст. 1930.

30. Федеральный закон от 18 июля 1995 г. № 108-ФЗ «О рекламе» (с послед. изм. и доп.) // СЗ РФ. 1995. № 30. Ст. 2864.

31. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (с послед. изм. и доп.) // СЗ РФ. 1995. № 33. Ст. 3349.

32. Федеральный закон от 17 ноября 1995 г. № 168-ФЗ «О прокуратуре Российской Федерации» (с послед. изм. и доп.) // СЗ РФ. 1995. № 47. Ст. 4472.

33. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (с послед. изм. и доп.) // СЗ РФ. 2002. № 30. Ст. 3031.

34. Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» // СЗ РФ. 2002. № 2. Ст. 127.

35. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (с послед. изм. и доп.) // СЗ РФ. 2003. № 28. Ст. 2895.

36. Федеральный закон от 10 января 2003 г. № 20-ФЗ «О государственной автоматизированной системе РФ «Выборы» (с послед. изм. и доп.) // СЗ РФ. 2003. № 2. Ст. 172.

37. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (с послед. изм. и доп.) // СЗ РФ. 2004, № 32, ст. 3283

38. Федеральный закон от 22 октября 2004 г. № 125-ФЗ; «Об архивном деле в Российской Федерации» (с послед. изм. и доп.) // СЗ РФ. 2004. № 43. Ст. 4169.

39. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» (с послед. изм. и доп.) // СЗ РФ. 2006. № 11. ст. 1146.

40. Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» // СЗ РФ. 2006. № 19. Ст. 2060.

41. Федеральный закон от 13 марта 2006 г. № 38-ФЗ; «О рекламе» (с послед. изм. и доп.) // СЗ РФ. 2006. № 12. ст. 1232.

42. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с послед. изм. и доп.) // СЗ РФ. 2006. № 31. ст. 3448.

43. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (с послед. изм. и доп.) // СЗ РФ. 2006. № 31. ст. 3451.

44. Федеральный закон от 28 февраля 2010 г. № 390-ФЗ «О безопасности» (с послед. изм. и доп.) // СЗ РФ. 2011. № 1. Ст. 2.

45. Федеральный закон от 07 февраля 2011 г. № 3-ФЗ «О полиции» (с послед. изм. и доп.) // СЗ РФ. 2011. № 7. Ст. 900.

46. Федеральный закон от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации" (с послед. изм. и доп.) // СЗ РФ. 2012. № 53 (ч.1). Ст. 7598.

47. Закон РФ от 21 июля 1993 № 5485-I «О государственной тайне» (с послед. изм. и доп.) // СЗ РФ. 1997. N 41.

48. Закон Российской Федерации от 11 марта 1992 г. № 2487-I «О частной детективной и охранной деятельности в Российской Федерации» (с послед. изм. и доп.) // ВСНД и ВС РФ. 1992. № 17. Ст. 888.

49. Закон РФ от 9 октября 1992 г. № 3612-1 «Основы законодательства Российской Федерации о культуре» (с послед. изм. и доп.) // Ведомости СНД РФ и ВС РФ. 1992. № 46. Ст. 2615.

50. Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» (с послед. изм. и доп.) // Ведомости СНД РФ и ВС РФ. 1992. № 7. Ст. 300.

51. Указ Президента РФ от 17 февраля 1995 г. № 161 «О гарантиях права граждан на охрану здоровья при распространении рекламы» (с послед. изм. и доп.) // СЗ РФ. 1956. № 8. Ст. 659.

52. Указ Президента РФ от 30 ноября 1995 г. №1203; «О перечне сведений, отнесенных к государственной тайне» (с послед. изм. и доп.) // СЗ РФ. 1998. №5. Ст.561; 2001. №24. Ст.2418.

53. Указ Президента РФ от 06 марта1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с послед. изм. и доп.) // СЗ РФ. 1997. N 10. Ст. 1127.

54. Указ Президента РФ от 15 февраля 2006 г. № 116 «О мерах по противодействию терроризму» (с послед. изм. и доп.) // СЗ РФ. 2006. № 8. Ст. 897.

55. Указ Президента РФ от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».

56. Указ Президента РФ от 18 мая 2009 г. № 559 «О представлении гражданами, претендующими на замещение должностей федеральной государственной службы, и федеральными государственными служащими сведений о доходах, об имуществе и обязательствах имущественного характера» (с послед. изм. и доп.) // СЗ РФ. 2009. № 21. Ст. 2544.

57. «Положение о Межведомственной комиссии по защите государственной тайны» утверждено Указом Президента РФ от 20 января 1996 г. №71 // СЗ РФ. 1996. № 4. Ст. 268.

58. Доктрина информационной безопасности РФ. Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895 // Российская газета. 2000. 28 сентября.

59. Концепция национальной безопасности Российской Федерации: Утверждена Указом Президента РФ от 17 декабря 1997 г. № 1300 (в редакции Указа Президента РФ от 10 января 2000 г. № 24). // СЗ РФ. 2000. № 2. Ст. 170.

60. Стратегия развития информационного общества в Российской Федерации. Утверждена Президентом РФ от 07.02.2008 №Пр-212.

61. Постановление Правительства РФ от 04 сентября 1995 г. № 870 «Правила отнесения сведений составляющих государственную тайну, к различным степеням секретности» (с послед. изм. и доп.) // СЗ РФ. 1995. № 37. Ст. 3619.

62. Постановление Правительства РФ от 28 февраля 1999 г. № 226 «О государственном учете и регистрации баз и банков данных» (с послед. изм. и доп.) // СЗ РФ. 1999 №12. Ст.1114.

63. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 №273-ФЗ.

64. Приказ Министерства науки и высшего образования Российской Федерации от 06.04.2021 №245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»

65. Образовательный стандарт ФГБОУ ВО «Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации», утвержденный приказом ректора Академии от 29.03.2021 г. № 01-3038 и разработанного на основе федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 40.04.01 Юриспруденция, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 25.11.2020 г. № 1451 (зарегистрировано в Министерстве юстиции Российской Федерации 09.03.2021 г., регистрационный № 62681).

66. Приказ Минтруда России от 23.03.2015 № 183н «Об утверждении профессионального стандарта «Следователь-криминалист» (рег.Минюст 0.7.04.2015 № 36755).

67. ГОСТ 6.10.4-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, созданным средствами вычислительной техники. М.: Изд-во Стандартов, 1985.

68. ГОСТ 6.10.1-88. Унифицированные системы документации. Основные положения. М.: Изд-во Стандартов, 1988.

69. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования. М., 1990.

70. ГОСТ Р 50922-96. Защита информации: Основные термины и определения. М., 1996.

71. ГОСТ Р 6.30-97. Унифицированные системы документации: Система организации норм распорядительной документации: Требования к оформлению документов. М.: Госстандарт. 1998.

72. ГОСТ 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования и методы испытания. М.: Изд-во Стандартов, 1999.

73. ГОСТ 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М., 2000.

74. ГОСТ Р 6.30-2003. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов. М.: Госстандарт, 2003.

7.5. Интернет-ресурсы.

1. Официальный сайт Государственной Думы Российской Федерации [Электронный ресурс] / Режим доступа: http://www.duma.gov.ru/ свободный. - Загл. с экрана.

2. Официальный сайт Правительства Российской Федерации [Электронный ресурс] / Режим доступа: http://government.ru// свободный. - Загл. с экрана.

3. Официальный сайт Президента Российской Федерации [Электронный ресурс] / Режим доступа: http://kremlin.ru/свободный. - Загл. с экрана.

4. Официальный сайт Совета Федерации Федерального Собрания Российской Федерации [Электронный ресурс] / Режим доступа: http://www.council.gov.ru/ свободный. - Загл. с экрана.

7.6. Иные источники.

1. Практикум : учебное пособие для вузов / Н.Н. Ковалева, Н.А. Жирнова, Ю.М. Тугушева, Е.В. Холодная ; под редакцией Н.Н. Ковалевой. - Москва : Юрайт, 2021. - 159 с. - (Высшее образование). - ISBN 978-5-534-12442-2. - Текст : электронный // ЭБС "Юрайт" : [сайт]. - URL: https://urait.ru/bcode/476680 (дата обращения: 27.08.2021). - Режим доступа: по подписке.

2. Информационное право : уч ебник / М.Б. Смоленский, М.В. Алексеева. - Москва : КноРус, 2021. - 166 с. - ISBN 978-5-406-02829-2. - Текст : электронный // ЭБС "BOOK.RU" : [сайт]. - URL: http://www.book.ru/book/936286 (дата обращения: 27.08.2021). - Режим доступа: по подписке.

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

8.1. Материально-техническая база

Перечень материально-технического обеспечения:

1. Учебные аудитории, оборудованные для проведения учебных занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, коллоквиумов, мероприятий текущего контроля и промежуточной аттестации, в том числе мультимедийным оборудованием для демонстрации электронных презентаций и аудио- и видеоматериалов.
2. Компьютерные классы для выполнения групповых тестовых и иных заданий, а также для самостоятельной работы обучающихся оснащенные компьютерной техникой и обеспечением доступа к сети «Интернет» и доступа в электронную информационно-образовательную среду организации.
3. Специализированные аудитории и лаборатории.
4. Библиотека с обеспечением печатными изданиями или электронно-библиотечная система обеспечивающая доступ к электронным изданиям (электронная библиотека).
5. Читальный зал.
6. Технические средства обучения: персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV и др.

8.2. Информационные технологии, программное обеспечение:

При осуществлении образовательного процесса по дисциплине используется информационные технологии и программное обеспечение:

1. Современная операционная система.
2. Kaspersky Endpoint Security (или аналог).
3. Средство просмотра файлов формата pdf.
4. Современные офисные средства (текстовые и табличные редакторы, средства работы с презентационными материалами и т.д.).
5. Архиватор 7-Zip.

6. Система дистанционного обучения.
7. Автоматизированная библиотечная система.

8.3 Информационные справочные системы:

1. https://www.urait.ru –Электронно-библиотечная система [ЭБС] Юрайт;
2. http://www.iprbookshop.ru – Электронно-библиотечная система [ЭБС] «IPR SMART» (ранее – IPRBooks)
3. https://e.lanbook.com - Электронно-библиотечная система [ЭБС] «Лань».
4. https://znanium.com - Электронно-библиотечная система [ЭБС] «Znanium.com».
5. https://www.book.ru - Электронно-библиотечная система [ЭБС] «Book.ru».
6. https://ibooks.ru - Электронно-библиотечная система [ЭБС] «ibooks.ru».
7. https://www.ezproxy.ranepa.ru:2443/login?url=https://dlib.eastview.com/ – East View. Полные тексты российских научных и практических журналов, а так же газет центральной прессы России.
8. https://www.ezproxy.ranepa.ru:2443/login?url=https://grebennikon.ru/ - Полные тексты 38 научно-практических журналов по маркетингу, менеджменту, финансам и управлению персоналом ИД «Гребенников»
9. http://www.consultant.ru/ - Справочно-правовая система «Консультант».
10. http://www.garant.ru/ Справочно-правовая система «Гарант».