Лебедева Екатерина Александровна
Подписано цифровой подписью: Лебедева Екатерина Александровна
Дата: 2026.06.25 12:28:39 +03'00'

Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.07 Информационная безопасность
(индекс, наименование дисциплины в соответствии с учебным планом)

40.04.01 Юриспруденция
(код, наименование направления подготовки)

Юридическое обеспечение национальной безопасности
(наименование образовательной программы)

заочная форма обучения
(форма обучения)

Год набора – 2026
Нижний Новгород, 2026 г.

Автор(ы)-составитель(и) РПД:

Кочеткова Светлана Вячеславовна, старший преподаватель кафедры правового обеспечения национальной безопасности

Заведующий кафедрой:

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

Рабочая программа дисциплины Б1.В.07 Информационная безопасность 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 программы
2. Объем и место дисциплины в структуре образовательной программы
3. Содержание и структура дисциплины
4. Типы оценочных материалов, показатели, критерии, шкалы оценивания
5. Формы аттестации и типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам
6. Формы промежуточной аттестации по дисциплине, типы оценочных материалов, показатели, критерии, шкалы оценивания
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 образовательной программы

Дисциплина Б1.В.07 Информационная безопасность 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**
A/01.7. Криминалистическое сопровождение производства предварительного расследования (производство предварительного расследования) преступлений «Следователь-криминалист», утв. приказом Минтруда России от 23.05.2015 № 183н*	**ПКс-2.1**	Способен устранять признаки нарушения 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	ИПКсС-2.1.2. З-1. ***Знает*** способы выявления и методы оценки признаков правонарушения в области требований законодательства в сфере безопасности Российской Федерации ИПКс-2.1.2. У-1. ***Умеет*** выявлять и оценить признаки правонарушения в области требований законодательства в сфере безопасности Российской Федерации

2. Объем и место дисциплины (модуля) в структуре образовательной программы

Общий объем дисциплины:

4,00 з.е., 144 ак. часов

заочная форма обучения: 2 курс – лекции – 8 а.ч., практические занятия – 16 а.ч., самостоятельная работа – 111 а. ч., экзамен – 9 а.ч.

Б1.В.07 Информационная безопасность реализуется на заочной форме обучения в 3-м семестре на 2-м курсе перед изучением дисциплин:

Б1.В.04 Национальная оборона и военная безопасность

Б1.В.02(П) Экспертно-консультационная практика

Б2.В.03 (Пд) Преддипломная практика

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Заочная 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	Кат тэк	Контроль	СРкр	СРэк	СР
			Л	ВЛ	ЛР	ПЗ								
Зачная форма обучения														
Тема 1.	Информационная безопасность как составляющая национальной безопасности	18	1	0	0	2	0	0	0	0		0	0	15	Устный опрос
Тема 2.	Основы информационной безопасности и защиты информации	19	1	0	0	2	0	0	0	0		0	0	16	Устный опрос, тестирование
Тема 3.	Виды и особенности угроз информационным ресурсам	19	1	0	0	2	0	0	0	0		0	0	16	Устный опрос, ситуационные задачи

Тема 4.	Основные направления и этапы работ по созданию комплексной системы информационной безопасности организации	20	2	0	0	2	0	0	0	0	0	0	16	Устный опрос
Тема 5.	Особенности работы с персоналом, владеющим конфиденциальной информацией	19	1	0	0	2	0	0	0	0	0	0	16	Устный опрос ситуационные задачи
Тема 6.	Защищенный документооборот	19	1	0	0	2	0	0	0	0	0	0	16	Устный опрос ситуационные задачи
Тема 7.	Инженерно-технические и программные методы защиты информации	21	1	0	0	4	0	0	0	0	0	0	16	Устный опрос
Промежуточная аттестация		9	0	0	0	0	0	0	0	9	0	0	0	Экзамен
Итого		144	8	0	0	16	0	0	0	9	0	0	111	

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 занятиям.

3.2 Содержание дисциплины

Тема 1. Информационная безопасность как составляющая национальной безопасности. ИПКс-2.1.2

Информационная безопасность как элемент национальной безопасности. Международные договоры в области информационной безопасности. Законодательство о безопасности и защите информации, его структура и содержание.

Тема 2. Основы информационной безопасности и защиты информации. ИПКс-2.1.2

Цели, задачи, уровни обеспечения информационной безопасности. Основные угрозы жизненно важным интересам личности, общества, государства в информационной сфере. Формы и методы обеспечения информационной безопасности.

Тема 3. Виды и особенности угроз информационным ресурсам. ИПКс-2.1.2

Правовой режим информационных ресурсов. Институт тайн в законодательстве Российской Федерации. Виды угроз информационным ресурсам. Понятие и виды правонарушений в информационной сфере.

Тема 4. Основные направления и этапы работ по созданию комплексной системы информационной безопасности организации. ИПКс-2.1.2

Понятие, цели, задачи, принципы построения, элементы системы защиты конфиденциальной информации. Компьютерные технологии и формирование основ системы защиты информации. Сертификация средств защиты информации.

Тема 5. Особенности работы с персоналом, владеющим конфиденциальной информацией. ИПКс-2.1.2

Угрозы безопасности информации, исходящие от персонала и направления противодействия им. Задачи и стадии работы с персоналом, обладающим конфиденциальными сведениями. Организация доступа персонала к конфиденциальным сведениям, документам и базам данных. Правовая ответственность персонала за разглашение информации ограниченного доступа.

Тема 6. Защищенный документооборот. ИПКс-2.1.2

Понятие и задачи, основные требования к защищённому документообороту. Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков. Технологические системы защиты и обработки документов, содержащих сведения ограниченного доступа.

Тема 7. Инженерно-технические и программные методы защиты информации. ИПКс-2.1.2

Физические защиты информации. Технические, программно-технические и программные методы обеспечения информационной безопасности. Криптографические средства защиты информации.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.11 Ребенок в информационной среде 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.07 Информационная безопасность используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Устный опрос, ситуационная задача, тестирование, доклад.

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

Тема 1. Информационная безопасность как составляющая национальной безопасности. ИПКс-2.1.2

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся 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 для проведения опроса по теме практического занятия;

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

– готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

1. Информационная безопасность как элемент национальной безопасности.

2. Международные договоры в области информационной безопасности.

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

Тема 2. Основы информационной безопасности и защиты информации. ИПКс-2.1.2

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся 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 для проведения опроса по теме практического занятия;

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

– готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

1. Цели, задачи, уровни обеспечения информационной безопасности.

2. Основные угрозы жизненно важным интересам личности, общества, государства в информационной сфере.

3. Формы и методы обеспечения информационной безопасности.

Тестовые задания с инструкцией по выполнению:

Тест 1.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать один верный ответ.

4. Записать только букву выбранного варианта ответа (например, а).

1. Состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность:

а) информационная безопасность;

б) безопасность информации;

в) защита информации;

г) система защиты информации.

2. Правовое определение информационной безопасности дано в:

а) ФЗ «О безопасности»;

б) «Стратегии развития информационного общества в Российской Федерации»;

в) Концепции информационной безопасности;

г) Доктрине информационной безопасности.

3. Общая стратегия обеспечения информационной безопасности в Российской Федерации определяется на:

а) законодательном уровне;

б) административном уровне;

в) процедурном уровне;

г) программно-техническом уровне.

4. Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию:

а) информационная безопасность;

б) безопасность информации;

в) защита информации;

г) система защиты информации.

5. Шифрование данных относится к:

а) организационным методам защиты информации;

б) техническим методам защиты информации;

в) экономическим методам защиты информации;

г) правовым методам защиты информации.

Тест 2.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько правильных ответов.

4. Записать только буквы выбранного варианта ответа (например, а, в).

1. Вопросы обеспечения информационной безопасности Российской Федерации рассматриваются в:

а) Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы;

б) Доктрине информационной безопасности Российской Федерации;

в) Стратегии национальной безопасности Российской Федерации;

г) Концепции национальной безопасности Российской Федерации.

2. Информационные права личности …

а) …могут быть ограничены в целях защиты основ конституционного строя, обеспечения обороны и безопасности государства;

б) …могут быть ограничены в целях сохранения исторического и культурного наследия страны;

в) …могут быть ограничены в целях в целях защиты здоровья и нравственности;

г) …не могут быть ограничены.

3. Информационная безопасность включает:

а) безопасность информации и её защиту

б) состояние защищённости информационной среды общества;

в) способность противостоять информационным воздействиям, которые могут привести к нежелательным последствиям;

г) проведение правовых, организационных и инженерно-технических мероприятий при формировании и использовании информационных технологий, инфраструктуры и информационных ресурсов.

4. К организационным методам защиты информации в организации относятся:

а) разработка внутренних документов (политика информационной безопасности, приказы, инструкции, планы реагирования на инциденты);

б) инструктаж и периодические проверки персонала, обучение сотрудников правилам работы с информацией;

в) создание системы страхования информационных рисков для физических и юридических лиц;

г) формирование в рабочем коллективе моральных и этических норм и правил, соблюдение которых гарантирует сохранность информационных данных.

5. Функции Совета Безопасности России в информационной сфере:

а) разрабатывает стратегии в области внешней и внутренней политики по информационной безопасности;

б) занимается подготовкой проектов указов Президента РФ по вопросам обеспечения информационной безопасности;

в) координирует деятельность федеральных и региональных органов исполнительной власти в информационной сфере;

г) разрабатывает рекомендации по совершенствованию системы обеспечения информационной безопасности.

Тема 3. Виды и особенности угроз информационным ресурсам. ИПКс-2.1.2

Подготовка к практическому занятию:

- внимательно прочитать материал лекций, относящихся 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 для проведения опроса по теме практического занятия;
- понять, что осталось неясными и постараться получить на них ответ заранее;
- готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

1. Правовой режим информационных ресурсов.
2. Институт тайн в законодательстве Российской Федерации.
3. Виды угроз информационным ресурсам.
4. Понятие и виды правонарушений в информационной сфере.

Ситуационные задачи:

Задача 1.

На детской книге, изданной ООО «Магирус» и содержащей описания антиобщественных действий отсутствовала наклейка с информацией о возрастной группе, для которой адресовано данное издание.

Нарушило ли ООО «Магирус» нормы информационного законодательства? Ответ аргументируйте.

Задача 2.

На одном из форумов в интернете Сидоров после ссоры с Петровым начал размещать сведения, отрицательно характеризующие Петрова в данном сообществе, не соответствующие действительности, настраивать против него других участников форума.

К какой категории информации можно отнести сведения, размещаемые Сидоровым? Есть ли в его действиях состав информационного правонарушения?

Тема 4. Основные направления и этапы работ по созданию комплексной системы информационной безопасности организации. ИПКс-2.1.2

Подготовка к практическому занятию:

- внимательно прочитать материал лекций, относящихся 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 для проведения опроса по теме практического занятия;
- понять, что осталось неясными и постараться получить на них ответ заранее;
- готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

1. Понятие, цели, задачи, принципы построения, элементы системы защиты конфиденциальной информации.
2. Компьютерные технологии и формирование основ системы защиты информации.
3. Сертификация средств защиты информации.

Тема 5. Особенности работы с персоналом, владеющим конфиденциальной информацией. ИПКс-2.1.2

Подготовка к практическому занятию:

- внимательно прочитать материал лекций, относящихся 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 для проведения опроса по теме практического занятия;
- понять, что осталось неясными и постараться получить на них ответ заранее;
- готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

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. Правовая ответственность персонала за разглашение информации ограниченного доступа.

Ситуационные задачи:

Ситуация 1.

Выпускник ВУЗа, обучавшийся по направлению от органа исполнительной власти, при заключении служебного контракта узнал, что будет замещать должность, для выполнения должностных обязанностей по которой ему необходимо будет работать с документами под грифом «секретно».

Назовите порядок допуска государственных служащих к сведениям, составляющим государственную тайну.

Ситуация 2.

В коммерческой организации вводится режим коммерческой тайны в отношении сведений, отражаемых во внутренних документах.

Какие разделы необходимо включить в Положение о режиме коммерческой тайны в организации?

Тема 6. Защищенный документооборот. ИПКс-2.1.2

Подготовка к практическому занятию:

- внимательно прочитать материал лекций, относящихся 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 для проведения опроса по теме практического занятия;
- понять, что осталось неясными и постараться получить на них ответ заранее;
- готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

1. Понятие и задачи, основные требования к защищённому документообороту.
2. Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков.
3. Технологические системы защиты и обработки документов, содержащих сведения ограниченного доступа.

Ситуационные задачи:

Ситуация 1.

Вам поручили создать в организации отдел конфиденциального делопроизводства для внешнего и внутреннего документооборота бумажных документов.

Опишите алгоритм действий по этапам.

Ситуация 2.

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

С какой категорией документов ограниченного доступа работал Соколов? Укажите, в каком нормативном акте приведён их перечень.

Тема 7. Инженерно-технические и программные методы защиты информации. ИПКс-2.1.2

Подготовка к практическому занятию:

- внимательно прочитать материал лекций, относящихся 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 для проведения опроса по теме практического занятия;

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

– готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

1. Физические методы защиты информации.

2. Технические, программно-технические и программные методы обеспечения информационной безопасности.

3. Криптографические средства защиты информации.

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	0,2	20
КТ 2	100	0,4	40
Итого:	х	0,6	60

Формула расчета результата контрольной точки:

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

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

КТ – 1.

Тема 1 - 4.

Доклад.

Тематика докладов:

1. Система национальной безопасности Российской Федерации.

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

3. Понятие, цели, задачи защиты информации.

4. Соотношение понятий «информационная безопасность», «безопасность информации», «защита информации».

5. Информационная безопасность и компьютеризация информационной среды.

6. Документирование информации как способ ее защиты.

7. Аналитическая работа по выявлению угроз информационной безопасности.

8. Структура комплексной системы защиты информации.

9. Формирование и актуализация системы защиты информации в реальных обстоятельствах существующих угроз информации.

10. Определение соотношения элементов системы защиты информации в соответствии с типом организации и видами угроз.

11. Задачи и функции подразделений служб безопасности по защите информации.

12. Формы и методы деятельности службы безопасности организации по защите информации.

13. Взаимодействие службы безопасности и службы персонала по защите информации.

14. Назначение и взаимосвязь плановой и контрольной работы службы безопасности, их место в построении и функционировании комплексной системы защиты информации организации.

15. Уголовная ответственность за совершение информационных преступлений.

16. Административная ответственность за совершение правонарушений в информационной сфере.

17. Гражданско-правовая ответственность за информационные правонарушения.

18. Дисциплинарная ответственность за информационные правонарушения.

19. Юридическая ответственность за нарушение правовых норм по вопросам защиты информации.

20. Информационные правонарушения в Интернете.

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 аспектов 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 5 - 7.
Тестирование
Тестовые задания с инструкцией по выполнению:

Тест 1.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.
2. Внимательно прочитать предложенные варианты ответа.
3. Выбрать один верный ответ.
4. Записать только букву выбранного варианта ответа (например, а).

1. Охраняемая законом конфиденциальная информация, полученная специалистом в ходе выполнения своих профессиональных обязанностей:
а) государственная тайна;
б) служебная тайна;
в) профессиональная тайна;
г) коммерческая тайна.

2. Принципы использования электронной подписи закреплены в:
а) ФЗ «Об электронной подписи»;
б) ФЗ «О государственной тайне»;
в) ФЗ «Об архивном деле»;
г) ФЗ «Об информации, информационных технологиях и защите информации».

3. Действие «Правил делопроизводства в государственных органах, органах местного самоуправления», утвержденных Приказом Росархива от 22.05.2019 N 71 не распространяется на:
а) федеральные органы государственной власти;
б) организационно-распорядительную документацию;
в) органы местного самоуправления;
г) организацию работы с документами, содержащими сведения, составляющие государственную тайну.

4. Специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования называются:
а) фишинговые методы защиты информации;
б) криптографические методы защиты информации;
в) инженерно-технические методы защиты информации;
г) организационно-правовые методы защиты информации.

5. Незаконное использование, передача, сбор и хранение компьютерной информации, содержащей персональные данные граждан, влечет за собой уголовную ответственность:

а) по ст. 272 УК РФ;

б) по ст. 272.1 УК РФ;

в) по ст. 137 УК РФ;

г) по ст. 138 УК РФ.

Тест 2.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько правильных ответов.

4. Записать только буквы выбранного варианта ответа (например, а, в).

1. В документообороте выделяются документопотоки:

а) входящие (поступающие) документы;

б) исходящие (отправляемые) документы;

в) конфиденциальные документы;

г) внутренние документы.

2. К организационным мерам обеспечения информационной безопасности относятся:

а) разработка положений, регламентов обеспечения информационной безопасности;

б) создание подразделений или назначение лиц, ответственных за обеспечение информационной безопасности;

в) построение информационной системы предприятия, позволяющей выстроить оборону против посягательств на конфиденциальные сведения;

г) разработка системы взаимодействия с государственными органами в случае запроса ими у организации информации, которая может быть отнесена к конфиденциальной.

3. Виды электронной подписи:

а) простая электронная подпись;

б) сложная электронная подпись;

в) усиленная квалифицированная электронная подпись;

г) усиленная неквалифицированная электронная подпись.

4. Федеральный орган по сертификации и органы по сертификации средств защиты информации имеют право приостанавливать или аннулировать действие сертификата в следующих случаях:

а) изменение нормативных и методических документов по защите информации в части требований к средствам защиты информации, методам испытаний и контроля;

б) изменение технологии изготовления, конструкции (состава), комплектности средств защиты информации и системы контроля их качества;

в) смены собственника организации;

г) отказ изготовителя обеспечить беспрепятственное выполнение своих полномочий лицами, осуществляющими государственные контроль и надзор, инспекционный контроль за сертификацией и сертифицированными средствами защиты информации.

5. За нарушение режима конфиденциальности информации возможно наступление:
а) уголовной ответственности;
б) административной ответственности;
в) гражданско-правовой ответственности;
г) дисциплинарной ответственности.

Правильный ответ: а, б, в, г.

Критерии оценивания тестовых заданий:

Диапазон баллов	Описание критерия	
85-100	85% и выше правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.
65-84	65% и выше правильных ответов.	Обучающимся материал освоен полностью, без существенных ошибок.
55-64	55% и выше правильных ответов.	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.
0-54	Менее 55% 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 ответа на вопросы студенту разрешается использование Конституции Российской Федерации.

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

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

6.2. Типовые оценочные материалы промежуточной аттестации

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

Тема 1. Информационная безопасность как составляющая национальной безопасности. ИПКс-2.1.2

Задания открытого типа.

Внимательно прочитать вопрос и дать развернутый ответ.

№ п.п.	Вопрос
1.	Юридически закрепленное понятие информационной безопасности
2.	Источники правовых норм, регулирующих международно-правовой режим информационной безопасности
3.	Нормы Закона О безопасности, регламентирующие обеспечение информационной безопасности

4.	Корпоративные правовые нормы в области информационной безопасности

Задания комбинированного типа.

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Существуют ли российские стандарты в области защиты информации? Варианты ответов: а) да б) нет.		
2.	Есть ли нормы, касающиеся обеспечения информационной безопасности в федеральных конституционных законах? Варианты ответов: а) да; б) нет.		

Задания закрытого типа.

Тестовые задания 1.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать один верный ответ.

4. Записать только букву выбранного варианта ответа (например, а).

1. Какое из понятий шире и включает в себя остальные: «информационная безопасность», «безопасность информации» или «защита информации»?

а) информационная безопасность;

б) безопасность информации;

в) защита информации;

г) это независимые равнозначные понятия.

2. Нормы общего характера об ограничении доступа к информации, обеспечении информационной безопасности, содержатся в:

а) Федеральном законе «О безопасности»;

б) Федеральном законе «Об информации, информационных технологиях и о защите информации»;

в) Законе РФ «О государственной тайне»;

г) Федеральном законе «О связи».

Тестовые задания 2.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько правильных ответов.

4. Записать только буквы выбранного варианта ответа (например, а, в).

1. В систему источников права, регламентирующих вопросы информационной безопасности, входят:

а) федеральные законы;

б) указы Президента Российской Федерации;

в) законы субъектов Российской Федерации;

г) локальные нормативные правовые акты.

2. Федеральные законы, регламентирующие оборот информации ограниченного доступа:

а) «О техническом регулировании»;

б) «О государственной тайне»;

в) «О безопасности критической информационной инфраструктуры»;

г) «О персональных данных».

Тема 2. Основы информационной безопасности и защиты информации. ИПКс-2.1.2

Задания открытого типа.

Внимательно прочитать вопрос и дать развернутый ответ.

№ п.п.	Вопрос
1.	Уровни обеспечения информационной безопасности
2.	Стратегические цели и основные направления обеспечения информационной безопасности: источник и классификация
3.	Задачи государственных органов в рамках деятельности по обеспечению информационной безопасности
4.	Цели обеспечения информационной безопасности на уровне организаций

Задания комбинированного типа.

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Относится ли защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации к стратегическим целям обеспечения информационной безопасности в стране? Варианты ответов:		

	а) да; в) нет.		
2.	Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации, это: Варианты ответов: а) информационная угроза; б) угроза информационной безопасности организации; в) угроза безопасности информации.		

Задания закрытого типа.

Тестовые задания 1.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать один верный ответ.

4. Записать только букву выбранного варианта ответа (например, а).

1. Обучение персонала, разработка инструкций по работе с информацией, контролем соблюдения правил безопасности, относятся:

а) к законодательному уровню защиты информации;

б) к организационному уровню защиты информации;

в) к процедурному уровню защиты информации;

г) к программно-техническому уровню защиты информации

2. Формирование в обществе или рабочем коллективе моральных и этических норм и правил, соблюдение которых гарантирует сохранность информационных данных, относится:

а) к правовым методам защиты информации;

б) к организационным методам защиты информации;

в) к экономическим методам защиты информации;

г) к морально-этическим методам защиты информации.

Тестовые задания 2.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько правильных ответов.

4. Записать только буквы выбранного варианта ответа (например, а, в).

1. В число технических методов защиты информации входит:

а) создание специальных подразделений, отвечающих за защиту информации;

б) охрана помещений, установка сигнализаций, камер видеонаблюдения;

в) разработка политики информационной безопасности организации;

г) шифрование данных, использование электронной подписи, хеширование.

2. К угрозам жизненно важным интересам общества в информационной сфере относятся:

а) массовое распространение ложной информации с целью манипулирования общественным мнением, создания социального напряжения или паники;

б) риск несанкционированного доступа к личным данным, которые человек оставляет в сети интернет;

в) неравный доступ к современным технологиям и информационным ресурсам из-за экономических, образовательных или технологических барьеров;

г) недостаток доступа к необходимым данным либо перегрузка информацией, которая вызывает стресс, когнитивные перегрузки и снижение продуктивности.

Тема 3. Обеспечение и защита прав личности в информационной сфере. ИПКо ОС-2.1

Задания открытого типа.

Внимательно прочитать вопрос и дать развернутый ответ.

№ п.п.	Вопрос
1.	Правовой режим информационных ресурсов
2.	Категории сведений, относящихся к информации ограниченного доступа. Виды тайн
3.	Угрозы информационным ресурсам
4.	Виды юридической ответственности за правонарушения в информационной сфере

Задания комбинированного типа.

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Иванову поступил звонок с сообщением, что он выиграл приз в лотерее, разыгрываемой случайным образом между абонентами сотовой связи. Для получения приза он назвал код из СМС. В результате этих действий злоумышленники получили доступ к банковскому счету Иванова и вывели оттуда денежные средства в сумме 500 000 рублей, которые он откладывал на покупку		

	нового автомобиля. Какое правонарушение совершено в отношении Иванова? Варианты ответов: а) административное правонарушение; б) гражданско-правовой деликт; в) уголовное преступление		
.	Информация в зависимости от категории доступа к ней делится на: Варианты ответов: а) закрытую; б) открытую; в) общедоступную; г) ограниченного доступа.		

Задания закрытого типа.

Тестовые задания 1.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать один верный ответ.

4. Записать только букву выбранного варианта ответа (например, а).

1. Информация, охраняемая в ходе правовой защиты права на неприкосновенность частной жизни:

а) семейная тайна;

б) государственная тайна;

в) коммерческая тайна;

г) служебная тайна.

2. Гражданско-правовая ответственность за нарушение правил информационной безопасности:

а) наступает всегда;

б) наступает, если потерпевший обратился в суд;

в) наступает, если потерпевший обратился с заявлением о совершении в отношении его преступления;

г) наступает, если потерпевшему нанесен какой-либо ущерб.

Тестовые задания 2.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько правильных ответов.

4. Записать только буквы выбранного варианта ответа (например, а, в).

1. Собственником информационных ресурсов может быть:
а) государство в лице органов государственной власти;
б) органы местного самоуправления;
в) организации;
г) физические лица.

2. По целям угрозы информационным ресурсам делятся на:
а) угрозы данным;
б) социальные;
в) технические;
г) угрозы аппаратному обеспечению.

Тема 4. Основные направления и этапы работ по созданию комплексной системы информационной безопасности организации. ИПКс-2.1.2

Задания открытого типа.

Внимательно прочитать вопрос и дать развернутый ответ.

№ п.п.	Вопрос
1.	Определение системы защиты конфиденциальной информации
2.	Принципы построения системы защиты конфиденциальной информации
3.	Организационные меры при использовании компьютерных технологий в системе защиты информации
4.	Сертификация средств защиты информации: определение, цель, виды.

Задания комбинированного типа.

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Перечень разновидностей конфиденциальной информации закреплён: Варианты ответов: а) в Доктрине информационной безопасности; б) в Законе об информации в) в указе Президента России; г) в постановлении Правительства России.		
2.	Полномочия федерального органа по сертификации средств защиты информации закреплены: Варианты ответов:		

	а) в Доктрине информационной безопасности; б) в Законе об информации в) в указе Президента России; г) в постановлении Правительства России.		

Задания закрытого типа.

Тестовые задания 1.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать один верный ответ.

4. Записать только букву выбранного варианта ответа (например, а).

1. Меры по поддержанию бесперебойной работы систем, резервирование и мониторинг используются для решения задач обеспечения:

а) конфиденциальности информации;

б) целостности информации;

в) доступности информации;

г) оригинальности информации.

2. Координация работ по организации сертификации средств защиты информации возлагается на:

а) Межведомственную комиссию по защите государственной тайны;

б) ФСТЭК России;

в) ФСБ России;

г) Министерство обороны Российской Федерации.

Тестовые задания 2.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько правильных ответов.

4. Записать только буквы выбранного варианта ответа (например, а, в).

1. Вопросы сертификации средств защиты информации регулируются нормами:

а) Федерального закона от 27.12.2002 N 184-ФЗ «О техническом регулировании»;

б) Указа Президента РФ № 188 от 06.03.1997 «Об утверждении перечня сведений конфиденциального характера»;

в) Постановления Правительства РФ от 26.06.1995 N 608 «О сертификации средств защиты информации»;

г) Закона РФ от 21.07.1993 N 5485-1 «О государственной тайне».

2. В полномочия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России входит:

а) лицензирование деятельности по разработке, производству, распространению шифровальных (криптографических) средств;

б) сертификация средств защиты информации;

в) регулирование ввоза на территорию Российской Федерации и вывоза за ее пределы шифровальных средств;

г) изготовление шифровальных средств.

Тема 5. Особенности работы с персоналом, владеющим конфиденциальной информацией. ИПКс-2.1.2

Задания открытого типа.

Внимательно прочитать вопрос и дать развернутый ответ.

№ п.п.	Вопрос
1.	Основные угрозы информационной безопасности, исходящие от персонала
2.	Задачи работы с персоналом, имеющим доступ к конфиденциальной информации
3.	Обязательные процедуры при оформлении допуска сотрудников к работе со сведениями конфиденциального характера
4.	Виды юридической ответственности персонала за разглашение информации ограниченного доступа

Задания комбинированного типа.

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Может ли быть работник уволен за разглашение сведений конфиденциального характера? Варианты ответов: а) нет; б) да		
2.	Имеет ли право работодатель требовать возмещения убытков, причиненных ему разглашением информации, составляющей коммерческую тайну, от уволившегося работника? Варианты ответов: а) нет; б) да; в) да, если у него во время работы был оформлен допуск к сведениям, составляющим коммерческую тайну организации.		

Задания закрытого типа.

Тестовые задания 1.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать один верный ответ.

4. Записать только букву выбранного варианта ответа (например, а).

1. Информация, охраняемая в ходе правовой защиты права на неприкосновенность частной жизни:

а) персональные данные;

б) государственная тайна;

в) коммерческая тайна;

г) служебная тайна.

2. Фиксация нарушений сотрудниками правил информационной безопасности относится к:

а) организационным мерам работы с персоналом;

б) юридическим мерам работы с персоналом;

в) техническим мерам работы с персоналом;

г) обучению и повышению осведомлённости персонала.

Тестовые задания 2.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько правильных ответов.

4. Записать только буквы выбранного варианта ответа (например, а, в).

1. Обязательные процедуры при увольнении сотрудников, имеющих официальный доступ к конфиденциальной информации:

а) обязательный отзыв доступов (аккаунты, пароли);

б) возврат корпоративных устройств;

в) контроль передачи дел и информации;

г) подтверждение удаления копий данных с личных устройств.

2. Осуществлять проверки соблюдения сотрудниками организации правил информационной безопасности имеют право:

а) руководитель организации;

б) непосредственный руководитель сотрудника;

в) уполномоченный сотрудник службы безопасности;

г) коллеги.

Тема 6. Защищенный документооборот. ИПКс-2.1.2

Задания открытого типа.

Внимательно прочитать вопрос и дать развернутый ответ.

№ п.п.	Вопрос
1.	Понятие и задачи защищенного документооборота

2.	Определение угроз документопотокам, задачи защиты традиционных и электронных документопотоков
3.	Принципы организации защиты документооборота
4.	Технологические системы защиты и обработки документов, содержащих сведения ограниченного доступа

Задания комбинированного типа.

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Политика информационной безопасности организации должна быть: Варианты ответов: а) доступна в виде документированной информации; б) доведена до сведения работников организации; в) доступна заинтересованным сторонам.		
2.	Будет ли иметь юридическую силу документ, заверенный квалифицированной электронной подписью? Варианты ответов: а) да; б) нет.		

Задания закрытого типа.

Тестовые задания 1.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать один верный ответ.

4. Записать только букву выбранного варианта ответа (например, а).

1. Манипулирование людьми с целью получения доступа к конфиденциальной информации, например, через фишинговые письма или обман сотрудников, это:

а) хакерские атаки;

б) социальная инженерия;

в) инсайдерские угрозы;

г) недостаточная аутентификация и авторизация.

2. Организационные меры, направленные на обеспечение конфиденциальности, целостности и доступности документов в процессе их создания, обработки, передачи и хранения:

а) использование защищенных протоколов связи и шифрования;

б) регулярное резервное копирование информации на защищённые носители;

в) разработка и внедрение политики информационной безопасности;

г) Внедрение систем мониторинга активности пользователей.

Тестовые задания 2.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько правильных ответов.

4. Записать только буквы выбранного варианта ответа (например, а, в).

1. Угрозы традиционным (бумажным) документопотокам:

а) Перехват данных, несанкционированное копирование, утечка информации через уязвимости системы или действия сотрудников;

б) Подделка подписей, печатей, штампов или содержания документов;

в) Посторонние лица могут получить доступ к документам, их копиям, черновикам или другим составным частям;

г) Слабые системы управления доступом, позволяющие посторонним получить доступ к данным или действовать от имени других пользователей.

2. Технические средства защиты документов, содержащих информацию ограниченного доступа:

а) средства доверенной загрузки;

б) межсетевые экраны;

в) системы видеонаблюдения;

г) электронные подписи.

Тема 7. Инженерно-технические и программные методы защиты информации. ИПКс-2.1.2

Задания открытого типа.

Внимательно прочитать вопрос и дать развернутый ответ.

№ п.п.	Вопрос
1.	Цели применения физических методов защиты информации
2.	Технические средства защиты информации: определение, решаемые задачи
3.	Определение и основные направления применения программной защиты информации
4.	Криптографические средства защиты информации: определение и функции

Задания комбинированного типа.

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Обеспечение защиты		

	информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации осуществляется с помощью: Варианты ответов: а) правовых мер; б) организационных мер; в) технических мер.		
2.	Можно ли для обеспечения защиты информации, содержащейся в государственных информационных системах использовать не сертифицированные СКЗИ? Варианты ответов: а) да б) нет.		

Задания закрытого типа.

Тестовые задания 1.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать один верный ответ.

4. Записать только букву выбранного варианта ответа (например, а).

1. Защита от пожаров и иных угроз, способствующих уничтожению информации, относится к:

а) физическим методам защиты информации;
б) техническим методам защиты информации;
в) организационным методам защиты информации;
г) программно-техническим методам защиты информации.

2. Экранирование относится к:

а) физическим методам защиты информации;
б) техническим методам защиты информации;
в) организационным методам защиты информации;
г) программно-техническим методам защиты информации.

Тестовые задания 2.

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько правильных ответов.

4. Записать только буквы выбранного варианта ответа (например, а, в).

1. Программные средства защиты информации:

а) обеспечивают мониторинг, обнаружение угроз;

б) создают физический барьер и предотвращают несанкционированный доступ к оборудованию;

в) контролируют сетевые потоки и защищают инфраструктуру;

г) обеспечивают защиту данных на уровне приложений и операционных систем.

2. Основные направления применения программных средств защиты информации:

а) создание электромагнитного зашумления для предотвращения утечки информации через электромагнитное излучение;

б) защита информации от несанкционированного доступа;

в) защита информации и программ от разрушения и модификации;

г) маскировка используемых в системе каналов связи.

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 обучающийся продемонстрировал 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	40
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,	0-19

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.	

6.4. Для решения практических заданий обучающемуся разрешается использование Уголовного кодекса Российской Федерации.

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 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. Бондаренко, И. С. Информационная безопасность: учебник / И. С. Бондаренко. — Москва: Издательский Дом МИСиС, 2023. — 254 с. — ISBN 978-5-907560-71-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/137525.html

2. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва: ЮНИТИ-ДАНА, 2023. — 287 с. — ISBN 978-5-238-02857-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/141624.html

8.2. Дополнительная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542340. - Режим доступа: по подписке.

2. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567915. - Режим доступа: по подписке. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2024. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543351 (дата обращения: 13.09.2025). - Режим доступа: по подписке.

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2024. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543351. - Режим доступа: по подписке.

8.3. Нормативные правовые документы и иная правовая информация

1. Всеобщая декларация прав человека (принята 10 декабря 1948 г. Генеральной Ассамблеей ООН) – Текст : электронный // СПС «КонсультантПлюс» : [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_120805 (дата обращения: 14.04.2025). – Режим доступа: свободный.

2. Международный пакт о гражданских и политических правах (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-ом пленарном заседании Генеральной Ассамблеи ООН)) – Текст : электронный // СПС «КонсультантПлюс» : [сайт]. –

URL: https://www.consultant.ru/document/cons_doc_LAW_5531 (дата обращения: 14.04.2025). – Режим доступа: свободный.

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) – Текст : электронный // ООН : [сайт]. – URL: https://www.un.org/ru/documents/decl_conv/declarations/st_hr1_141.shtml (дата обращения: 14.04.2025). – Режим доступа: свободный.

4. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) – Текст : электронный // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_121499 (дата обращения: 14.04.2025). – Режим доступа: свободный.

5. Директива Европейского Парламента и Совета Европейского Союза 2009/24/ЕС от 23 апреля 2009 г. о правовой охране компьютерных программ (кодифицированная версия) – Текст : электронный // СПС «ГАРАНТ» : [сайт]. – URL: https://base.garant.ru/71657620 (дата обращения: 14.04.2025). – Режим доступа: свободный.

6. Всеобщая декларация о геноме человека и правах человека (принята 11 ноября 1997 г. на 29-й сессии Генеральной конференции ЮНЕСКО)) – Текст : электронный // ООН : [сайт]. – URL: https://www.un.org/ru/documents/decl_conv/declarations/human_genome.shtml (дата обращения: 14.04.2025). – Режим доступа: свободный.

7. Окинавская хартия глобального информационного общества от 22 июля 2000 – Текст : электронный // Президент России : [сайт]. – URL: http://www.kremlin.ru/supplement/3170 (дата обращения: 14.04.2025). – Режим доступа: свободный.

8. Типовой закон ЮНСИТРАЛ об электронных подписях (принят ЮНСИТРАЛ 5 июля 2001 г.) – Текст : электронный // СПС «ГАРАНТ» : [сайт]. – URL: https://base.garant.ru/2567278 (дата обращения: 14.04.2025). – Режим доступа: свободный.

9. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) .) – Текст : электронный // СПС «ГАРАНТ» : [сайт]. – URL: https://base.garant.ru/4089723 (дата обращения: 14.04.2025). – Режим доступа: свободный.

10. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с послед. изм. и доп.) – Текст : электронный // Официальный интернет-портал правовой информации (www.pravo.gov.ru) от 6.10.2022 г. , ст. 0001202210060013. – Режим доступа: свободный.

11. Федеральный конституционный закон от 30 мая 2001 г. № 3-ФКЗ «О чрезвычайном положении» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. – 2001. – № 23. – Ст. 2277.

12. Федеральный конституционный закон от 30 января 2002 года № 1-ФКЗ «О военном положении» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. – 2002. – № 5. – Ст. 375.

13. О Правительстве Российской Федерации : федеральный конституционный закон от 17.12.1997 N 2-ФКЗ // Российская газета. – 1997. – N 245.

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

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

16. Уголовный кодекс Российской Федерации (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.

17. Кодекс Российской Федерации об административных правонарушениях (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. – 2002. – № 1 (ч. 1). – Ст. 1.

18. О полиции: федеральный закон от 07 февраля 2011 г. № 3-ФЗ (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. – 2011. – № 7. – Ст. 900.

19. О прокуратуре Российской Федерации: федеральный закон от 17 ноября 1995 г. № 168-ФЗ (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. – 1995. – № 47. – Ст. 4472.

20. О федеральной службе безопасности: федеральный закон от 3 апреля 1995 г. № 40-ФЗ (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. – 1995. – № 15. – Ст. 1269.

21. Федеральный закон от 24 июня 1999 г. № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации – 1999. – № 26. – Ст. 3177.

22. Федеральный закон от 08 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации – 2001 – № 33 (ч. 1). – Ст. 3430.

23. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации – 2002. – № 30. – Ст. 3031.

24. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации – 2006. – № 11. – ст. 1146.

25. Федеральный закон от 28 февраля 2010 г. № 390-ФЗ «О безопасности» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. – 2011. – № 1. – Ст. 2.

26. Федеральный закон от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с послед. изм. и доп.) //Собрание законодательства Российской Федерации. – 2011. – № 1. – Ст. 48.

27. Федеральный закон от 29 декабря 1994 г. № 77-ФЗ «Об обязательном экземпляре документов» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. 1995. № 1. Ст. 1.

28. Федеральный закон от 29 декабря 1994 г. № 78-ФЗ «О библиотечном деле» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. 1995. № 1. Ст. 2.

29. Федеральный закон от 18 июля 1995 г. № 108-ФЗ «О рекламе» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. 1995. № 30. Ст. 2864.

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

31. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. 2004, № 32, ст. 3283

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

33. Федеральный закон от 13 марта 2006 г. № 38-ФЗ; «О рекламе» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. 2006. № 12. ст. 1232.

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

35. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. 2006. № 31. ст. 3451.

36. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. 2017. № 31. Ст. 4736. (часть I)

37. Закон РФ от 21 июля 1993 № 5485-I «О государственной тайне» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. 1997. N 41.

38. 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.

39. 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.

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

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

42. Указ Президента РФ от 06 марта1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. – 1997. – N 10. – Ст. 1127.

43. Указ Президента РФ от 05 декабря 2016 г. N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

44. Указ Президента РФ от 09 мая 2017 г. N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

45. Указ Президента РФ от 02 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. 2021. № 27. Ст. 5351. (Часть II).

46. "Концепция общественной безопасности в Российской Федерации" утв. Президентом РФ 14.11.2013 N Пр-2685 – Текст : электронный // Официальный сайт Президента РФ [Электронный ресурс]. - URL: http://kremlin.ru/acts/news/19653 (дата обращения: 19.09.2025). - Режим доступа: свободный.

47. Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [Электронный ресурс]. Режим доступа: https://base.garant.ru/70727118/ свободный. - Загл. с экрана.

48. Приказ ФСБ России от 24.10.2022 N 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» [Электронный ресурс]. Режим доступа: https://www.garant.ru/products/ipo/prime/doc/405670815/ свободный. - Загл. с экрана.

49. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» – Текст : электронный // электронный фонд правовых и нормативно-технических документов «КОДЕКС» : [сайт]. – URL: https://docs.cntd.ru/document/1200057516 (дата обращения: 14.04.2025). – Режим доступа: свободный.

50. ГОСТ 6.10.4-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения. – Текст : электронный // электронный фонд правовых и нормативно-технических документов «КОДЕКС» : [сайт]. – URL: https://docs.cntd.ru/document/9010879 (дата обращения: 14.04.2025). – Режим доступа: свободный.

51. ГОСТ Р 50922-2006. Защита информации: Основные термины и определения. – Текст : электронный // электронный фонд правовых и нормативно-технических документов «КОДЕКС» : [сайт]. – URL: https://docs.cntd.ru/document/1200058320 (дата обращения: 14.04.2025). – Режим доступа: свободный.

52. ГОСТ Р 7.0.97-2025. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов (утв. Приказом Росстандарта от 26.06.2025 N 622-ст). Режим доступа: [Электронный ресурс]. https://www.consultant.ru/document/cons_doc_LAW_510883 свободный. - Загл. с экрана.

53. ГОСТ Р 7.0.8-2025. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения (утв. Приказом Росстандарта от 17.10.2013 N 1185-ст) [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_500321 свободный. - Загл. с экрана.

54. ГОСТ Р 71207-2024 «Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования». Описывает порядок выполнения статического анализа, классификацию ошибок, обнаруженных при его проведении, требования к инструментам статического анализа. (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 января 2024 г. N 25-ст). [Электронный ресурс]. Режим доступа: https://base.garant.ru/408571109 свободный. - Загл. с экрана.

55. ГОСТ Р 71206-2024 «Защита информации. Разработка безопасного программного обеспечения. Безопасный компилятор языков С/С++. Общие требования». Задаёт требования к динамической компоновке и загрузке программ, выполнение которых необходимо для поддержки работы безопасного компилятора. (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 января 2024 г. N 24-ст). [Электронный ресурс]. Режим доступа: https://fstec.ru/tk-362/deyatelnost-tk362/prikazy-ob-utverzhdenii-natsionalnykh-standartov/prikaz-rosstandarta-ot-18-yanvarya-2024-g-n-24-st свободный. - Загл. с экрана.

56. ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования». Разработан с целью регулирования работ, связанных с созданием защищённого ПО и обеспечением оперативного устранения обнаруженных в нём уязвимостей и недостатков. (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2024 г. N 1504-ст). [Электронный ресурс]. Режим доступа: https://base.garant.ru/410749342/ свободный. - Загл. с экрана.

57. ГОСТ Р 71753-2024 «Защита информации. Системы автоматизированного управления учётными записями и правами доступа. Общие требования». Даёт рекомендации по разработке и внедрению таких систем. (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 30 октября 2024 г. N 1558-ст). [Электронный ресурс]. Режим доступа: https://fstec.ru/tk-

362/deyatelnost-tk362/prikazy-ob-utverzhdenii-natsionalnykh-standartov/prikaz-rosstandarta-ot-30-oktyabrya-2024-g-n-1558-st свободный. - Загл. с экрана.

58. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27001-2021 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. N 1653-ст). [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200181890 свободный. - Загл. с экрана.

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

60. 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».

61. Положение о единой балльно-рейтинговой системе оценивания успеваемости студентов и ее использовании при проведении текущей и промежуточной аттестации, утвержденное приказом ФГБОУ ВО «Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации» от 12 декабря 2024 г. № 02-2531.

8.4. Интернет-ресурсы

1. www.kremlin.ru Президент Российской Федерации
2. www.gov.ru Сервер органов государственной власти Российской Федерации
3. www.pravo.gov.ru. Официальный Интернет-портал правовой информации
4. https://epp.genproc.gov.ru/web/gprf Генеральная прокуратура РФ
5. http://www.gov.ru/main/page7.html Федеральное собрание РФ
6. http://www.duma.gov.ru/ Государственная Дума ФС РФ
7. www.vsrf.ru Верховный Суд Российской Федерации
8. www.ksrf.ru Конституционный Суд Российской Федерации
9. 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 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.

9.2. Информационные технологии, программное обеспечение:

При осуществлении образовательного процесса по дисциплине используются 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, средстваработы с презентационными материалами и т.д.).
5. Архиватор 7-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. 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. 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-правовая система «Консультант».
9. http://www.garant.ru/ Справочно-правовая система «Гарант».