

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.08 Кибербезопасность

42.04.05 Медиакоммуникации

«Медиаменеджмент и связи с общественностью в государственных и
бизнес-структурах»

Заочная формы обучения

Год набора – 2026

Барнаул

Автор(ы)-составитель(и) РПД:

Лопухов Виталий Михайлович, доцент кафедры гуманитарных и естественнонаучных дисциплин

Заведующий кафедрой:

Лысенко Лариса Михайловна, к.с-х.н., доцент, заведующий кафедрой гуманитарных и естественнонаучных дисциплин

Рабочая программа дисциплины Б1.О.08 Кибербезопасность одобрена на заседании кафедры гуманитарных и естественнонаучных дисциплин протокол № 1 от «26» августа 2025 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
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.О.08 Кибербезопасность 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
ФГОС ВО	ОПК-6.	Способен отбирать и внедрять в процесс медиапроизводства современные технические средства и информационно-коммуникационные технологии	ОПК-6.1	Использует современные технические средства и информационно-коммуникационные технологии в профессиональной деятельности для обеспечения эффективного медиапроизводства.	ОПК-6. Н-1 Владеет навыками оценки потенциальных рисков и угроз безопасности при осуществлении продвижения социально значимых проектов

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

Общий объем дисциплины:

2,00 з.е., 72 ак.час.

Контактная работа обучающихся с преподавателем по видам учебных занятий: 12 ак. час на контактную работу с преподавателем, из них 4 ак.час на лекции и 8 ак.час на практические занятия. 60 ак. час на самостоятельную работу обучающихся.

Б1.О.08 Кибербезопасность реализуется на 2-м курсе.

3. Содержание и структура дисциплины (модуля)

3.1. Структура дисциплины (модуля)

№ 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/ПОЗ									
Тема 1	Концептуальная модель кибербезопасности	19	1	0	0	2	0	0	0	0	0	0	0	16	Тестирование
Тема 2	Конфиденциальная информация в киберпространстве.	19	1	0	0	2	0	0	0	0	0	0	0	16	Тестирование

	Законодательство Российской Федерации о кибербезопасности													
Тема 3	Обеспечение кибербезопасности медиапроизводства	34	2	0	0	4	0	0	0	0	0	0	28	Тестирование, Доклад-презентация
Промежуточная аттестация		0	0	0	0	0	0	0	0	0	0	0	0	Зачет
Итого		72	4	0	0	8	0	0	0	4	0	0	60	

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. Концептуальная модель кибербезопасности. ОПК-6.1.

Кибербезопасность как наука и научная дисциплина. Актуальность защиты информации. Терминология области защиты данных. Преступления в сфере компьютерной информации. Система защиты информации. Концептуальная модель кибербезопасности: угрозы информации, объекты угроз, цели злоумышленников, способы защиты информации, источники угроз, основные направления, средства защиты информации, действия, приводящие к неправомерному овладению конфиденциальной информацией. Модели области защиты данных. Направления обеспечения кибербезопасности: правовое, организационное и инженерно-техническое. Комплексный подход к разработке системы защиты информации. Противоправные действия с информацией. Угрозы кибербезопасности профессиональной деятельности. Классификация угроз и специфические виды угроз для компьютерных сетей. Цели, субъекты и уровни уязвимости кибербезопасности. Каналы утечки информации. Пути несанкционированного доступа к информации. Проектирование системы обеспечения кибербезопасности. Типовой порядок действий по обеспечению кибербезопасности. Использование информации в компьютерных сетях для совершения правонарушений и преступлений. Критерии безопасности компьютерных систем. Криптографическая защита. Электронная подпись. Разграничение доступа, ролевое управление доступом. Защита компьютерных систем. Идентификация и аутентификация. Компьютерные вирусы и вредоносное программное обеспечение. Восстановление данных. Анализ защищённости. Служба защиты информации и её организационно-методическая работа. Мониторинг информационного обмена и аудит действий пользователей в компьютере. Методы и средства физической, программной, аппаратной и криптографической защиты информации. Правила поведения в сети «Интернет» и «компьютерная гигиена». Преступления в «киберпространстве», «кибервойна». Принципы кибербезопасности. Экспертные группы, занимающиеся изучением инцидентов компьютерной безопасности. Предметные области кибербезопасности и ее субъекты¹.

¹ Данный вопрос относится к одному из направлений воспитательной работы с обучающимися в соответствии с рабочей программой воспитания.

Тема 2. Конфиденциальная информация в киберпространстве. Законодательство Российской Федерации о кибербезопасности. ОПК- 6.1.

Доступ к информации, классификация информации по доступу к ней. Виды информации ограниченного доступа в медиапроизводстве. Правовое регулирование профессиональной тайны. Обеспечение профессиональной тайны. Правовое регулирование профессиональной тайны. Структура и состав организационно-правового обеспечения профессиональной тайны. Проблемы правовой ответственности в сфере профессиональной тайны. Обеспечение защиты персональных данных. Структура и состав организационно-правового обеспечения защиты персональных данных. Проблемы правовой ответственности в сфере персональных данных. Виды служебной и профессиональной тайн. Правовое регулирование служебной и профессиональной тайны. Объекты авторского и патентного права, их правовое регулирование. Структура информационного законодательства о кибербезопасности в Российской Федерации. Международное законодательства о кибербезопасности. Правовое обеспечение безопасности в информационной сфере. Государственные регуляторы в области кибербезопасности. Стандарты в сфере кибербезопасности. Защита прав граждан в информационной сфере. Государственная политика в сфере обеспечения кибербезопасности. Нормативные документы по кибербезопасности медиапроизводства. Интернет как явление и процесс. Правовые проблемы Интернета. Нормативная правовая база по вопросам функционирования сети «Интернет» в России. Правовые аспекты обеспечения безопасности в Интернете. Ответственность за нарушение законодательства в области информационной безопасности. Современные проблемы кибербезопасности в России. Положительный опыт зарубежных государств в правовом обеспечении кибербезопасности.

Тема 3. Обеспечение кибербезопасности медиапроизводства. ОПК-6.1.

Противоправные действия с информацией. Угрозы информационной безопасности в медиасреде. Использование информации в компьютерных сетях для совершения правонарушений и преступлений. Критерии безопасности компьютерных систем. Криптографическая защита. Электронная подпись. Экранирование, персональные и корпоративные межсетевые экраны, их назначение. Разграничение доступа, ролевое управление доступом. Защита компьютерных систем. Идентификация и аутентификация, парольная аутентификация, идентификация/аутентификация с помощью биометрических данных.

Правила выбора пароля. Сетевые вирусы. Правила поведения в сети «Интернет» и «компьютерная гигиена». Преступления в «киберпространстве», «кибервойна».

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.О.08 Кибербезопасность 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 предложенных	Прочитайте текст, выберите правильный ответ	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	Прочитайте текст, выберите правильные ответы	<ol style="list-style-type: none"> 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 	Ответ считается верным, если правильно установлены все соответствия (позиции из

правильных ответов из нескольких вариантов предложенных		<p>2. Внимательно прочитать предложенные вариант-ты ответа.</p> <p>3. Выбрать несколько правильных ответов.</p> <p>4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).</p>	одного столбца верно сопоставлены с позициями другого)
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	<p>1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.</p> <p>2. Внимательно прочитать предложенные варианты ответа.</p> <p>3. Построить верную последовательность из предложенных элементов.</p> <p>4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).</p>	Ответ считается верным, если правильно указана вся последовательность цифр
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа	<p>1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.</p> <p>2. Внимательно прочитать предложенные варианты ответа.</p> <p>3. Выбрать один верный ответ.</p> <p>4. Записать только номер (или букву) выбранного варианта ответа.</p>	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа

		5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	<p>1. Внимательно прочитать текст задания и понять суть вопроса.</p> <p>2. Продумать логику и полноту ответа.</p> <p>3. Записать ответ, используя четкие компактные формулировки.</p> <p>4. В случае расчетной задачи, записать решение и ответ</p>	<p>Ответ считается верным:</p> <p>1. Отсутствие фактических ошибок.</p> <p>2. Раскрытие объема используемых понятий (полнота ответа).</p> <p>3. Обоснованность ответа (наличие аргументов).</p> <p>4. Логическая последовательность излагаемого материала.</p>

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС²

Итоговая балльная оценка	Традиционная система	Бинарная система	ECTS	
			Для традиционной системы	Для бинарной системы
	Отлично	Зачтено	A	P/ Passed
			B	P/ Passed
	Хорошо		C	P/ Passed
			D	P/ Passed
	Удовлетворительно		E	P/ Passed
	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.О.08 Кибербезопасность используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Тестирование, Доклад-презентация.

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

Тема 1. Концептуальная модель кибербезопасности. ОПК-6.1.

² БРС при изучении данной дисциплины не применяется.

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

Тест 1

Укажите термин, соответствующий определению: средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

- а) Компьютерная атака;
- б) Компьютерный инцидент;
- в) Защищаемый объект информатизации;
- г) Техника защиты информации;

Тест 2

Укажите термин, соответствующий определению: комплекс мер для защиты компьютерных систем, сетей, программ и данных от цифровых атак, кражи информации и повреждения. Её цель— обеспечить конфиденциальность, целостность и доступность данных в цифровой среде путем предотвращения несанкционированного доступа и минимизации рисков

- а) Кибербезопасность;
- б) Система защиты информации;
- в) Основы безопасности жизнедеятельности;
- г) Цифровые права.

Тест 3

Ботнет - это ...

- а) Это компьютерная сеть (network), состоящая из некоторого количества хостов, с запущенными ботами (robot), т.е. автономным ПО;
- б) Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей;
- в) DDoS- атака, которая начинается с чужого адреса, скрывающего хакера;
- г) Внедрение сторонних данных или команд в систему с целью изменения хода работы системы и получения доступа к закрытым функциям и информации.

**Тема 2. Конфиденциальная информация в киберпространстве.
Законодательство Российской Федерации о кибербезопасности. ОПК-6.1.**

Тестовые задания с инструкцией по выполнению и ключами правильных ответов:

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)).

Тест 1.

Какой вид тайны определяется как Режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

- а) Коммерческая;
- б) Государственная;
- в) Служебная;
- г) Профессиональная;

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 буквы выбранного варианта ответа (например, а), в)).

Тест 2.

Укажите, что относится к видам служебной и профессиональной тайн.

Варианты ответа:

- a. Государственная тайна
- b. Персональные данные
- c. Адвокатская тайна
- d. Тайна страхования
- e. Банковская тайна
- f. Нотариальная тайна
- g. Тайна судопроизводства

h. Тайна связи

Тест 3.

Укажите виды конфиденциальной информации, связанной с хозяйственной деятельностью.

Варианты ответа:

- a. коммерческая тайна
- b. объекты авторского права
- c. объекты патентного права
- d. сведения, содержащие государственную тайну
- e. персональные данные
- f. общедоступная информация

Тема 3. Обеспечение кибербезопасности медиапроизводства. ОПК-6.1.

Тестовые задания с инструкцией по выполнению и ключами правильных ответов:

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)).

Укажите к какому этапу работы службы безопасности с сотрудниками, владеющими конфиденциальными сведениями организации, относятся следующие действия:

- написание сотрудником заявления с указанием причины увольнения;
- прием служебной конфиденциальной документации всех числящихся за сотрудником документов;
- сдача сотрудником пропуска для входа в рабочую зону, всех ключей, печатей и паролей;
- проведение с сотрудником беседы с целью напоминания ему об обязательстве сохранения тайны, а также выяснения истинной причины увольнения, что должно убереечь работодателя от такой угрозы, как «обиженные сотрудники».

а) Подготовка приема сотрудников для работы с информацией ограниченного доступа;

- б) Отбор кандидатов на работу, связанную с конфиденциальной информацией;
- в) Текущая работа с персоналом, владеющим конфиденциальной информацией, а также его контроль;
- г) Увольнение сотрудника, владеющего конфиденциальной информацией.

Тест 2.

Укажите документ(ы), где указывается:

- порядок сохранения тайны при проведении совещаний, заседаний и переговоров;
 - требования к помещению для работы с конфиденциальной информацией;
 - порядок охраны территории, зданий, помещений, транспортных средств и персонала;
 - порядок пропускного режима помещений, учет и порядок выдачи пропусков и удостоверений.
- а) Технологический документ "Инструкция по обеспечению безопасности конфиденциальной информации";
 - б) основополагающие документы (устав организации, типовые соглашения и контракты);
 - в) Технологический документ "Перечень сведений конфиденциального характера";
 - г) Организационно-методические документы (положение о службе безопасности, положение о службе конфиденциальной документации и должностные инструкции сотрудников этих служб);
 - д) Технологический документ "Инструкция по обработке, хранению и движению конфиденциальных документов";

Тест 3.

Укажите к какому этапу работы службы безопасности с сотрудниками, владеющими конфиденциальными сведениями организации, относятся следующие действия:

- подбор предполагаемого кандидата;
- изучение резюме или личного дела руководителем структурного подразделения и службы безопасности;
- информирование кандидатов об их будущих обязанностях, связанных с владением конфиденциальной информацией;
- обновление материалов личного дела, работающего в фирме

сотрудника, получение представления на новую должность от руководителя структурного подразделения.

а) Подготовка приема сотрудников для работы с информацией ограниченного доступа;

б) Отбор кандидатов на работу, связанную с конфиденциальной информацией;

в) Текущая работа с персоналом, владеющим конфиденциальной информацией, а также его контроль;

г) Увольнение сотрудника, владеющего конфиденциальной информацией.

Критерии оценивания тестовых заданий:

Система оценивания	Описание критерия	
Отлично	Свыше 80% правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.
Хорошо	Свыше 65% и менее 80% правильных ответов.	Обучающимся материал освоен полностью, без существенных ошибок.
Удовлетворительно	Свыше 50% и менее 65% правильных ответов.	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.
Не удовлетворительно	Менее 50% правильных ответов.	Обучающимся материал не освоен, знания обучающегося ниже базового уровня.

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	Коэффициент веса контрольной точки
КТ 1	0,5
КТ 2	0,2
Итого:	0,7

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 3.

Доклад-презентация.

Подготовка докладов-презентаций «Методы и средства обеспечения кибербезопасности». Доклады с обсуждением возможности применения методов и средств в медиасфере.

Тематика докладов-презентаций (примерная):

1. Информационная безопасность образовательного процесса. Актуальность включения дисциплины по информационной безопасности в программу среднего общего образования.
2. Политика информационной безопасности при работе в сети «Интернет»
3. Защита персональных данных
4. НПА области защиты информации. Правовые коллизии и дыры.
5. Положительный опыт зарубежных государств в правовом обеспечении информационной безопасности
6. Big Data: польза и угрозы
7. Польза и угрозы современных информационных технологий
8. Фиксация «электронных» доказательств. Юридическая сила электронной информации.
9. Возможные угрозы при цифровизации
10. Судебные компьютерные экспертизы. Применение ИТ для осуществления электронного уголовно-процессуального доказывания.
11. Специалисты в информационной безопасности
12. Социальная инженерия
13. Обеспечение ИБ при использовании беспроводных сетей
14. Статистика и примеры нарушений ИБ; «кибервойна»
15. Политика ИБ
16. Методика расследования преступлений в сфере компьютерных технологий.
17. Настройка безопасной работы ПК с ОС Windows

18. Восстановление потерянных данных
19. Электронная подпись
20. Защита сведений, относящихся в коммерческой тайне
21. Комплексная защита информации физического лица
22. Возможные угрозы информации физического лица
23. Противодействие мошенничеству
24. Стандарты и методики в области ИБ
25. Компании, основной функцией которых является защита информации (российские, в Алтайском крае, Новосибирской области)
26. Блокчейн и цифровые валюты: польза и угрозы
27. Теневой Интернет
28. Организационно-правовые вопросы информационной безопасности цифровой экономики
29. Цифровые права и цифровой след: польза и угрозы
30. Смарт-контракты и токены: польза и угрозы
31. Современные цифровые технологии: польза и угрозы
32. Массовые социально значимые услуги (сервисы), переведённые в электронный формат: польза и угрозы
33. Интернет вещей: польза и угрозы
34. Искусственный интеллект: польза и угрозы
35. Гаджеты, электронные устройства: польза и угрозы
36. Маркетплейсы: польза и угрозы
37. Виртуальная и дополненная реальность (VR и AR) : польза и угрозы
38. Облачные технологии: польза и угрозы
39. Мессенджеры: польза и угрозы

Критерии оценивания доклада (не удовлетворительно, удовлетворительно, хорошо или отлично):

- новизна информации (информация об актуальных цифровых технологиях/инструментах/ресурсах с указанием конкретно кем и где на данный момент востребованы;
- доходчивость пояснения нового материала (введение терминологии из НПА и научной литературы; классификация; примеры, в том числе из судебной практики; представление сложно воспринимаемой информации в двух видах);
- актуальность информации (источники не старше 5 лет),
- освещение нормативного регулирования вопроса (Российское законодательство на различных уровнях, законопроекты, международные

акты, положительный опыт зарубежного правового регулирования вопроса, выявленные проблемы правового регулирования),

- рассмотрение вопроса о развитии и трендах (цели и задачи развития, польза, что будет в будущем, современные угрозы, направления развития и новшества, которые будут в ближайшем будущем),

- примеры использования указанного инструментария (скриншоты, пошаговые инструкции, демоверсии, способы получения доступа к информации),

- практическая значимость (польза данной информации для применения в профессиональной и жизнедеятельности, методические рекомендации по полезному и безопасному использованию).

Критерии оценки	Вклад в оценку, %	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

Система оценивания	Итого
Отлично	Свыше 80%
Хорошо	Свыше 65% и менее 80%
Удовлетворительно	Свыше 50% и менее 65%
Не удовлетворительно	Менее 50%

КТ – 2.

Темы 1-3.

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

Укажите термин, соответствующий определению: совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

- а) Информационная сфера;
- б) Угроза информационной безопасности РФ;
- в) Информационная безопасность;
- г) Обеспечение информационной безопасности;
- д) Система обеспечения информационной безопасности;
- е) Информационная инфраструктура.

Какой действующий ФЗ определяет персональные данные?

- а) 63-ФЗ;
- б) 152-ФЗ;
- в) 149-ФЗ;
- г) Постановление Правительства РФ № 1114;

Укажите документ(ы), где указывается:

- обязанности сотрудника фирмы при работе с конфиденциальной информацией;
- порядок доступа сотрудников к конфиденциальным документам, оформление доступа;
- обеспечение сохранности документов на всех видах носителей при работе с ними.

а) организационно-методические документы (положение о службе безопасности, положение о службе конфиденциальной документации и должностные инструкции сотрудников этих служб);

б) основополагающие документы (устав организации, типовые соглашения и контракты);

в) Технологический документ "Перечень сведений конфиденциального

характера";

г) Технологический документ "Инструкция по обеспечению безопасности конфиденциальной информации";

д) Технологический документ "Инструкция по обработке, хранению и движению конфиденциальных документов";

Критерии оценивания тестовых заданий:

Система оценивания	Описание критерия	
Отлично	Свыше 80% правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.
Хорошо	Свыше 65% и менее 80% правильных ответов.	Обучающимся материал освоен полностью, без существенных ошибок.
Удовлетворительно	Свыше 50% и менее 65% правильных ответов.	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.
Не удовлетворительно	Менее 50% правильных ответов.	Обучающимся материал не освоен, знания обучающегося ниже базового уровня.

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

6.1. Промежуточная аттестация (зачет) проводится в форме компьютерного тестирования.

6.2. Типовые оценочные материалы промежуточной аттестации

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

Тема 1. Концептуальная модель кибербезопасности. ОПК-6.1.

Тест 1

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

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать один правильный ответ.

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

Укажите термин, соответствующий определению: совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

- а) Информационная сфера;
- б) Угроза информационной безопасности РФ;
- в) Информационная безопасность;
- г) Обеспечение информационной безопасности;
- д) Система обеспечения информационной безопасности;
- е) Информационная инфраструктура.

Укажите термин, соответствующий определению: средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

- а) Компьютерная атака;
- б) Компьютерный инцидент;
- в) Защищаемый объект информатизации;
- г) Техника защиты информации;

Укажите термин, соответствующий определению: комплекс мер для защиты компьютерных систем, сетей, программ и данных от цифровых атак, кражи информации и повреждения. Её цель— обеспечить конфиденциальность, целостность и доступность данных в цифровой среде путем предотвращения несанкционированного доступа и минимизации рисков

- а) Кибербезопасность;
- б) Система защиты информации;
- в) Основы безопасности жизнедеятельности;
- г) Цифровые права.

Ботнет - это ...

- а) Это компьютерная сеть (network), состоящая из некоторого количества хостов, с запущенными ботами (robot), т.е. автономным ПО;
- б) Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей;
- в) DDoS- атака, которая начинается с чужого адреса, скрывающего хакера;
- г) Внедрение сторонних данных или команд в систему с целью изменения хода работы системы и получения доступа к закрытым функциям и

информации.

Тест 2.

Вопросы на расстановку по порядку

Расставьте в порядке убывания частоты появления (первое – самое часто появляющееся по статистике) внутренние и внешние угрозы:

– 1	– совершаются случайными лицами
– 2	– совершаются собственными сотрудниками фирмы либо при их прямом или опосредованном участии
– 3	– совершаются извне – внешние угрозы

Упорядочите в хронологическом порядке этапы работы компьютерного вируса:

– 1	– вирусный код внедряет свой вирусный код в другие файлы компьютера или нарушает нормальную работу компьютера
– 2	– зараженный вирусом файл попадает на компьютер
– 3	– когда начинается работа с зараженным файлом, незаметно активизируется встроенный в него участок вирусного кода

Тест 3.

Вопросы открытого типа.

Прочитайте текст вопроса и запишите развернутый ответ:

№ п.п.	Вопрос	Ответ
1.	Кибербезопасность, отличие от информационной безопасности	
2.	Классификация компьютерных вирусов и их виды	
3.	Меры защиты в кибербезопасности	

4.	Угроза защиты в кибербезопасности	
----	-----------------------------------	--

**Тема 2. Конфиденциальная информация в киберпространстве.
Законодательство Российской Федерации о кибербезопасности. ОПК-6.1.**

Тестовые задания с инструкцией по выполнению и ключами правильных ответов:

Тест 1.

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

2. Внимательно прочитайте предложенные варианты ответа.

3. Выбрать один верный ответ.

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

Какой действующий ФЗ определяет персональные данные?

а) 63-ФЗ;

б) 152-ФЗ;

в) 149-ФЗ;

г) Постановление Правительства РФ № 1114;

Какой вид тайны определяется как Режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

а) Коммерческая;

б) Государственная;

в) Служебная;

г) Профессиональная;

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

2. Внимательно прочитайте предложенные варианты ответа.

3. Выбрать несколько правильных ответов.

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

Укажите, что относится к видам служебной и профессиональной тайн.

Варианты ответа:

- i. Государственная тайна
- j. Персональные данные
- k. Адвокатская тайна
- l. Тайна страхования
- m. Банковская тайна
- n. Нотариальная тайна
- o. Тайна судопроизводства
- p. Тайна связи

Укажите виды конфиденциальной информации, связанной с хозяйственной деятельностью.

Варианты ответа:

- g. коммерческая тайна
- h. объекты авторского права
- i. объекты патентного права
- j. сведения, содержащие государственную тайну
- k. персональные данные
- l. общедоступная информация

Тест 2.

Задание на установление соответствия и на выставления порядка:

Расставьте в порядке убывания частоты появления (первое – самое часто появляющееся по статистике) методы неправомерного овладения конфиденциальной информацией:

– 1	– традиционный обмен производственным опытом
– 2	– отсутствие на фирме надлежащего контроля и жестких условий обеспечения информационной безопасности
– 3	– несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок
– 4	– разглашение (излишняя болтливость сотрудников)
– 5	– наличие предпосылок возникновения среди сотрудников конфликтных ситуаций
– 6	– отсутствие высокой трудовой дисциплины, психологическая несовместимость, случайный подбор кадров, слабая работа кадров по сплочению коллектива

– 7	– бесконтрольное использование информационных систем
-----	--

А) Соедините правильным образом термины и их определения:

Б) Расставьте термины в предложение: «Внедрённая ... и ... - являются, действиями, нарушающими ... и относятся к»

а. Преступление в сфере компьютерной информации	I.уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация
б. Вредоносная программа	II.созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети
с. Неправомерный доступ	III.несанкционированное обращение к компьютерной информации
д. Информационная безопасность	IV.все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки

Тест 3.

Вопросы открытого типа.

Прочитайте текст и запишите развернутый обоснованный ответ:

№ п.п.	Вопрос	Ответ
1)	Профессиональная тайна и её виды	

2)	Государственная тайна	
3)	Служебная тайна, основные признаки и виды	
4)	Объекты авторских прав	

Тема 3. Обеспечение кибербезопасности медиапроизводства. ОПК-6.1.

Тестовые задания с инструкцией по выполнению и ключами правильных ответов:

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)).

Укажите документ(ы), где указывается:

- обязанности сотрудника фирмы при работе с конфиденциальной информацией;

- порядок доступа сотрудников к конфиденциальным документам, оформление доступа;

- обеспечение сохранности документов на всех видах носителей при работе с ними.

а) организационно-методические документы (положение о службе безопасности, положение о службе конфиденциальной документации и должностные инструкции сотрудников этих служб);

б) основополагающие документы (устав организации, типовые соглашения и контракты);

в) Технологический документ "Перечень сведений конфиденциального характера";

г) Технологический документ "Инструкция по обеспечению безопасности конфиденциальной информации";

д) Технологический документ "Инструкция по обработке, хранению и движению конфиденциальных документов";

Укажите к какому этапу работы службы безопасности с сотрудниками, владеющими конфиденциальными сведениями организации, относятся следующие действия:

- написание сотрудником заявления с указанием причины увольнения;
- прием служебной конфиденциальной документации всех числящихся за сотрудником документов;
- сдача сотрудником пропуска для входа в рабочую зону, всех ключей, печатей и паролей;
- проведение с сотрудником беседы с целью напоминания ему об обязательстве сохранения тайны, а также выяснения истинной причины увольнения, что должно уберечь работодателя от такой угрозы, как «обиженные сотрудники».

а) Подготовка приема сотрудников для работы с информацией ограниченного доступа;

б) Отбор кандидатов на работу, связанную с конфиденциальной информацией;

в) Текущая работа с персоналом, владеющим конфиденциальной информацией, а также его контроль;

г) Увольнение сотрудника, владеющего конфиденциальной информацией.

Укажите документ(ы), где указывается:

- порядок сохранения тайны при проведении совещаний, заседаний и переговоров;

- требования к помещению для работы с конфиденциальной информацией;

- порядок охраны территории, зданий, помещений, транспортных средств и персонала;

- порядок пропускного режима помещений, учет и порядок выдачи пропусков и удостоверений.

а) Технологический документ "Инструкция по обеспечению безопасности конфиденциальной информации";

б) основополагающие документы (устав организации, типовые соглашения и контракты);

в) Технологический документ "Перечень сведений конфиденциального характера";

г) Организационно-методические документы (положение о службе безопасности, положение о службе конфиденциальной документации и

должностные инструкции сотрудников этих служб);

д) Технологический документ "Инструкция по обработке, хранению и движению конфиденциальных документов";

Укажите к какому этапу работы службы безопасности с сотрудниками, владеющими конфиденциальными сведениями организации, относятся следующие действия:

- подбор предполагаемого кандидата;

- изучение резюме или личного дела руководителем структурного подразделения и службы безопасности;

- информирование кандидатов об их будущих обязанностях, связанных с владением конфиденциальной информацией;

- обновление материалов личного дела, работающего в фирме сотрудника, получение представления на новую должность от руководителя структурного подразделения.

а) Подготовка приема сотрудников для работы с информацией ограниченного доступа;

б) Отбор кандидатов на работу, связанную с конфиденциальной информацией;

в) Текущая работа с персоналом, владеющим конфиденциальной информацией, а также его контроль;

г) Увольнение сотрудника, владеющего конфиденциальной информацией.

Тест 2.

Задание на установление соответствия:

1) Соедините правильным образом термины и их определения:

а. Система защиты информации	І. – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации
------------------------------	---

b. Угроза	II. – потенциальная причина инцидента, который может нанести ущерб системе или организации
c. Конфиденциальность информации	III. – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
d. Информационная война	IV. – противостояние между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массовой психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противостоящей стороны

Отнесите средство или метод защиты информации из правого столбца с направлением обеспечения информационной безопасности в левом столбце

– Правовое обеспечение	– Политика защиты информации
– Организационное обеспечение	– Разработка документа "Перечень сведений конфиденциального характера"
– Инженерно-техническое обеспечение	– Аудит действий пользователя ПК
	– Мониторинг за работой сотрудников с конфиденциальными сведениями
	– Системы контроля и управление доступом
	– Антивирусные программы
	– Система видеонаблюдения
	– Охранные системы и средства

	охранной сигнализации
--	-----------------------

Тест 3.

Вопросы открытого типа.

Прочитайте текст вопроса и запишите развернутый ответ:

№ п.п.	Вопрос	Ответ
1)	Защита информации и требования к этому процессу	
2)	Организационное обеспечение информационной безопасности, его основные меры	
3)	Утечка, как действие, приводящие к неправомерному овладению конфиденциальной информацией	
4)	Несанкционированный доступ (НСД), как действие, приводящие к неправомерному овладению конфиденциальной информацией	

6.3. Критерии и шкала оценивания на основе БРС³.

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно,	Отлично/зачтено

³ БРС при изучении данной дисциплины не применяется.

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.	Хорошо/зачтено
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.	Удовлетворительно/зачтено
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.	Неудовлетворительно/не зачтено

7. Методические материалы по освоению дисциплины (модуля)

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. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — 2-е изд. — Москва, Вологда : Инфра-Инженерия, 2025. — 692 с. — ISBN 978-5-9729-2520-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/154736.html>
2. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В.А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/555950>
3. Биометрические средства идентификации и аутентификации человеческой личности в системах информационной безопасности : учебное пособие / Н. В. Болдырихин, И. А. Сосновский, О. В. Куликова [и др.] ; под редакцией Л. В. Черкесовой. — Ростов-на-Дону : Донской государственный технический университет, 2024. — 326 с. — ISBN 978-5-7890-2263-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/150044.html>
4. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/580668>

8.2. Дополнительная литература

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 266 с. — ISBN 978-5-4497-3316-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/142285.html>

2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542739>

3. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов : Вузовское образование, 2024. — 214 с. — ISBN 978-5-4487-1026-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/142805.html>

4. 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>

8.3. Нормативные правовые документы и иная правовая информация

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями) информации". [Электронный ресурс]. URL: Гарант / Справочные правовые системы. 2025. Режим доступа: <http://www.garant.ru>.

2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями и дополнениями). [Электронный ресурс]. URL: Гарант / Справочные правовые системы. 2025. Режим доступа: <http://www.garant.ru>.

3. Указ Президента РФ от 22.05.2015 N 260 «О некоторых вопросах информационной безопасности РФ». [Электронный ресурс]. URL: Гарант / Справочные правовые системы. 2025. Режим доступа: <http://www.garant.ru>.

4. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры РФ». [Электронный ресурс]. URL: Гарант / Справочные правовые системы. 2025. Режим доступа: <http://www.garant.ru>.

8.4. Интернет-ресурсы

1. Информационная безопасность в СМИ. Режим доступа: https://spravochnick.ru/informatika/informacionnaya_bezopasnost_v_smi/
2. Информационная безопасность в медийной среде. Режим доступа: <https://smif.spbu.ru/ru/publikatsii/2-uncategorised/136-informatsionnaya-bezopasnost-v-medijnoj-srede-2.html>
3. Портал правовой информации Российской Федерации. Режим доступа: pravo.gov.ru
4. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Режим доступа: <https://digital.gov.ru/ru/>
5. Национальный проект «Экономика данных и цифровая трансформация государства» <https://digital.gov.ru/target/naczionalnyj-proekt-ekonomika-dannyh-i-czifrovaya-transformacziya-gosudarstva>

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

Алтайский филиал РАНХиГС имеет комплексное современное материально-техническое оснащение, призванное поддерживать разные форматы обучения и позволяющее кардинально трансформировать учебный процесс, выходя далеко за пределы традиционной лекционной модели. Филиал располагает учебными аудиториями для проведения занятий лекционного типа, лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов, а также специализированными помещениями, такими как (компьютерный класс, электронный зал для самостоятельной работы).

Оснащение учебных аудиторий и иных помещений в Алтайском филиале РАНХиГС представлено современными технологиями и оборудованием, включая интерактивные панели и доски, системы видеоконференцсвязи, звуковое оборудование и высокоскоростной Wi-Fi, проекторы или ЖК-панели, а также удобную и эргономичную мебель. Все

учебные аудитории оснащены компьютерным оборудованием и лицензионным программным обеспечением. При реализации дисциплины «Б1.О.08 Кибербезопасность» используются следующее программное обеспечение и информационно-справочные системы: (Microsoft Windows, Р7-Офис, Microsoft Office, Гарант, КонсультантПлюс).