Лебедева Екатерина Александровна
Подписано цифровой подписью: Лебедева Екатерина Александровна
Дата: 2026.06.23 11:53:33 +03'00'

Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.04.02 ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(индекс, наименование дисциплины в соответствии с учебным планом)

09.04.03 Прикладная информатика
(код, наименование направления подготовки)

«Информационные технологии в государственном и муниципальном управлении»
(наименование образовательной программы)

очная, заочная форма обучения
(форма обучения)

Год набора – 2026
Нижний Новгород, 2026 г.

Автор(ы)-составитель(и) РПД:

Лапатников Максим Владимирович, доцент кафедры правового обеспечения национальной безопасности, канд. юрид. наук, доцент

Заведующий кафедрой:

Балалаева Марина Викторовна, канд. юрид. наук, доцент, заведующий кафедрой правового обеспечения национальной безопасности

Рабочая программа дисциплины Б1.В.ДВ.04.02 Правовые основы информационной безопасности одобрена на заседании кафедры правового обеспечения национальной безопасности

протокол № 7 от «20» февраля 2026 г.

СОДЕРЖАНИЕ

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

2. Объем и место дисциплины в структуре образовательной программы

3. Содержание и структура дисциплины

4. Типы оценочных материалов, показатели и критерии их оценивания

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

7. Методические материалы по освоению дисциплины

8. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»

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

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

Дисциплина *Б1.В.ДВ.04.02 Правовые основы информационной безопасности* обеспечивает формирование у обучающихся следующих профессиональных компетенций:

ОТФ/ТФ и реквизиты ПС *(при наличии)*	**Код компетенции**	**Наименование компетенции**	**Код индикатора достижения компетенций**	**Наименование индикатора достижения компетенций**	**Образовательный результат**
ОТФ. D/09.7 Разработка инструментов и методов адаптации бизнес-процессов заказчика к возможностям ИС в рамках управления работами по сопровождению и проектами создания (модификации)	ПК-12	способен проектировать информационные процессы и системы с использованием инновационных инструментальных средств, адаптировать современные ИКТ к задачам прикладных ИС.	ИПК-12.2	Применяет технологии подбора современных ИКТ в соответствии с решаемыми прикладными задачами с учетом действующих правовых норм.	*ИПК-12.2 З-1* **Знает** методы анализа прикладной области, методологии и технологии проектирования информационных систем; ИПК-12.2 З-2 **Знает** методики, методы и средства управления процессами проектирования, состав функциональных и обеспечивающих подсистем информационных систем; ИПК-12.2 У-1 **Умеет** разрабатывать компоненты информационного, программного, технического и технологического обеспечений, включая описание и создание нормативно-справочной, оперативной информации и результатных данных, разработку человеко-машинного интерфейса, написание пользовательской документации; ИПК-12.2 У-2 **Умеет** применять типовые проектные решения и пакеты прикладных программ в зависимости от условий задачи.

D/08.7 Разработка инструментов и методов проектирования бизнес-процессов заказчика в рамках управления работами по сопровождению и проектами создания (модификации) ИС D/09.7 Разработка инструментов и методов адаптации бизнес-процессов заказчика к возможностям ИС в рамках управления работами по сопровождению и проектами создания (модификации) ИС D/17.7 Организационное и технологическое обеспечение разработки баз данных ИС в рамках управления работами по сопровождению и проектами создания (модификации) ИС	ПК-20	Способен использовать международные информационные ресурсы и стандарты в информатизации предприятий и организаций.	ИПК-20.2	Применяет международные стандарты и информационные ресурсы на практике, внедряя их в производственно-технологический процесс	ИПК-20.2 У-1 **Умеет** применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы; ИПК-20.2 У-2 **Умеет** применять методы алгоритмизации, языки и технологии программирования при решении профессиональных задач в области информационных систем и технологий; ИПК-20.2 У-3 **Умеет** осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем, применять современные технологии для реализации информационных систем.

2. Объем и место дисциплины в структуре образовательной программы

Общая трудоемкость дисциплины составляет 72 а.ч. (2 з.е.)

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

- очная форма обучения: лекции – 8 а.ч., практические занятия – 24 а.ч., самостоятельная работа – 48 а.ч.
- заочная форма обучения: лекции – 4 а.ч., практические занятия – 8 а.ч., самостоятельная работа – 56 а.ч., контроль – 4 а.ч..

Дисциплина Б1.В.ДВ.04.02 «Правовые основы информационной безопасности» входит в в число дисциплин по выбору части, формируемой участниками образовательных отношений, Блока 1 Дисциплины (модули) в соответствии с учебным планом.

Освоение дисциплины опирается на необходимый объем теоретических знаний, полученных при изучении таких дисциплин, как Тенденции развития Web- пространства (Б1.О.07); Технологии межведомственного электронного взаимодействия (Б1.В.01.05), Организационные основы обеспечения

информационной безопасности (Б1.В.ДВ.03.01); Программно-техническое обеспечение компьютерной безопасности (Б1.В.ДВ.03.02).

Форма промежуточной аттестации в соответствии с учебным планом – зачет.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час											Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа		
			Период теоретического обучения						Период промежуточной аттестации (сессия)					
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Каттэк	Контроль	СРкр	СРэк	СР
			Л	ВЛ	ЛР	ПЗ								
Тема 1	Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасности.	8	2	0	0	2	0	0	0	0		0	0	4	Устный опрос
Тема 2	Основные понятия, виды и источники информации, подлежащей защите.	8	0	0	0	2	0	0	0	0		0	0	6	Устный опрос
Тема 3	Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности	12	2	0	0	4	0	0	0	0		0	0	6	Устный опрос, ситуационная задача
Тема 4	Понятие и режим	12	0	0	0	4	0	0	0	0		0	0	8	Устный

	государственной тайны. Понятие и режим коммерческой тайны в РФ.													опрос,
Тема 5	Проблемы и угрозы информационной безопасности.	12	2	0	0	4	0	0	0	0	0	0	6	Устный опрос,
Тема 6	Особенности работы с персоналом, владеющим конфиденциальной информацией	8	0	0	0	4	0	0	0	0	0	0	4	Устный опрос,
Тема 7	Защищенный документооборот	8	2	0	0	4	0	0	0	0	0	0	2	Устный опрос, ситуационная задача
Промежуточная аттестация														Зачет
Итого		**72**	**8**			**24**	**0**	**0**	**0**				**48**	

Заочная форма обучения

№ п/п	**Наименование тем и (или) разделов**		**Объем дисциплины, ак.час**												**Форма текущего контроля успеваемости, промежуточной аттестации**
		ВСЕГО	**Контактная работа обучающихся с преподавателем по видам учебных занятий**									**Самостоятельная работа**			
			Период теоретического обучения						**Период промежуточной аттестации (сессия)**						
			Занятия лекционного типа		**Занятия семинарского типа**		**ИК**	**КСР**	**КЭ**	**Кат тэк**	**Контроль**	**СРкр**	**СРэк**	**СР**	
			Л	**ВЛ**	**ЛР**	**ПЗ**									
Тема 1	Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасно-	10	1	0	0	1	0	0	0	0		0	0	8	Устный опрос, тест

	сти.													
Тема 2	Основные понятия, виды и источники информации, подлежащей защите.	9	0	0	0	1	0	0	0	0	0	0	8	Самостоятельная работа
Тема 3	Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности	10	1	0	0	1	0	0	0	0	0	0	8	Самостоятельная работа
Тема 4	Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ.	10	0	0	0	1	0	0	0	0	0	0	9	Устный опрос,
Тема 5	Проблемы и угрозы информационной безопасности.	12	1	0	0	1	0	0	0	0	0	0	10	Самостоятельная работа
Тема 6	Особенности работы с персоналом, владеющим конфиденциальной информацией	8	0	0	0	1	0	0	0	0	0	0	7	Самостоятельная работа
Тема 7	Защищенный документооборот	9	1	0	0	2	0	0	0	0	0	0	6	Самостоятельная работа
Промежуточная аттестация		4								4				Зачет
Итого		72	4			8	0	0	0	4			56	

Используемые сокращения:

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях,).

ВЛ – видео лекции. ЛР – лабораторные работы. ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы
КЭ – консультации перед экзаменом
Каттэк – контактная работа на аттестацию в период экзаменационных сессий
СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.
СРэк – самостоятельная работа на подготовку к экзамену. СР – самостоятельная работа в семестре на подготовку к учебным занятия

3.2. Содержание дисциплины

Тема 1 Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасности.

Основные понятия. Общие положения. Типы и виды информационной безопасности. Участники отношений в области информационной безопасности. Федеральные, региональные, местные законы по информационной безопасности. Основные международные акты, регулирующие сферу информационной безопасности.

Объективные и субъективные предпосылки создания глобального общества. Роль Интернета в мировом информационном пространстве. Глобальные ожидания и опасения человечества. Негативные последствия глобальной информатизации общества.

Конституция РФ о правовом обеспечении информационной сферы. Федеральное законодательство в сфере информационной безопасности. Федеральные законы, Указы Президента РФ и иные нормативно-правовые акты по вопросам информационной безопасности. Организационное обеспечение информационной безопасности.

Международное сотрудничество России в области обеспечения информационной безопасности.

Тема 2 Основные понятия, виды и источники информации, подлежащей защите.

Информация и право. Научно-технический прогресс и условия формирования информационного общества. Информатика и правовые дисциплины. Информационное право.

Виды информации, подлежащей защите. Понятие информации с ограниченным доступом.

Виды конфиденциальной информации: тайна частной жизни, коммерческая тайна, банковская тайна,

Тема 3 Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности

Методы государственного регулирования информационной безопасности. Программы развития информационной безопасности. Статистическое наблюдение в области информационной безопасности. Государственная поддержка информационной безопасности в Российской федерации. Информационное обеспечение информационной

Тема 4 Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ.

Понятие государственной тайны, правовое регулирование. Режим государственной тайны. Перечень сведений, запрещенных к засекречиванию:

- ✓ о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- ✓ о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- ✓ о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- ✓ о фактах нарушения прав и свобод человека и гражданина;
- ✓ о размерах золотого запаса и государственных валютных резервов Российской Федерации;
- ✓ о состоянии здоровья высших должностных лиц Российской Федерации;
- ✓ о фактах нарушения законности органами государственной власти и их должностными лицами.

Понятие коммерческой тайны, правовое регулирование. Режим коммерческой тайны. Практика правового регулирования и защиты коммерческой тайны за рубежем.

Тема 5 Проблемы и угрозы информационной безопасности.

Понятие информационной безопасности. Основные проблемы информационной безопасности и пути их решения. Виды и источники угроз информационной безопасности. Информационные противостояния от древности до Нового времени. Информационные войны XXI века. Место информационной безопасности в системе национальной безопасности России.

Тема 6 Особенности работы с персоналом, владеющим конфиденциальной информацией

Угрозы безопасности информации от персонала и направления ее защиты. Задачи и стадии работы с персоналом, обладающим конфиденциальными сведениями.

Доступ персонала к конфиденциальным сведениям, документам и базам данных

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

Методы контроля соблюдения персоналом правил работы с конфиденциальной информацией. Правовая ответственность персонала за разглашение информации ограниченного доступа.

Тема 7 Защищенный документооборот

Понятие и задачи, основные требования к защищённому документообороту. Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков.

Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации. Технологические системы защиты и обработки документов, содержащих сведения ограниченного доступа.

Принципы учёта документов, содержащих сведения ограниченного доступа.

Технология обработки подготовленных документов, содержащих сведения ограниченного доступа.

Порядок работы персонала с документами, содержащих сведения ограниченного доступа. Проверка наличия документов, дел и носителей информации.

Формирование и хранение дел, содержащих информацию ограниченного доступа.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.ДВ.04.02 «Правовые основы информационной безопасности» входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляют фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа — это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос

сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа — это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	Прочитайте текст, выберите правильные ответы	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	Ответ считается верным, если правильно указана вся последовательность цифр
Задание комбинированного типа с	Прочитайте текст, выберите правильный	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных	Ответ считается верным, если правильно указана цифра или буква

выбором одного правильного ответа из предложенных и обоснованием выбора	ответ и запишите аргументы, обосновывающие выбор ответа	вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	и приведены корректные аргументы, используемые при выборе ответа
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	1. Внимательно прочитать текст задания и понять суть вопроса. 2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки. 4.В случае расчетной задачи, записать решение и ответ	Ответ считается верным: 1. Отсутствие фактических ошибок. 2. Раскрытие объема используемых понятий (полнота ответа). 3.Обоснованность ответа (наличие аргументов). 4. Логическая последовательность излагаемого материала.

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС

Итоговая балльная оценка	**Традиционная система**	**Бинарная система**	**ECTS**	
			Для традиционной системы	**Для бинарной системы**
95-100	Отлично	Зачтено	A	P/ Passed
85-94			B	P/ Passed
75-84	Хорошо		C	P/ Passed
65-74			D	P/ Passed
55-64	Удовлетворительно		E	P/ Passed
0-54	Неудовлетворительно	Не зачтено	F	F/Failed

Соотношение баллов за текущий контроль успеваемости и промежуточную аттестацию, а также повторную промежуточную аттестацию:

Максимальная сумма баллов за текущий контроль успеваемости	Максимальная сумма баллов за промежуточную аттестацию	Максимальная итоговая балльная оценка	Максимальная сумма баллов за повторную промежуточную аттестацию
60 баллов	40 баллов	100 баллов	100 баллов

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

5.1. В ходе реализации дисциплины Б1.В.ДВ.04.02 «Правовые основы информационной безопасности» используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Устный опрос, ситуационная задача, тестирование.

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек):

Тема 1. *Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасности.* ИПК-12.2

Вопросы для устного опроса:

1. Какие основные задачи решает правовое регулирование в сфере информационной безопасности на международном уровне?

2. Назовите ключевые международные стандарты, регулирующие информационную безопасность, и поясните их значение для организаций.

3. В чём заключаются особенности национального законодательства Российской Федерации в области информационной безопасности по сравнению с международными стандартами?

Ситуационные задачи

1. Составьте сравнительную таблицу, в которой отразите основные положения российского законодательства и международных стандартов (*ISO/IEC 27001, GDPR*) по защите персональных данных.

2. Составьте таблицу, в которой сопоставьте основные международные стандарты в области информационной безопасности, их назначение и область применения.

Тема 2. *Основные понятия, виды и источники информации, подлежащей защите* ИПК-12.2

Вопросы для устного опроса:

1. Что такое информация, подлежащая защите? Приведите примеры.

2. Какие основные виды информации выделяют в законодательстве Российской Федерации с точки зрения необходимости её защиты?

3. Что такое персональные данные? Какие категории персональных данных существуют?

Ситуационные задачи

1. Составьте таблицу, в которой сопоставьте основные виды информации, подлежащей защите, с их определениями и примерами.

2. Заполните таблицу, отражающую основные источники информации, подлежащей защите, и возможные угрозы для каждого источника.

Тема 3. *Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности* ИПК-12.2

Вопросы для устного опроса:

1.Каковы основные цели и задачи государственной политики Российской Федерации в области информационной безопасности?

2.Какие нормативные правовые акты определяют основы государственной политики в сфере информационной безопасности в России?

3. Назовите ключевые принципы обеспечения информационной безопасности, закреплённые в Доктрине информационной безопасности РФ.

Ситуационные задачи

1. Составьте таблицу, отражающую основные направления государственной политики Российской Федерации в области информационной безопасности.

2. Заполните таблицу, сопоставив органы государственной власти и их функции в сфере обеспечения информационной безопасности.

Тема 4. *Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ* ИПК-12.2

Вопросы для устного опроса:

1. Что такое государственная тайна? Каковы её основные признаки?
2. Какие сведения могут быть отнесены к государственной тайне в Российской Федерации?
3. Назовите основные уровни степени секретности сведений, составляющих государственную тайну, и их отличия.

Ситуационные задачи

1. Составьте сравнительную таблицу «Государственная тайна и коммерческая тайна: понятие и основные признаки».
2. Заполните таблицу «Степени секретности сведений, составляющих государственную тайну».

Тема 5. *Проблемы и угрозы информационной безопасности* ИПК-12.2

Вопросы для устного опроса:

1. Что такое угроза информационной безопасности? Приведите примеры.
2. Какие основные виды угроз информационной безопасности вы знаете?
3. В чём различие между умышленными и неумышленными угрозами? Приведите примеры.

Ситуационные задачи

1. Составьте таблицу, в которой классифицируйте основные угрозы информационной безопасности по источнику возникновения.
2. Заполните таблицу, отражающую основные виды кибератак и их краткое описание

Тема 6. *Особенности работы с персоналом, владеющим конфиденциальной информацией* ИПК-12.2

Вопросы для устного опроса:

1. Почему работа с персоналом, имеющим доступ к конфиденциальной информации, считается одним из ключевых направлений обеспечения информационной безопасности?
2. Какие этапы включает в себя работа с сотрудниками при приёме на работу, связанную с доступом к конфиденциальным сведениям?
3. Каковы основные обязанности сотрудника, допущенного к конфиденциальной информации?

Тема 7. *Защищенный документооборот* ИПК-12.2

Вопросы для устного опроса:

1. Что такое защищённый документооборот и каковы его основные цели?
2. Какие виды документов подлежат обязательной защите в организации?

3. В чём отличие защищённого электронного документооборота от традиционного бумажного?

Ситуационные задачи

1. Составьте сравнительную таблицу «Особенности бумажного и электронного защищённого документооборота».

2. Заполните таблицу, отражающую основные этапы жизненного цикла защищённого документа и меры безопасности на каждом этапе.

5.3. Один или несколько тематических блоков дисциплины завершаются контрольной точкой (далее – КТ). Текущий контроль успеваемости по дисциплине предусматривает не менее 2 (двух) и не более 10 (десяти) КТ в течение периода освоения дисциплины.

Максимальное количество баллов за любой тип работ в рамках КТ составляет 100 (сто) баллов.

Распределение весовых коэффициентов по КТ в рамках текущего контроля успеваемости по дисциплине и формулы расчета:

Наименование контрольной точки	Максимальное количество баллов за работу в рамках КТ, которое может набрать обучающийся	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,1	10
КТ 2	100	0,2	20
КТ 3	100	0,3	30
Итого:	x	0,6	60

Формула расчета результата контрольной точки:

Результат контрольной точки = Количество баллов за работу в рамках КТ X Коэффициент веса контрольной точки.

5.4. Формы текущего контроля успеваемости обучающихся в рамках КТ и типовые оценочные материалы:

КТ – 1.
Тема 1-7.

Тематика докладов:

1. Эволюция правового регулирования информационной безопасности в России и мире: сравнительный анализ.
2. Влияние международных стандартов *ISO/IEC 27001* на формирование национальных систем защиты информации.
3. *GDPR* как эталон регулирования персональных данных: опыт внедрения и уроки для России.
4. Роль международных организаций (*ISO, ITU, ENISA*) в разработке стандартов информационной безопасности.
5. Проблемы гармонизации российского и международного законодательства в сфере ИБ.

6. Классификация информации ограниченного доступа: государственная, коммерческая, служебная тайна.
7. Персональные данные как особый объект правовой защиты: современные вызовы и решения.
8. Источники угроз информационной безопасности в современных организациях.
9. Профессиональная тайна: понятие, виды и особенности правового регулирования.
10. Значение классификации информации для построения системы защиты в компании.
11. Доктрина информационной безопасности РФ: ключевые направления и реализация.
12. Государственная политика России в области защиты критической информационной инфраструктуры.
13. Организационно-правовые методы обеспечения информационной безопасности в банковской сфере.
14. Роль Банка России в формировании системы финансово-информационной безопасности страны.
15. Взаимодействие государственных органов и бизнеса в противодействии киберугрозам.
16. Государственная тайна: понятие, степени секретности и порядок допуска.
17. Коммерческая тайна как инструмент защиты конкурентных преимуществ предприятия.
18. Сравнительный анализ режима государственной и коммерческой тайны в РФ.
19. Ответственность за разглашение государственной и коммерческой тайны: анализ законодательства.
20. Практика введения режима коммерческой тайны в российских компаниях: проблемы и решения.

.

Методические рекомендации по подготовке доклада.

Подготовка доклада способствует формированию навыков исследовательской работы, расширяет познавательные интересы, приучает критически мыслить. При написании доклада по заданной теме составляется план, подбираются основные источники. В процессе работы с источниками, систематизируют полученные сведения, делают выводы и обобщения.

Подготовка доклада требует от обучающегося большой самостоятельности и серьезной интеллектуальной работы, которая принесет наибольшую пользу, если будет включать с себя следующие этапы: изучение наиболее важных научных работ по данной теме, перечень которых дает сам преподаватель; анализ изученного материала, выделение наиболее значимых для раскрытия темы фактов, мнений разных ученых и научных положений; обобщение и логическое построение материала доклада, например, в форме развернутого плана; написание текста доклада с соблюдением требований научного стиля.

Построение доклада включает три части: вступление, основную часть и заключение. Во вступлении указывается тема доклада, устанавливается логическая связь ее с другими темами или место рассматриваемой проблемы среди других проблем, дается краткий обзор источников, на материале которых раскрывается тема и т. п. Основная часть должна иметь четкое логическое построение, в ней должна быть раскрыта тема доклада. В заключении обычно подводятся итоги, формулируются выводы, подчеркивается значение рассмотренной проблемы и т. п.

Критерии оценивания доклада:

Критерии оценки	Диапазон баллов	Описание критерия
Содержание и раскрытие темы	0-20	Детальное, последовательное описание всех этапов с конкретными примерами
Грамотность изложения	0-20	Соблюдены все правила грамматики, орфографии и пунктуации
Стилистика	0-20	Единый стиль изложения, точные формулировки, уместное использование терминов, лаконичность
Логика изложения	0-20	Чёткая последовательность изложения, логические связи между частями текста, аргументы подтверждают выводы
Оригинальность	0-20	Уникальный подход к теме, нестандартные решения, инновационные идеи, собственная позиция автора
Итого максимально:	100	

КТ – 2.

Тема 1 - 7.
Устный опрос:

Вопросы для опроса:

№ п.п.	Содержание вопроса
1.	Какие основные задачи решает правовое регулирование в сфере информационной безопасности?
2.	Назовите ключевые международные стандарты в области информационной безопасности и их значение для организаций.
3.	В чём заключаются основные различия между национальным и международным регулированием ИБ?
4.	Как международные стандарты (*ISO/IEC 27001*, *GDPR*) влияют на формирование национальных правовых актов?
5.	Какие категории информации подлежат обязательной защите согласно российскому законодательству?
6.	Дайте определение персональным данным, коммерческой тайне, служебной тайне. В чём их различия?
7.	Перечислите основные источники информации, подлежащей защите, в современной организации.
8.	Почему важно классифицировать информацию по степени конфиденциальности?

9.	Каковы основные цели государственной политики РФ в области информационной безопасности?
10.	Какие органы государственной власти отвечают за реализацию политики ИБ в России?
11.	Что такое финансово-информационная безопасность и почему она выделяется в отдельное направление?
12.	Какова роль Банка России в обеспечении информационной безопасности финансовой системы?

Критерии оценивания опроса:

Диапазон баллов	Описание критерия
85-100	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.
65-84	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
55-64	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
0-54	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

КТ – 3.

Тема 1.

Тестирование

Тест

1. Стратегия – это:

а) управление персоналом;

б) выбор уровней управления;

в) план деятельности по распределению ограниченных ресурсов во времени для достижения целей организации;

г) система последовательных решений задач, обеспечивающих перспективное движение к поставленной цели с учетом изменений внешней и внутренней среды.

1. Какова основная цель правового регулирования в сфере информационной безопасности на международном уровне?
а) Ограничение доступа к информации для граждан.
б) Обеспечение устойчивого развития информационного общества и защита национальных интересов.
в) Стандартизация программного обеспечения.
г) Увеличение прибыли IT-компаний.
2. Какие международные организации разрабатывают стандарты в области информационной безопасности? (Укажите не менее двух)
а) *ISO/IEC*.б) *UNESCO*.
в) *NIST*.
г) *ВОЗ*.
3. Какой международный стандарт определяет требования к системе управления информационной безопасностью (*СУИБ*)?
а) *ISO/IEC 27001*.
б) *ISO 9001*.
в) *PCI DSS*.
г) *GDPR*.
4. В чём заключается основное отличие национального правового регулирования ИБ от международного?
а) Национальное регулирование всегда строже.
б) Международные стандарты обязательны для всех стран.
в) Национальное законодательство учитывает специфику страны, а международные стандарты носят рекомендательный характер.
г) Международные стандарты касаются только государственных структур.
5. Какой нормативный акт регулирует вопросы защиты персональных данных в Европейском союзе?
а) *ФЗ-152 «О персональных данных»*.
б) *GDPR* (General Data Protection Regulation)
в) *ISO/IEC 27002*.
г) *Доктрина информационной безопасности РФ*.
6. Какие принципы закреплены в международных стандартах по информационной безопасности? (Укажите не менее двух)
а) Принцип открытости.
б) Принцип конфиденциальности.
в) Принцип доступности.
г) Принцип коммерческой выгоды.

Критерии оценивания тестовых заданий:

Диапазон баллов	Описание критерия	
85-100	Свыше 80% правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.
65-84	Свыше 70% правильных ответов.	Обучающимся материал освоен полностью, без существенных ошибок.
55-64	Свыше 50% правильных ответов.	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.
0-54	Менее 50% правильных ответов.	Обучающимся материал не освоен, знания обучающегося ниже базового уровня.

5.5. Описание дополнительных материалов и оборудования, необходимых для

выполнения проверочных заданий (*при необходимости*).

Для решения практических заданий обучающемуся разрешается использование Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.06 № 149-ФЗ, Федерального закона «О государственной тайне» от 21.09.93 № 182, Доктрины информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. N 646).

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1. Промежуточная аттестация (зачет) проводится в устной форме. Обучающийся получает экзаменационный билет и готовится к устному ответу.

6.2. Типовые оценочные материалы промежуточной аттестации

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

Тема 1 Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасности ИПК-12.2

1. Каковы основные цели и задачи правового регулирования в сфере информационной безопасности на международном и национальном уровнях?
2. Какие ключевые международные стандарты в области информационной безопасности вы знаете? Дайте краткую характеристику *ISO/IEC 27001* и *ISO/IEC 27002*.
3. Как международные стандарты влияют на формирование и развитие национального законодательства в области информационной безопасности (на примере РФ)?
4. Какие категории информации подлежат обязательной защите согласно российскому законодательству? Приведите примеры.

Тема 2. Основные понятия, виды и источники информации, подлежащей защите ИПК-12.2

1. Что такое информация, подлежащая защите? Каковы её основные признаки?
2. Какие виды информации выделяют в законодательстве РФ с точки зрения необходимости её защиты? Приведите примеры для каждого вида.
3. Дайте определение персональным данным. Какие категории персональных данных существуют и чем они отличаются?

Тема 3. Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности ИПК-12.2

1. Каковы основные цели и задачи государственной политики Российской Федерации в области информационной безопасности?
2. Какие нормативные правовые акты определяют основы государственной политики в сфере информационной безопасности в России?
3. Назовите ключевые принципы обеспечения информационной безопасности, закреплённые в Доктрине информационной безопасности РФ.

Тема 4. *Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ* ИПК-12.2

1. Что такое государственная тайна? Каковы её основные признаки и правовая основа?
2. Какие сведения могут быть отнесены к государственной тайне в Российской Федерации? Приведите примеры.
3. Назовите основные степени секретности сведений, составляющих государственную тайну, и их отличия.

Тема 5. Проблемы и угрозы информационной безопасности ИПК-12.2

1. Что такое угроза информационной безопасности? Чем она отличается от уязвимости?
2. Какие основные виды угроз информационной безопасности существуют? Приведите примеры для каждого вида.
3. В чём различие между умышленными и неумышленными угрозами? Почему важно их разделять?

Тема 6. Особенности работы с персоналом, владеющим конфиденциальной информацией ИПК-12.2

1. Какие меры ответственности предусмотрены для персонала за разглашение или неправомерное использование конфиденциальной информации?
2. Как организуется обучение и повышение осведомлённости сотрудников по вопросам информационной безопасности? Какова его периодичность?
3. В чём заключается роль системы мотивации и лояльности персонала в защите конфиденциальной информации?

Тема7. Защищенный документооборот ИПК-12.2

1. Что такое защищённый документооборот и каковы его основные цели в современной организации?
2. Какие виды документов подлежат обязательной защите при организации документооборота?
3. В чём заключаются основные отличия защищённого электронного документооборота от традиционного бумажного?

Практико-ориентированные (практические) задания к промежуточной аттестации:

ИПК-12.2

Способен проектировать информационные процессы и системы с использованием инновационных инструментальных средств, адаптировать современные ИКТ к задачам прикладных ИС.

Задание. Заполните таблицу, в которой укажите основные источники угроз информационной безопасности и их характеристики.

6.3. Критерии и шкала оценивания на основе БРС.

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал	40

знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок	
Дан развернутый ответ на поставленный вопрос, где обучающийся демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.	30-39
Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.	20-29
Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. обучающийся не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	0-19

6.4. Для решения практических заданий обучающемуся разрешается использование Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.06 № 149-ФЗ, Федерального закона «О государственной тайне» от 21.09.93 № 182, Доктрины информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. N 646).

7. Методические материалы по освоению дисциплины

Подготовка к лекциям.

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его

нужно положить рабочие программы изучаемых в семестре дисциплин. Каждому обучающемуся следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Самостоятельная работа на лекции.

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лекции лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места, определения, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек. Лучше если они будут собственными, чтобы не приходилось просить их у однокурсников и тем самым не отвлекать их во время лекции. Целесообразно разработать собственную «маркографию» (значки, символы), сокращения слов. Не лишним будет и изучение основ стенографии. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть знаниями.

Подготовка к практическим занятиям.

Подготовку к каждому практическому занятию каждый обучающийся должен начать с ознакомления с планом практического занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованную к данной теме. На основе индивидуальных предпочтений обучающемуся необходимо самостоятельно выбрать тему доклада по проблеме практического занятия и по возможности подготовить по нему презентацию. Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенной инструкции (устно или 10 письменно). Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы практического занятия, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Структура практического занятия:

В зависимости от содержания и количества отведенного времени на изучение каждой темы может практическое занятие состоять из четырех-пяти частей:

1. Обсуждение теоретических вопросов, определенных программой дисциплины.

2. Доклад и/ или выступление с презентациями по проблеме практического занятия.

3. Обсуждение выступлений по теме – дискуссия.

4. Выполнение практического задания с последующим разбором полученных результатов или обсуждение практического задания, выполненного дома, если это предусмотрено программой.

5. Подведение итогов занятия.

Первая часть – обсуждение теоретических вопросов - проводится в виде фронтальной беседы со всей группой и включает выборочную проверку преподавателем теоретических знаний обучающихся. Примерная продолжительность — до 15 минут. Вторая часть — выступление обучающихся с докладами, которые должны сопровождаться презентациями с целью усиления наглядности восприятия, по одному из вопросов практического занятия. Обязательный элемент доклада – представление и анализ статистических данных, обоснование социальных последствий любого экономического факта, явления или процесса. Примерная продолжительность — 20-25 минут. После докладов следует их обсуждение – дискуссия. В ходе этого этапа практического занятия могут быть заданы уточняющие вопросы к докладчикам. Примерная продолжительность – до 15-20 минут. Если программой предусмотрено выполнение практического задания в рамках конкретной темы, то преподавателями определяется его содержание и дается время на его выполнение, а затем идет обсуждение результатов. Если практическое задание должно было быть выполнено дома, то на практическом занятии преподаватель проверяет его выполнение (устно или письменно). Примерная продолжительность – 15-20 минут. Подведением итогов заканчивается практическое занятие. Обучающимся должны быть объявлены оценки за работу и даны их четкие обоснования. Примерная продолжительность — 5 минут.

Работа с литературными источниками.

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на занятиях, выявить широкий спектр мнений по изучаемой проблеме.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642 (дата обращения: 17.04.2024). – Режим доступа: по подписке.

2. Крылов, Г.О. Базовые понятия информационной безопасности : монография / Г.О. Крылов, С.Л. Ларионова, В.Л. Никитина. - Москва : Русайнс, 2020. - 257 с. - Internet access. - ISBN 978-5-4365-1557-1. - Текст : электронный // ЭБС "BOOK.RU" : [сайт]. -

URL: http://www.book.ru/book/932492 (дата обращения: 02.03.2024). - Режим доступа: по подписке.

3. Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации : учебник / сост. И. Г. Дровникова, А. В. Калач, И. И. Лившиц [и др]. - Воронеж : Научная книга, 2022. - 304 с. - ISBN 978-5-4446-1743-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1999941 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

8.2. Дополнительная литература

1. Даниленков, А. О. Интернет-право/ДаниленковА.О. - Москва : Юстицинформ, 2014. - 232 с. ISBN 978-5-7205-1225-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/542852 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

2. Рассолов, И. М. Право и Интернет. Теория кибернетического права : монография / И.М. Рассолов. — 3-е изд., доп. — Москва : Норма : ИНФРА-М, 2026. — 304 с. - ISBN 978-5-00156-142-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2244256 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

8.3. Нормативные правовые документы и иная правовая информация

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

2. 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»

3. Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.03 Прикладная информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 №916 (зарегистрировано в Министерстве юстиции Российской Федерации 10.10.2017, регистрационный номер № 48495).Всеобщая декларация прав человека (принята 10 декабря 1948 г. Генеральной Ассамблеей ООН) // Международное публичное право: Сборник документов. Т. 1. М.: БЕК, 1996.

4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.06 № 149-ФЗ;

5. Федерального закона «О государственной тайне» от 21.09.93 № 182;

6. Доктрины информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. N 646).

www.kremlin.ru Президент Российской Федерации
www.gov.ru Сервер органов государственной власти Российской Федерации
http://www.gov.ru/main/page7.html Федеральное собрание РФ
http://www.duma.gov.ru/ Государственная Дума ФС РФ
www.vsrf.ru Верховный Суд Российской Федерации
www.ksrf.ru Конституционный Суд Российской Федерации
http://www.cikrf.ru Центральная избирательная комиссия РФ

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

9.1. Материально-техническая база

Перечень материально-технического обеспечения:

1. Учебные аудитории, оборудованные для проведения учебных занятий лекционногоисеминарскоготипа,групповыхииндивидуальныхконсультаций,коллоквиумов,мероприятийтекущегоконтроляипромежуточнойаттестации,втомчислемультимедийным 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 и информационно-образовательную среду организации;
3. Специализированные аудитории и лаборатории;
4. Библиотека с обеспечением печатными изданиями или электронно-библиотечнаясистемаобеспечивающаядоступкэлектроннымизданиям (электронная библиотека);
5. Читальный зал;
6. Техническиесредстваобучения:персональныекомпьютеры;компьютерныепроекторы;звуковыединамики;программныесредства,обеспечивающиепросмотрвидеофайловвформатахAVI,MPEG-4, DivX, RMVB,WMVи др.

9.2. 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. Архиватор7-Zip.
6. Система дистанционного обучения.
7. Автоматизированная библиотечная система.

9.3. Информационные справочные системы:

1. https://www.iprbookshop.ru – Электронно-библиотечная система [ЭБС]«IPRSMART»(ранее–IPRBooks)
2. https://e.lanbook.com -Электронно-библиотечная система [ЭБС] «Лань».
3. https://znanium.ru - Электронно-библиотечная система [ЭБС] «Znanium.com».
4. https://www.book.ru - Электронно-библиотечная система[ЭБС]«Book.ru».
5. https://ibooks.ru-Электронно-библиотечная система [ЭБС]«ibooks.ru».
6. https://ranepalib.miflib.ru - Электронная библиотека издательства «МИФ».
7. https://eivis.ru–Ивис (EastView). Полные тексты российских научных и практических журналов, а также газет центральной прессы России. Доступ с ip-адресов локальной сети Института.
8. http://www.consultant.ru/-Справочно-правоваясистема «Консультант».
9. http://www.garant.ru/Справочно-правоваясистема «Гарант».