Лебедева
Екатерина
Александровна

Подписано цифровой подписью:
Лебедева Екатерина
Александровна
Дата: 2026.06.25 12:28:16 +03'00'

Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.06 Кибер преступления и национальная безопасность

40.04.01 Юриспруденция
(код, наименование направления подготовки)

Юридическое обеспечение национальной безопасности

заочная форма обучения
(форма обучения)

Год набора – 2026
Нижний Новгород, 2026 г.

Автор(ы)-составитель(и) РПД:

Хмельницкая Татьяна Владимировна, доцент кафедры правового обеспечения национальной безопасности, канд. юрид. наук

Заведующий кафедрой:

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

Рабочая программа дисциплины Б1.В.06 Кибер преступления и национальная 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
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.06 Кибер преступления и национальная 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**
Организация и осуществление криминалистической деятельности, связанной с проведением следственных и иных процессуальных действий с целью предварительного расследования преступлений (ОТФ (А) Выполнение отдельных функций процессуального контроля (ТФ (А/02.7)	ПКс 2.1	Способен устранять признаки нарушения требований законодательства в сфере безопасности Российской Федерации	ИПКс -2.1.1	Демонстрирует способность анализировать обстоятельства возникновения признаков нарушения требований законодательства в сфере безопасности Российской Федерации	ИПКс 2.1.1 З.1 ***Знает:*** Знает признаки нарушения требований законодательства в сфере безопасности Российской Федерации ИПКс -2.1.1 У-1. ***Умеет:*** анализировать обстоятельства возникновения признаков нарушения требований законодательства в сфере безопасности Российской Федерации

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

общий объем дисциплины:

заочная форма обучения:

3 з.е., 108 ак.час.

1 сем. - лекции – 4 а.ч., практические занятия – 8 а.ч., самостоятельная работа – 87 а.ч., экзамен – 9 а.ч.

Б1.В.06 Кибер преступления и национальная безопасность реализуется на 1,2-м семестрах 1-го курса после изучения дисциплин:

- Государственная и общественная безопасность.
- Финансово-экономическая безопасность.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Заочная форма обучения

№ п/п	Наименование тем и (или) разделов		Объем дисциплины, ак.час											Форма текущего контроля успеваемости, промежуточной аттестации
		ВСЕГО	Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа		
			Период теоретического обучения						Период промежуточной аттестации (сессия)					
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Кат тэк	Контроль	СРкр	СРэк	СР
			Л	ВЛ	ЛР	ПЗ								
Тема 1.	Кибер преступления как угроза обеспечения национальной безопасности	20	2	0	0	2	0	0	0	0		0	0	16	Устный опрос, доклады

Тема 2.	Нормативно-правовое обеспечение кибер безопасности	18	0	0	0	2	0	0	0	0	0	0	16	Устный опрос, доклады
Тема 3.	Уголовно-правовая характеристика преступлений, совершаемых в киберпространстве	20	2	0	0	2	0	0	0	0	0	0	16	Устный опрос, доклады
Тема 4.	Расследование отдельных видов преступлений в сфере компьютерной информации	18	0	0	0	2	0	0	0	0	0	0	16	Устный опрос, доклады
Тема 5.	Расследование хищений, совершаемых с использованием сети Интернет	23	0	0	0	0	0	0	0	0	0	0	23	Устный опрос, доклады
Промежуточная аттестация		9	0	0	0	0	0	0	0	9	0	0	0	Экзамен

Итого		**108**	**4**	**0**	**0**	**8**	**0**	**0**	**0**	**9**	**0**	**0**	**87**	

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. Киберпреступления как угроза обеспечения национальной безопасности ПКс-2.1.

1. Национальная безопасность: понятие и ее содержание.
2. Виды угроз национальной безопасности.
3. Понятие и сущность киберпреступлений в Российской Федерации.
4. Современное состояние киберпреступности в Российской Федерации.

ТЕМА 2. Нормативно-правовое обеспечение кибербезопасности ПКс-2.1 .

1. Основные понятия информационной безопасности и защиты информации.
2. Доктрина информационной безопасности Российской Федерации.
3. Стратегия развития информационного общества в Российской Федерации.
4. Основы государственной политики Российской Федерации в области международной информационной безопасности.

ТЕМА 3. Уголовно-правовая характеристика преступлений, совершаемых в киберпространстве ПКс-2.1.

1. Объективные признаки преступлений в сфере компьютерной информации.
2. Субъективные признаки преступлений в сфере компьютерной информации.
3. Объективные признаки хищений, совершаемых с использованием сети Интернет.
4. Субъективные признаки хищений, совершаемых с использованием сети Интернет.

ТЕМА 4. Расследование отдельных видов преступлений в сфере компьютерной информации ПКс-2.1.

1. Криминалистическая характеристика неправомерного доступа к компьютерной информации.
2. Особенности возбуждения уголовных дел о неправомерном доступе к компьютерной информации.
3. Особенности производства отдельных следственных действий.
4. Назначение, виды и производство экспертиз по уголовным делам о неправомерном доступе к компьютерной информации.

ТЕМА 5. Расследование хищений, совершаемых с использованием сети Интернет ПКс-2.1 .

1. Криминалистическая характеристика хищений, совершаемых с использованием сети Интернет.
2. Особенности возбуждения уголовных дел о хищениях, совершаемых с использованием сети Интернет.
3. Особенности производства отдельных следственных действий при расследовании хищений, совершаемых с использованием сети Интернет.
4. Назначение, виды и производство экспертиз по уголовным делам о хищениях, совершаемых с использованием сети Интернет.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.06 Кибер преступления и национальная безопасность 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 варианты 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 варианты 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	Прочитайте текст и установите	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается	Ответ считается верным, если правильно указана вся

последовательности	последовательность	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).	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	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 номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	Ответ считается верным, если правильно указана цифра или буква 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.06 Кибер преступления и национальная безопасность используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Устный опрос, ситуационная задача, кейс-задание, тестирование.

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

Тема 1. Киберпреступления как угроза обеспечения национальной безопасности ПКс-2.1

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 содержание национальной безопасности.
2. Виды угроз национальной безопасности.
3. Криминологическая характеристика киберпреступности.

Примерный перечень тем докладов

1. Динамика и структура киберпреступности на современном этапе.
2. Международный опыт борьбы с киберпреступностью.

Тема 2. Нормативно-правовое обеспечение кибербезопасности ПКс-2.1

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 содержание кибербезопасности.
2. Информация и информационная безопасность: понятие и характеристика.
3. Основные направления политики государства в сфере кибербезопасности.

Примерный перечень тем докладов

1. Особенности доктринального подхода к обеспечению информационной безопасности Российской Федерации.
2. Общая характеристика «Стратегии развития информационного общества в Российской Федерации».

Тема 3. Уголовно-правовая характеристика преступлений, совершаемых в киберпространстве ПКс-2.1

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. Характеристика объективных признаков хищений, совершаемых с использованием сети Интернет.
2. Характеристика субъективных признаков хищений, совершаемых с использованием сети Интернет.
3. Понятие и уголовно-правовая характеристика отдельных видов преступлений в сфере компьютерной информации.

Примерный перечень тем докладов

1. Проблемные вопросы квалификации хищений, совершаемых с использованием сети Интернет.
2. Особенности уголовной ответственности за хищения, совершаемые с использованием сети Интернет в зарубежных странах.
3. Особенности уголовной ответственности за совершение преступлений в сфере компьютерной информации.

Тема 4. Расследование отдельных видов преступлений в сфере компьютерной информации ПКс-2.1

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 криминалистическая характеристика преступлений сфере компьютерной информации.
2. Особенности планирования расследования преступлений сфере компьютерной информации
3. Особенности тактики производства отдельных следственных действий при расследовании преступлений сфере компьютерной информации.

Примерный перечень тем докладов

1. Особенности назначения и производства судебных экспертиз по уголовным делам о преступлениях в сфере компьютерной информации.

Тема 5. Расследование хищений, совершаемых с использованием сети Интернет ПКс-2.1

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 криминалистическая характеристика хищений, совершаемых с использованием сети Интернет.
2. Особенности планирования расследования хищений, совершаемых с использованием сети Интернет.
3. Особенности тактики производства отдельных следственных действий при расследовании хищений, совершаемых с использованием сети Интернет.

Примерный перечень тем докладов

1. Особенности назначения и производства судебных экспертиз по уголовным делам о хищениях, совершаемых с использованием сети Интернет.

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

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

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

Наименование контрольной точки	Максимальное количество баллов за работу в рамках КТ, которое может набрать обучающийся	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,1	10
КТ 2	100	0,2	20
КТ 3	100	0,3	30
Итого:	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 1-5.

Доклад.

Тематика докладов:

1.Динамика и структура киберпреступности на современном этапе.

2.Международный опыт борьбы с киберпреступностью.

3. Особенности доктринального подхода к обеспечению информационной безопасности Российской Федерации.

Общая характеристика «Стратегии развития информационного общества в

Российской Федерации».

4. Проблемные вопросы квалификации хищений, совершаемых с использованием сети Интернет.

5. Особенности уголовной ответственности за хищения, совершаемые с использованием сети Интернет в зарубежных странах.

6. Особенности уголовной ответственности за совершение преступлений в сфере компьютерной информации.

7. Особенности назначения и производства судебных экспертиз по уголовным делам о преступлениях в сфере компьютерной информации.

8. Особенности назначения и производства судебных экспертиз по уголовным делам о хищениях, совершаемых с использованием сети Интернет.

Методические рекомендации по подготовке доклада.

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

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

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

Критерии оценивания доклада:

Критерии оценки	Диапазон баллов	Описание критерия
Содержание и раскрытие темы	0-20	Детальное, последовательное описание всех этапов с конкретными примерами
Грамотность изложения	0-20	Соблюдены все правила грамматики, орфографии и пунктуации
Стилистика	0-20	Единый стиль изложения, точные формулировки, уместное использование терминов, лаконичность
Логика изложения	0-20	Чёткая последовательность изложения, логические связи между частями текста,

		аргументы подтверждают выводы
Оригинальность	0-20	Уникальный подход к теме, нестандартные решения, инновационные идеи, собственная позиция автора
Итого максимально:	100	

КТ – 2.
Тема 1 - 5.
Устный опрос:
Вопросы для опроса:

№ п.п.	Содержание вопроса
1.	Понятие и содержание национальной безопасности.
2.	Понятие и содержание кибербезопасности.
3.	Характеристика объективных признаков хищений, совершаемых с использованием сети Интернет.
4.	Понятие и криминалистическая характеристика преступлений сфере компьютерной информации.
5.	Понятие и криминалистическая характеристика хищений, совершаемых с использованием сети Интернет.
6.	Особенности планирования расследования хищений, совершаемых с использованием сети Интернет.
7.	Особенности тактики производства отдельных следственных действий при расследовании хищений, совершаемых с использованием сети Интернет.

Критерии оценивания опроса:

Диапазон баллов	Описание критерия
85-100	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.
65-84	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.

55-64	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
0-54	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

КТ – 3.

Тема 1-5.

Тестирование

1. Информационная безопасность это:
- осуществление взаимоувязанных мер по предотвращению угроз
- защита от случайных или преднамеренных воздействий
- состояние защищенности информации и поддерживающей инфраструктуры
- комплекс мероприятий, направленных на обеспечение защищенности информации

2. Защита информации это:
- осуществление взаимоувязанных мер по предотвращению угроз
- защита от случайных или преднамеренных воздействий
- состояние защищенности информации и поддерживающей инфраструктуры
- комплекс мероприятий, направленных на обеспечение защищенности информации

3. Обеспечение информационной безопасности это:
- осуществление взаимоувязанных мер по предотвращению угроз
- защита от случайных или преднамеренных воздействий
- состояние защищенности информации и поддерживающей инфраструктуры
- комплекс мероприятий, направленных на обеспечение защищенности информации

4. Защита информации:
- направлена на реализацию средств обеспечения информационной безопасности
- направлена на обеспечение достоверности информации
- состояние защищенности информации и поддерживающей инфраструктуры
- направлена на обеспечение целостности конфиденциальности и доступности информации

5. Система официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере - это:
- доктрина информационной безопасности
- стратегия национальной безопасности
- комплекс мер по обеспечению национальной безопасности

6. Где дано определение информационной безопасности состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз
- доктрина информационной безопасности
- стратегия национальной безопасности
- Закон «Об информации…»

7. Совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам РФ в информационной сфере
- угроза информационной безопасности
- обеспечение информационной безопасности
- информационная безопасность

- защита информации

8. Какие виды угроз информационной безопасности НЕ выделены в Доктрине информационной безопасности РФ

- наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях
- оказание информационно-психологического воздействия, направленного на дестабилизацию ситуации в различных регионах мира
- использование механизмов информационного воздействия террористическими и экстремистскими организациями
- компьютерная преступность
- угрозы экономической системе государства

9. Источники угроз информационной безопасности Российской Федерации делятся на:

- внешние и внутренние
- абсолютные и относительные
- политические и экономические
- социальные и конституционные

10. Защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях есть стратегическая цель

- в области обороны страны
- в области государственной и общественной безопасности;
- в экономической сфере;
- в области науки, технологий и образования;

11. Рост компьютерных атак на объекты критической информационной инфраструктуры, и усиление разведывательной деятельности иностранных государств в отношении РФ есть стратегическая цель

- в области обороны страны
- в области государственной и общественной безопасности;
- в экономической сфере;
- в области науки, технологий и образования;

12. Нарастание угроз применения информационных технологий в целях нанесения ущерба суверенитету, политической и социальной стабильности РФ есть стратегическая цель

- в области обороны страны
- в области государственной и общественной безопасности;
- в экономической сфере;
- в области науки, технологий и образования;

13. Защита суверенитета РФ в информационном пространстве посредством осуществления самостоятельной и независимой политики

- есть стратегическая цель РФ в экономической сфере
- есть стратегическая цель РФ в области стратегической стабильности
- угроза ИБ в области государственной и общественной безопасности
- одно из основных направлений обеспечения ИБ

14. Одно из основных направлений обеспечения ИБ в области стратегической стабильности

- развитие национальной системы управления российским сегментом сети "Интернет"
- создание перспективных информационных технологий

- ликвидация зависимости отечественной промышленности от зарубежных информационных технологий
- противодействие использованию ИТ для пропаганды экстремистской идеологии

15. Одно из основных направлений обеспечения ИБ в области науки, технологий, образования
- развитие национальной системы управления российским сегментом сети "Интернет"
- создание перспективных информационных технологий
- ликвидация зависимости отечественной промышленности от зарубежных информационных технологий
- противодействие использованию ИТ для пропаганды экстремистской идеологии

16. Одно из основных направлений обеспечения ИБ в области государственной и общественной безопасности
- участие в формировании системы международной ИБ
- создание перспективных информационных технологий
- ликвидация зависимости отечественной промышленности от зарубежных информационных технологий
- противодействие использованию ИТ для пропаганды экстремистской идеологии

17. Государственная система защиты информации состоит из:
- лицензирования деятельности и сертификации продукции
- администрирования и ограничения доступа к информации
- лицензирования деятельности и ограничения доступа к информации

18. Меры обеспечения информационной безопасности делятся на:
- организационные и программно-технические
- лицензионные и разрешительные
- государственные и индивидуальные

19. К организационным мерам защиты информации НЕ относятся:
- нормативно-правовые
- морально-этические
- процедурные меры
- программно-технические

20. Правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, регламентируют ... меры.
- нормативно-правовые
- организационные (административные)
- физические
- технические

21. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации:
- политика информационной безопасности
- практика информационной безопасности
- теория информационной безопасности

22. Какой акт регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий и обеспечении защиты информации.
- ФЗ "Об информации, информационных технологиях и защите информации" от 27.06.2006 г. № 149-ФЗ.
- ФЗ "Об электронной подписи" от 06.04.2011 г. № 63-ФЗ.

- «Положение о методах и способах защиты информации в информационных системах персональных данных»

23. Защита информации направлена на:

- защиту информации в информационных системах
- защиту конституционных прав граждан
- обеспечение защиты информации от неправомерного доступа

24. К преступлениям в сфере компьютерной информации относится:

- неправомерный доступ к охраняемой компьютерной информации
- нарушение правил защиты информации
- нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах
- нарушение правил работы с архивными документами

25. Согласно ч. 1 ст. 272 УК РФ наказывается неправомерный доступ к охраняемой законом компьютерной информации.

- если это деяние причинило крупный ущерб или совершено из корыстной заинтересованности;
- если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации;
- если это деяние совершено лицом с использованием своего служебного положения;
- если это деяние повлекло тяжкие последствия или создало угрозу их наступления;
- если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации и причинило крупный ущерб.

26. Крупным ущербом в статьях главы 28 УК РФ признается ущерб, сумма которого превышает …

- двести пятьдесят тысяч рублей;
- один миллион рублей;
- полтора миллиона рублей;
- шесть миллионов рублей;
- среди перечисленных нет правильного ответа.

27. По ч. 1 ст. 273 УК РФ наказываются создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации …

- совершенные группой лиц по предварительному сговору или организованной группой;
- совершенные лицом с использованием своего служебного положения;
- если они повлекли тяжкие последствия или создали угрозу их наступления;
- среди перечисленных нет правильного ответа.

28. Согласно ч. 1 ст. 274 УК РФ уголовно-наказуемым является нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям.

- причинившее крупный ущерб;
- повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации;
- повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб;

- повлекшее тяжкие последствия или создавшее угрозу их наступления.

Критерии оценивания тестовых заданий:

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

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий (*при необходимости*).

Для ответа на вопросы студенту разрешается использование Уголовно-процессуального кодекса РФ, Уголовного кодекса РФ.

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

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

6.2. Типовые оценочные материалы промежуточной аттестации

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

Тема 1. Киберпреступления как угроза обеспечения национальной безопасности ПКс-2.1

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Понятие и содержание национальной безопасности.
2.	Виды угроз национальной безопасности.
3.	Криминологическая характеристика киберпреступности.

1.2. Контрольные задания .

Задание 1.

Студент технического вуза Иванченко во время занятий по информатике подключилс я к сети «Интернет» и регулярно получал в течение семестра материалы разного содержан

ия, в том числе и сексуального характера. В конце семестра в институт поступил запрос о работе в «Интернет» и пришёл чек на оплату 105 часов пребывания в сети «Интернет». Ру ководство института поставило вопрос о привлечении Иванченко к уголовной и гражданс кой ответственности.

Задание

1. Дайте правовую оценку действиям студента Иванченко.

2. Подлежит ли он уголовной ответственности? Обоснуйте ответ со ссылкой на УК Р Ф.

3. Может ли наступить гражданская ответственность? Если да, то в каком порядке?

2. Задания комбинированного типа:

1.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Информационная безопасность это: а)осуществление взаимоувязанных мер по предотвращению угроз б)защита от случайных или преднамеренных воздействий		
2.	Защита информации это: а)осуществление взаимоувязанных мер по предотвращению угроз б)защита от случайных или преднамеренных воздействий		

3. Задания закрытого типа.

3.1. Тестовые задания.

1. Обеспечение информационной безопасности это:
   - осуществление взаимоувязанных мер по предотвращению угроз
   - защита от случайных или преднамеренных воздействий
   - состояние защищенности информации и поддерживающей инфраструктуры
   - комплекс мероприятий, направленных на обеспечение защищенности информации

2. Защита информации:
   - направлена на реализацию средств обеспечения информационной безопасности
   - направлена на обеспечение достоверности информации
   - состояние защищенности информации и поддерживающей инфраструктуры
   - направлена на обеспечение целостности конфиденциальности и доступности информации

Тема 2. Нормативно-правовое обеспечение кибербезопасности ПКс-2.1

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Понятие и содержание кибербезопасности.
2.	Информация и информационная безопасность: понятие и характеристика.
3.	Основные направления политики государства в сфере кибербезопасности.

1.2. Контрольные задания .

Задание 1.

Аспирант университета Хохлов (23 года) занимался исследовательской работой по компьютерной «вирусологии». Целью работы было выяснение масштаба глобальной сетевой инфраструктуры. В результате ошибки в механизме размножения вирусы («сетевые черви») проникли в университетскую компьютерную сеть и уничтожили информацию, содержащуюся в компьютерах факультетов и подразделений. В результате были полностью уничтожены: списки сотрудников университета; расчёты бухгалтерии по зарплате; материалы научно-исследовательской работы, включая две кандидатские и одну докторскую диссертации.

Задания:

Решите вопрос о правомерности действий Хохлова.

Квалифицируйте деяние с точки зрения уголовного законодательства (укажите статью УК РФ).

В чём заключается субъективная сторона преступлений в сфере компьютерной информации?

2. Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Система официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере - это: а)доктрина информационной безопасности стратегия национальной безопасности б)комплекс мер по обеспечению национальной безопасности		
2.	Где дано определение информационной безопасности состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз		

	а)доктрина информационной безопасности б)стратегия национальной безопасности Закон «Об информации…»		

3. Задания закрытого типа.

3.1. Тестовые задания.

1. Совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам РФ в информационной сфере

- угроза информационной безопасности
- обеспечение информационной безопасности
- информационная безопасность
- защита информации

2. Какие виды угроз информационной безопасности НЕ выделены в Доктрине информационной безопасности РФ

- наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях
- оказание информационно-психологического воздействия, направленного на дестабилизацию ситуации в различных регионах мира
- использование механизмов информационного воздействия террористическими и экстремистскими организациями
- компьютерная преступность
- угрозы экономической системе государства

Тема 3. Уголовно-правовая характеристика преступлений, совершаемых в киберпространстве ПКс-2.1

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Характеристика объективных признаков хищений, совершаемых с использованием сети Интернет.
2.	Характеристика субъективных признаков хищений, совершаемых с использованием сети Интернет.
3.	Понятие и уголовно-правовая характеристика отдельных видов преступлений в сфере компьютерной информации.

1.2. Контрольные задания.

Задание 1.

Савченко осуществлял рассылку подложных электронных писем с целью завладения персональной информацией клиентов «Ситибанка». Рассылка представляла собой электро нное письмо с сообщением о переводе 100 долларов США на личный счёт клиента и содер

жала просьбу зайти в систему интернет-банкинга «CitibankOnline» для подтверждения пер евода. При переходе по ссылке пользователь попадал на сайт, созданный Савченко и очен ь похожий на стартовый экран «CitibankOnline». Десять человек ввели номер кредитной ка рты и PIN-код. Воспользовавшись полученной информацией, Савченко похитил денежные средства Павлова и Костенко (15 и 20 тысяч долларов соответственно).

Задания:

Квалифицируйте содеянное Савченко. Укажите статьи УК РФ.

Какие меры профилактики подобных преступлений можно предложить банку и клиен там?

Опишите алгоритм действий потерпевшего при обнаружении факта хищения средств таким способом.

1. Задания комбинированного типа:

2.1 Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Какие виды угроз информационной безопасности НЕ выделены в Доктрине информационной безопасности РФ а)наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях б)оказание информационно-психологического воздействия, направленного на дестабилизацию ситуации в различных регионах мира		
2.	Источники угроз информационной безопасности Российской Федерации делятся на: а)внешние и внутренние б)абсолютные и относительные		

3. Задания закрытого типа.

3.1. Тестовые задания.

1. Защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях есть стратегическая цель

- в области обороны страны
- в области государственной и общественной безопасности;
- в экономической сфере;

- в области науки, технологий и образования;

2. Рост компьютерных атак на объекты критической информационной инфраструктуры, и усиление разведывательной деятельности иностранных государств в отношении РФ есть стратегическая цель

- в области обороны страны
- в области государственной и общественной безопасности;
- в экономической сфере;
- в области науки, технологий и образования;

Тема 4. Расследование отдельных видов преступлений в сфере компьютерной информации ПКс-2.1

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Понятие и криминалистическая характеристика преступлений сфере компьютерной информации.
2.	Особенности планирования расследования преступлений сфере компьютерной информации
3.	Особенности тактики производства отдельных следственных действий при расследовании преступлений сфере компьютерной информации.

1.2. Контрольные задания .

Задача 1

Гуляшов, студент факультета вычислительной математики, организовывал сетевые атаки, заключающиеся в получении обманным путём доступа в сеть посредством имитации соединения. Таким образом он получил доступ к информации о счетах пользователей интернета и номерам некоторых кредитных карт и PIN-кодов. Полученную информацию Гуляшов передавал Сорокиной за вознаграждение, которая использовала её для хищения денежных средств.

Задания:

Что такое фишинг, спуфинг и фарминг?

Признаки какого явления усматриваются в деянии Гуляшова?

Квалифицируйте действия Гуляшова и Сорокиной. Укажите статьи УК РФ и обоснуйте квалификацию.

2.Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением		

	информационных технологий в военно-политических целях есть стратегическая цель а)в области обороны страны б)в области государственной и общественной безопасности;		
2.	Рост компьютерных атак на объекты критической информационной инфраструктуры, и усиление разведывательной деятельности иностранных государств в отношении РФ есть стратегическая цель а)в области обороны страны б)в области государственной и общественной безопасности;		

Задания закрытого типа.

3.1. Тестовые задания.

1. Нарастание угроз применения информационных технологий в целях нанесения ущерба суверенитету, политической и социальной стабильности РФ есть стратегическая цель

- в области обороны страны
- в области государственной и общественной безопасности;
- в экономической сфере;
- в области науки, технологий и образования;

2. Защита суверенитета РФ в информационном пространстве посредством осуществления самостоятельной и независимой политики

- есть стратегическая цель РФ в экономической сфере
- есть стратегическая цель РФ в области стратегической стабильности
- угроза ИБ в области государственной и общественной безопасности
- одно из основных направлений обеспечения ИБ

Тема 5. Расследование хищений, совершаемых с использованием сети Интернет ПКс-2.1

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Понятие и криминалистическая характеристика хищений, совершаемых с использованием сети Интернет.
2.	Особенности планирования расследования хищений, совершаемых с использованием сети Интернет.
3.	Особенности тактики производства отдельных следственных действий при расследовании хищений, совершаемых с использованием сети Интернет.

1.2. Контрольные задания .

Задача №1

Оператор ЭВМ одного из государственных учреждений Утевский, используя многочисленные дискеты с информацией, получаемые от сотрудников других организаций, не всегда проверял их на наличие «вирусов», доверяясь заверениям поставщиков о том, что «вирусов» нет. В результате в компьютер Утевского, а затем и в компьютерную сеть учреждения попал комбинированный вирус, что привело к утрате информации, содержащей государственную тайну, и поставило под угрозу срыва запуск одного из космических объектов.

Задания:

Дайте юридический анализ действий Утевского.

Что следует понимать под тяжкими последствиями при нарушении правил эксплуатации информационно-телекоммуникационных сетей (ст. 274 УК РФ)?

Какие меры информационной безопасности должны быть реализованы в государственных

2.Задания комбинированного типа:

1.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Одно из основных направлений обеспечения ИБ в области стратегической стабильности а)развитие национальной системы управления российским сегментом сети "Интернет" б)создание перспективных информационных технологий		
2.	Одно из основных направлений обеспечения ИБ в области науки, технологий, образования а)развитие национальной системы управления российским сегментом сети "Интернет" б)создание перспективных информационных технологий		

3.Задания закрытого типа.

3.1. Тестовые задания.

1. Одно из основных направлений обеспечения ИБ в области науки, технологий, образования

- развитие национальной системы управления российским сегментом сети "Интернет"
- создание перспективных информационных технологий
- ликвидация зависимости отечественной промышленности от зарубежных информационных технологий
- противодействие использованию ИТ для пропаганды экстремистской идеологии

2. Одно из основных направлений обеспечения ИБ в области государственной и общественной безопасности

- участие в формировании системы международной ИБ
- создание перспективных информационных технологий
- ликвидация зависимости отечественной промышленности от зарубежных информационных технологий
- противодействие использованию ИТ для пропаганды экстремистской идеологии

6.3. Критерии и шкала оценивания на основе БРС.

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал 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, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными	0-19

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 Уголовно-процессуального кодекса РФ, Уголовного кодекса РФ.

7. Методические материалы по освоению дисциплины

Подготовка к лекциям.

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его нужно положить рабочие программы изучаемых в семестре дисциплин. Каждому обучающемуся следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Самостоятельная работа на лекции.

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

Подготовка к практическим занятиям.

Подготовку к каждому практическому занятию каждый обучающийся должен начать

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

Структура практического занятия:

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

1. Обсуждение теоретических вопросов, определенных программой дисциплины.
2. Доклад и/ или выступление с презентациями по проблеме практического занятия.
3. Обсуждение выступлений по теме – дискуссия.
4. Выполнение практического задания с последующим разбором полученных результатов или обсуждение практического задания, выполненного дома, если это предусмотрено программой.
5. Подведение итогов занятия.

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

Работа с литературными источниками.

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более

глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Вопросы для самостоятельной подготовки к лекционным и практическим занятиям:

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий: практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. — Москва: Ай Пи Ар Медиа, 2025. — 263 с. — ISBN 978-5-4497-4085-4. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/147936.html

2. Деятельность органов внутренних дел по профилактике IT-преступлений против собственности: учебное пособие / М. Г. Жилкин, В. В. Качалов, Ю. В. Никонорова [и др.]. — Москва: Ай Пи Ар Медиа, 2025. — 97 с. — ISBN 978-5-4497-4332-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/150458.html

8.2. Дополнительная литература

1. *Эксархопуло, А. А.* Криминалистика в схемах: учебное пособие для вузов / А. А. Эксархопуло. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2021. — 422 с. — (Высшее образование). — ISBN 978-5-534-08242-5. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/470868

2. *Эксархопуло, А. А.* Криминалистика: история и перспективы развития: монография / А. А. Эксархопуло, И. А. Макаренко, Р. И. Зайнуллин. — Москва: Издательство Юрайт, 2021. — 167 с. — (Актуальные монографии). — ISBN 978-5-534-09497-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475128.

3. Введение в криминалистику. Организация раскрытия и расследования преступлений : учебное пособие для вузов / А. Г. Филиппов [и др.]; под общей редакцией А. Г. Филиппова. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2021. — 149 с. — (Высшее образование). — ISBN 978-5-534-04899-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/470232.

8.3. Нормативные правовые документы и иная правовая информация

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ) // Собрание законодательства РФ. 2014. N 15. Ст. 1691.

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 01.07.2021)// "Российская газета", N 249, 22.12.2001.

3. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 01.07.2021) (с изм. и доп., вступ. в силу с 22.08.2021)// "Собрание законодательства РФ", 17.06.1996, N 25, ст. 2954.

4. Федеральный закон от 07.02.2011 N 3-ФЗ (ред. от 11.06.2021) "О полиции"// "Российская газета", N 25, 08.02.2011.

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

6. 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».

7. 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. http://www.gov.ru/main/page7.html Федеральное собрание РФ
4. http://www.duma.gov.ru/ Государственная Дума ФС РФ
5. www.vsrf.ru Верховный Суд Российской Федерации
6. www.ksrf.ru Конституционный Суд Российской Федерации
7. 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».