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

Волгоградский институт управления – филиал РАНХиГС

Юридический факультет

Кафедра уголовного права, уголовного процесса и криминалистики

УТВЕРЖДЕНА
учёным советом
Волгоградского института управления –
филиала РАНХиГС
Протокол №13 от 27.04.2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДЭ.05.01 Уголовно-правовые аспекты кибербезопасности

*(*индекс, наименование дисциплины в соответствии с учебным планом*)*

40.05.01 Правовое обеспечение национальной безопасности

(код, наименование направления подготовки /специальности)

Уголовно-правовая

(наименование образовательной программы)

Очная, заочная

(форма (формы) обучения)

Год набора – 2026 г.

Волгоград, 2026 г.

Автор-составитель РПД:

канд. юрид. наук, доцент кафедры уголовного права, уголовного процесса и криминалистики С.С. Симонова

И.о. заведующего кафедрой:

Симонова С.С. канд. юрид. наук, и.о. заведующего кафедрой уголовного права, уголовного процесса и криминалистики

Рабочая программа дисциплины Б1.В.ДЭ.05.01 Уголовно-правовые аспекты кибербезопасности одобрена на заседании кафедры уголовного права, уголовного процесса и криминалистики.
Протокол от 16 марта 2026 года № 7

СОДЕРЖАНИЕ

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

1.1. Осваиваемые компетенции

Дисциплина **Б1.В.ДЭ.05.01 Уголовно-правовые аспекты кибербезопасности** обеспечивает формирование у обучающихся следующих общепрофессиональных и профессиональных компетенций:

ОТФ/ТФ и реквизиты ПС *(при наличии)***	**Код компетенции ****	**Наименование компетенции ****	**Код индикатора достижения компетенций ****	**Наименование индикатора достижения компетенций ****	**Образовательный результат ****
Образовательный стандарт по специальности высшего образования 40.05.01 Правовое обеспечение национальной безопасности (утв. Приказом Академии от 7 сентября 2023 г. № 01-24595 (в ред. Приказов Академии от 15 августа 2024 г. № 01-13917, от 19 августа 2025 г. № 01-13018)	ПКс-2	Способен принимать законные и обоснованные решения в сфере осуществления юридической деятельности на основе профессионального правосознания, правового мышления и правовой культуры	ПКс-2.1	Способен принимать законные и обоснованные решения в сфере осуществления юридической деятельности на основе развитого правового сознания	ПКс-2.1. З-1. Знает содержание, основные принципы и условия формирования профессионального правосознания, правового мышления и правовой культуры
					ПКс-2.1. У-1. Умеет аргументировать законность и обоснованность принятого решения при осуществлении юридической деятельности с учётом высокого уровня профессионального правосознания, правового мышления и правовой культуры
					ПКс-2.1. Н-1. Владеет навыками принятия законного и обоснованного решения в сфере осуществления юридической деятельности с учётом высокого уровня профессионального правосознания, правового мышления и правовой культуры
			ПКс-2.2	ПКс-2.2. Способен принимать законные и обоснованные	ПКс-2.2. З-1. Знает содержание, основные принципы и условия принятия законных и

				решения в сфере осуществления юридической деятельности на основе развитого правового мышления	обоснованных решений в сфере осуществления юридической деятельности на основе развитого правового мышления
					ПКс-2.2. У-1. Умеет применять основные принципы и законы развитого правового мышления в процессе принятия законного и обоснованного решения при осуществлении юридической деятельности
					ПКс-2.2. Н-1. Владеет навыками принятия законного и обоснованного решения в сфере осуществления юридической деятельности на основе развитого правового мышления
			ПКс-2.3.	Способен принимать законные и обоснованные решения в сфере осуществления юридической деятельности на основе развитой правовой культуры	ПКс-2.3. З-1. Знает содержание, основные принципы и условия формирования правовой культуры юриста
					ПКс-2.3. У-1. Умеет организовывать порядок принятия законного и обоснованного решения в сфере осуществления юридической деятельности с учётом высокого уровня правовой культуры юриста
					ПКс-2.3. Н-1. Владеет навыками принятия законного и обоснованного решения в сфере осуществления юридической деятельности на основе развитой правовой культуры юриста

2. Объем и место дисциплины в структуре образовательной программы

Учебная дисциплина Б1.В.ДЭ.05.01 «Уголовно-правовые аспекты кибербезопасности» относится к блоку вариативной части дисциплин. В соответствии с учебным планом, по очной форме обучения дисциплина осваивается на 4 курсе в 7 семестре (зачет), по заочной форме обучения дисциплина осваивается на 5 курсе, общая трудоемкость дисциплины в зачетных единицах составляет 72 часа (2 ЗЕТ).

По очной форме обучения количество академических часов, выделенных на контактную работу с преподавателем - 40 часов, из них 20 часов лекционных занятий, 16 часа практических занятий (из них 4 часа с использованием ДОТ), 32 часа выделено на самостоятельную работу обучающихся и 4 часа на контроль.

По заочной форме обучения количество академических часов, выделенных на контактную работу с преподавателем - 8 часов, из них 4 часов лекционных занятий, 4 часов практических занятий, 60 часов выделено на самостоятельную работу обучающихся и 4 часа на контроль. Форма промежуточной аттестации в соответствии с учебным планом – зачет.

Учебная дисциплина Б1.В.ДЭ.05.01 Уголовно-правовые аспекты кибербезопасности реализуется после изучения дисциплин Правоохранительные органы, «Уголовно-процессуальное право (Уголовный процесс)», Уголовное право.

Освоение дисциплины опирается на минимально необходимый объем теоретических знаний и навыков, полученные при изучении таких дисциплин, как «Теория права и государства», «Конституционное право», «Уголовное право».

Знания, полученные в ходе изучения дисциплины Б1.В.08 «Уголовно-правовые аспекты кибербезопасности», могут быть полезны при изучении таких дисциплин как «Прокурорский надзор», «Правовые основы стратегического планирования в сфере обеспечения национальной безопасности», ряда других дисциплин, предусмотренных учебным планом подготовки специалистов.

Учебная дисциплина Б1.В.ДЭ.05.01 «Уголовно-правовые аспекты кибербезопасности» реализуется после изучения дисциплины Уголовно-процессуальное право (Уголовный процесс), Уголовное право, Криминология, Основы национальной безопасности; одновременно с изучением дисциплин Международное сотрудничество в борьбе с организованной преступностью, Учение о наказании.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Каттэк	Контроль	СРкр	СРэк	СР	
			Л/ДОТ	ВЛ	ЛР	ПЗ/ДОТ									
Тема 1	Понятие кибербезопасности. Основные риски и угрозы в области кибербезопасности	12	4			2								6	О, Р
Тема 2	Понятие и виды киберпреступности	14	4			4								6	О, Р
Тема 3	Преступления в сфере компьютерной информации	16	4			4/2								8	О, Р, Т

Тема 4	Киберпреступления экономического характера	14	4			4								6	О, Р
Тема 5	Противодействие киберпреступности	12	4			2/2								6	Т
Промежуточная аттестация											4				Зачет
Итого		**72**	**20**			**16/4**					**4**			**32**	

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;

Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения ;

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.

***** *электронные часы*

Примечание: формы текущего контроля успеваемости: опрос (О), тестирование (Т), реферат (Р), ситуационная задача (СЗ), решение задач (З)

Заочная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Каттэк	Контроль	СРкр	СРэк	СР	
			Л/ДОТ	ВЛ	ЛР	ПЗ/ДОТ									
Тема 1	Понятие кибербезопасности. Основные риски и угрозы в области кибербезопасности	14	1			1								12	О, Т
Тема 2	Понятие и виды киберпреступности	13	1											12	О, Т
Тема 3	Преступления в сфере компьютерной информации	14	1			1								12	О, Р
Тема 4	Киберпреступления экономического характера	14	1			1								12	Т
Тема 5	Противодействие киберпреступности	13				1								12	Т
Промежуточная аттестация											4				Зачет
Итого		**72**	**4**			**4**					**4**			**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;

Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения ;

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.

Примечание: формы текущего контроля успеваемости: опрос (О), тестирование (Т), реферат (Р), ситуационная задача (СЗ), решение задач (З)

3.2 Содержание дисциплины

Тема 1. Понятие кибербезопасности. Основные риски и угрозы в области кибербезопасности. ПКс-2.1

Понятие кибербезопасности. Соотношение кибербезопасности и информационной безопасности. Области кибербезопасности. Безопасность сетей. Безопасность приложений. Безопасность информации. Операционная безопасность.

Нормативно-правовое регулирование кибербезопасности. Международное правовое регулирование кибербезопасности. Конвенция Совета Европы о компьютерных преступлениях. Законодательство Российской Федерации в сфере кибербезопасности.

Основные риски кибербезопасности. Современные угрозы в области кибербезопасности.

Тема 2. Понятие и виды киберпреступности. ПКс-2.2

Понятие киберпреступности. Соотношение киберпреступности и компьютерных преступлений. «Беловоротничковая» преступность. Виды киберпреступлений. Противоправные деяния против конфиденциальности, доступности и целостности компьютерных систем и данных (несанкционированное вмешательство). Действия, связанные с компьютерами (подлог, мошенничество). Противоправные поступки, связанные с контентом (содержанием) информации. Правонарушения в сфере авторских и смежных прав.

Основные современные уголовно-правовые риски в киберсреде. Промышленный шпионаж и иные посягательства на охраняемые законом тайны и персональные данные (ст. 137-138 УК РФ). Киберпреступления, посягающие на личные права и государственные интересы.

Тема 3. Преступления в сфере компьютерной информации. ПКс-2.1

Понятие компьютерных преступлений. Характеристика составов компьютерных преступлений. Киберпреступления, посягающие на личные права и государственные интересы. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272.1 УК РФ).

Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ).

Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции (ст. 274.3 УК РФ). Организация деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации (ст. 274.4 УК РФ). Организация деятельности по передаче информации, необходимой для регистрации и (или) авторизации пользователя сети "Интернет" для получения доступа к функциональным возможностям информационного ресурса (ст. 274.5 УК РФ).

Тема 4. Киберпреступления экономического характера. ПКс-2.3

Основные черты современно уголовного законодательства в сфере охраны экономических отношений. Уголовная политика в сфере охраны экономических отношений.

Характеристика экономических преступлений, совершаемых в киберпространстве. Классификация экономических преступлений. Экономическое мошенничество. Преступления в сфере предпринимательства. Кредитные преступления. Преступления в сфере конкуренции. Преступления на рынке ценных бумаг и финансовые преступления. Преступления в сфере банкротства. Служебные экономические преступления.

Преступления, совершаемые с использованием криптовалют и блокчейн технологий. Криптовалюта как признак состава преступления. Криптовалюта как предмет хищения. Неправомерное использование инсайдерской информации. Манипулирование рынком.

Тема 5. Противодействие киберпреступности. ПКс-2.1

Нормативно-правовая основа противодействия киберпреступности. Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий. Противодействие распространению информации противоправного характера в сети "Интернет". Субъекты противодействия киберпреступности. Кибердружины.

Виктимологическая профилактика киберпреступлений. Реализация мер, направленных на повышение уровня цифровой и финансовой грамотности граждан. Меры по снижению риска от посягательств в киберсфере. Организация и проведение мероприятий по предупреждению вовлечения несовершеннолетних в противоправную деятельность в информационно-коммуникационной сфере.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.ДЭ.05.01 «Уголовно-правовые аспекты кибербезопасности» входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляет фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи»

правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

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

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

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

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

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

4.4. Типы заданий, сценарии выполнения, критерии оценивания

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

установление 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 используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Тестирование, реферат, опрос, контрольная работа.

№ п/п	Наименование тем (разделов)	Методы текущего контроля успеваемости
Тема 1	Понятие кибербезопасности. Основные риски и угрозы в области кибербезопасности	*Устный опрос*
Тема 2	Понятие и виды киберпреступности	*Устный опрос*
Тема 3	Преступления в сфере компьютерной информации	*Устный опрос, тестирование*
Тема 4	Киберпреступления экономического характера	*Устный опрос*
Тема 5	Противодействие киберпреступности	*Устный опрос, тестирование, контрольная работа*

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

Тема 1. Понятие кибербезопасности. Основные риски и угрозы в области кибербезопасности. ПКс-2.1

Вопросы для проведения опроса на занятиях

1.Понятие кибербезопасности. Соотношение кибербезопасности и информационной безопасности.

2. Области кибербезопасности. Безопасность сетей. Безопасность приложений. Безопасность информации. Операционная безопасность.

3. Международно-правовое регулирование кибербезопасности. Конвенция Совета Европы о компьютерных преступлениях.

4. Законодательство Российской Федерации в сфере кибербезопасности.

5. Основные риски кибербезопасности. Современные угрозы в области кибербезопасности.

Тестовые задания:

Тест 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое кибербезопасность?

1. Защита только компьютерных сетей.
2. Защита информации и информационных систем от угроз.
3. Использование антивирусов.
4. Хранение данных на флешке.

Какой из перечисленных факторов не относится к основным угрозам кибербезопасности?

1. Вирусы и вредоносное ПО.
2. Социальная инженерия.
3. Физическая кража компьютера.
4. Сильный пароль.

Тест 2. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое социальная инженерия в контексте кибербезопасности?

1. Метод взлома с помощью технических средств.
2. Манипуляция людьми с целью получения конфиденциальной информации.
3. Разработка антивирусных программ.
4. Создание защищённых сетей.

Какой из перечисленных принципов является основой кибербезопасности?

1. Открытость всех данных.
2. Конфиденциальность, целостность и доступность информации.
3. Использование только бесплатных программ.
4. Хранение всех данных на одном устройстве.

Тема 2. Понятие и виды киберпреступности. ПКс-2.2

Вопросы для проведения опроса на занятиях

1. Понятие киберпреступности. Соотношение киберпреступности и компьютерных преступлений.

2. Виды киберпреступлений. Противоправные деяния против конфиденциальности, доступности и целостности компьютерных систем и данных (несанкционированное вмешательство).

3. Действия, связанные с компьютерами (подлог, мошенничество). Противоправные поступки, связанные с контентом (содержанием) информации. Правонарушения в сфере авторских и смежных прав.

4. Основные современные уголовно-правовые риски в киберсреде. Промышленный шпионаж и иные посягательства на охраняемые законом тайны и персональные данные (ст. 137-138 УК РФ).

5. Киберпреступления, посягающие на личные права и государственные интересы.

Тестовые задания:

Тест 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое киберпреступность?

1. Любое преступление, совершённое с использованием компьютерных технологий или в сети Интернет.

2. Преступления, связанные только с кражей компьютеров.

3. Нарушение правил пользования компьютером.

4. Преступления, совершённые только в отношении государственных информационных систем.

Чем киберпреступность отличается от компьютерных преступлений?

1. Киберпреступность — это более широкое понятие, включающее преступления в цифровой среде, а компьютерные преступления — только те, где компьютер выступает объектом или инструментом.

2. Это синонимы.

3. Компьютерные преступления — это только взлом паролей.

4. Киберпреступность — это преступления против личности, а компьютерные — против государства.

Тест 2. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Какой из перечисленных примеров относится к киберпреступности?

1. Кража ноутбука из офиса.

2. Фишинг с целью хищения данных банковских карт.

3. Порча имущества в общественном месте.

4. Нарушение правил дорожного движения.

Что такое компьютерное преступление?

1. Преступление, совершённое исключительно с помощью компьютера или направленное на компьютерные системы.

2. Любое преступление, совершённое в интернете.

3. Преступление, связанное с нарушением авторских прав на программное обеспечение.

4. Преступление, совершённое только против государственных структур.

Тема 3. Преступления в сфере компьютерной информации. ПКс-2.1

Вопросы для проведения опроса на занятиях

1. Понятие компьютерных преступлений. Характеристика составов компьютерных преступлений.
2. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).
3. Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272.1 УК РФ).
4. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).
5. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).
6. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).
7. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ).
6. Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции (ст. 274.3 УК РФ).
7. Организация деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации (ст. 274.4 УК РФ).
8. Организация деятельности по передаче информации, необходимой для регистрации и (или) авторизации пользователя сети "Интернет" для получения доступа к функциональным возможностям информационного ресурса (ст. 274.5 УК РФ).

Тестовые задания:

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое преступление в сфере компьютерной информации?

1. Любое нарушение правил работы с компьютером.
2. Уголовно наказуемое деяние, связанное с неправомерным доступом, использованием, распространением или уничтожением компьютерной информации.
3. Кража компьютерного оборудования.
4. Нарушение авторских прав на программное обеспечение.

Какой из перечисленных примеров относится к преступлению в сфере компьютерной информации?

1. Кража системного блока из офиса.
2. Неправомерный доступ к защищённой компьютерной информации.
3. Порча имущества в общественном месте.
4. Нарушение правил дорожного движения.

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ или несколько.

Что такое неправомерный доступ к компьютерной информации?
1. Доступ к информации с разрешения владельца.
2. Доступ к информации без права на это, с нарушением установленных правил.
3. Использование компьютера в личных целях.
4. Установка антивирусной программы.

Какой вид преступления связан с созданием и распространением вредоносных программ?
1. Мошенничество.
2. Создание, использование и распространение вредоносных компьютерных программ.
3. Кража данных.
4. Нарушение авторских прав.

Тема 4. Киберпреступления экономического характера. ПКс-2.3

Вопросы для проведения опроса на занятиях

1. Основные черты современно уголовного законодательства в сфере охраны экономических отношений. Уголовная политика в сфере охраны экономических отношений.
2. Характеристика экономических преступлений, совершаемых в киберпространстве. Классификация экономических преступлений.
3. Экономическое мошенничество.
4. Преступления в сфере предпринимательства.
5. Кредитные преступления.
6. Преступления в сфере конкуренции. Преступления на рынке ценных бумаг и финансовые преступления.
7. Преступления в сфере банкротства.
8. Служебные экономические преступления.
9. Преступления, совершаемые с использованием криптовалют и блокчейн технологий.
10. Неправомерное использование инсайдерской информации. Манипулирование рынком.

Тестовые задания:

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое киберпреступления экономического характера?
1. Преступления, связанные с кражей компьютерного оборудования.

2. Преступления, направленные на хищение финансовых средств, мошенничество, незаконное получение экономической выгоды с использованием цифровых технологий.
3. Преступления, совершаемые только в отношении государственных учреждений.
4. Нарушение авторских прав на программное обеспечение.

Какой из перечисленных примеров относится к киберпреступлениям экономического характера?
1. Кража ноутбука из офиса.
2. Фишинг с целью хищения данных банковских карт.
3. Порча имущества в общественном месте.
4. Нарушение правил дорожного движения.

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое фишинг в контексте экономических киберпреступлений?

1. Вид интернет-мошенничества с целью получения доступа к финансовым данным.
2. Программа для защиты от вирусов.
3. Метод шифрования данных.
4. Способ восстановления паролей.

Что такое криптоскам?

1. Легальная торговля криптовалютой.
2. Мошенничество, связанное с криптовалютами (фальшивые биржи, ICO, кошельки).
3. Майнинг криптовалюты на своём компьютере.
4. Хранение криптовалюты в банке.

Тема 5. Противодействие киберпреступности. ПКс-2.1

Вопросы для проведения опроса на занятиях

1. Нормативно-правовая основа противодействия киберпреступности. Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий.
2. Противодействие распространению информации противоправного характера в сети "Интернет". Субъекты противодействия киберпреступности.
3. Кибердружины: понятие и функции.
4. Виктимологическая профилактика киберпреступлений. Реализация мер, направленных на повышение уровня цифровой и финансовой грамотности граждан.
5. Меры по снижению риска от посягательств в киберсфере.
6. Организация и проведение мероприятий по предупреждению вовлечения несовершеннолетних в противоправную деятельность в информационно-коммуникационной сфере.

Тестовые задания:

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Какой из перечисленных методов относится к техническим мерам противодействия киберпреступности?

1. Обучение сотрудников.
2. Установка и обновление антивирусного ПО, межсетевых экранов.
3. Разработка законов.
4. Проведение опросов.

Какой из перечисленных способов является организационной мерой противодействия киберпреступности?

1. Установка антивируса.
2. Разработка политики информационной безопасности, обучение персонала, контроль доступа.
3. Взлом хакерских сайтов.
4. Использование сложных паролей.

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Какой из перечисленных методов относится к превентивным мерам противодействия киберпреступности?

1. Расследование уже совершённого преступления.
2. Установка систем обнаружения вторжений и анализ уязвимостей.
3. Наказание виновных лиц.
4. Восстановление данных после атаки.

Что такое мониторинг событий информационной безопасности?

1. Просмотр фильмов о хакерах.
2. Постоянное наблюдение за действиями в системе для выявления подозрительной активности.
3. Разработка программного обеспечения.
4. Проведение праздников в офисе.

Шкала оценивания

Устный опрос

Уровень знаний, умений и навыков обучающегося при устном ответе во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критериями оценивания при проведении устного опроса является демонстрация основных теоретических положений, в рамках осваиваемой компетенции, умение применять полученные знания на практике, овладение навыками анализа и систематизации криминалистически значимой информации.

При оценивании результатов устного опроса используется следующая шкала оценок:

100% - 85%	Учащийся демонстрирует совершенное знание основных теоретических положений, в рамках осваиваемой компетенции, умеет применять полученные знания на практике, владеет навыками анализа и систематизации криминалистически значимой информации и норм уголовно-исполнительного права
84% - 65%	Учащийся демонстрирует знание большей части основных теоретических положений, в рамках осваиваемой компетенции, умеет применять полученные знания на практике в отдельных сферах профессиональной деятельности, владеет основными навыками анализа и систематизации криминалистически значимой информации и норм уголовно-исполнительного права
64% - 55%	Учащийся демонстрирует достаточное знание основных теоретических положений, в рамках осваиваемой компетенции, умеет использовать полученные знания для решения основных практических задач в отдельных сферах профессиональной деятельности, частично владеет основными навыками анализа и систематизации криминалистически значимой информации и норм уголовно-исполнительного права
менее 55%	Учащийся демонстрирует отсутствие знания основных теоретических положений, в рамках осваиваемой компетенции, не умеет применять полученные знания на практике, не владеет навыками анализа и систематизации криминалистически значимой информации и норм уголовно-исполнительного права

Тестирование

Уровень знаний, умений и навыков обучающегося при устном ответе во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критерием оценивания при проведении тестирования, является количество верных ответов, которые дал студент на вопросы теста. При расчете количества баллов, полученных студентом по итогам тестирования, используется следующая формула:

$$Б = \frac{В}{О}' 100\%,$$

где Б – количество баллов, полученных студентом по итогам тестирования;
В – количество верных ответов, данных студентом на вопросы теста;
О – общее количество вопросов в тесте.

Решение задач

Уровень знаний, умений и навыков обучающегося при решении задач во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критерием оценивания при решении задач, является количество верно решенных задач. При расчете количества баллов, полученных студентом по итогам решения задач, используется следующая формула:

$$Б = \frac{В}{О}' 100\%,$$

где Б – количество баллов, полученных студентом по итогам решения задач;
В – количество верно решенных задач;
О – общее количество задач.

Решение ситуационной задачи

Уровень знаний, умений и навыков обучающегося при выполнении ситуационной задачи во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критериями оценивания является сбор и обобщение необходимой информации,

правильное выполнение необходимых расчетов, достоверность и обоснованность выводов.

При оценивании результатов решения ситуационной задачи используется следующая шкала оценок:

100% - 85%	Учащийся демонстрирует совершенное знание основных теоретических положений, умеет собирать и обобщать необходимую информацию, правильно осуществляет расчеты, делает обоснованные выводы
84% - 65%	Учащийся демонстрирует знание большей части основных теоретических положений, может собрать большую часть необходимой информации, рассчитывает необходимые показатели, делает выводы, допуская при этом незначительные ошибки
64% - 55%	Учащийся демонстрирует знание некоторой части основных теоретических положений, может собрать некоторую часть необходимой информации, рассчитывает необходимые показатели, делает выводы, допуская при этом ошибки
менее 55%	Учащийся демонстрирует отсутствие знания основных теоретических положений, умений и навыков в рамках осваиваемой компетенции

5.3. Один или несколько тематических блоков дисциплины завершаются контрольной точкой (далее – КТ). Текущий контроль успеваемости по дисциплине предусматривает 2 (две) 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 студент	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,3	30
КТ 2	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 1-3.

Тестовые задания с инструкцией по выполнению:

Тест 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое кибербезопасность?

1. Защита только компьютерных сетей.

2. Защита информации и информационных систем от угроз.

3. Использование антивирусов.

4. Хранение данных на флешке.

Какой из перечисленных факторов не относится к основным угрозам кибербезопасности?

1. Вирусы и вредоносное ПО.

2. Социальная инженерия.

3. Физическая кража компьютера.

4. Сильный пароль.

Тест 2. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое киберпреступность?

1. Любое преступление, совершённое с использованием компьютерных технологий или в сети Интернет.

2. Преступления, связанные только с кражей компьютеров.

3. Нарушение правил пользования компьютером.

4. Преступления, совершённые только в отношении государственных информационных систем.

Чем киберпреступность отличается от компьютерных преступлений?

1. Киберпреступность — это более широкое понятие, включающее преступления в цифровой среде, а компьютерные преступления — только те, где компьютер выступает объектом или инструментом.

2. Это синонимы.

3. Компьютерные преступления — это только взлом паролей.

4. Киберпреступность — это преступления против личности, а компьютерные — против государства.

Тест 3. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое преступление в сфере компьютерной информации?

1. Любое нарушение правил работы с компьютером.

2. Уголовно наказуемое деяние, связанное с неправомерным доступом, использованием, распространением или уничтожением компьютерной информации.

3. Кража компьютерного оборудования.

4. Нарушение авторских прав на программное обеспечение.

Какой из перечисленных примеров относится к преступлению в сфере компьютерной информации?

1. Кража системного блока из офиса.

2. Неправомерный доступ к защищённой компьютерной информации.

3. Порча имущества в общественном месте.

4. Нарушение правил дорожного движения.

Тест 4. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое неправомерный доступ к компьютерной информации?

1. Доступ к информации с разрешения владельца.

2. Доступ к информации без права на это, с нарушением установленных правил.

3. Использование компьютера в личных целях.

4. Установка антивирусной программы.

Какой вид преступления связан с созданием и распространением вредоносных программ?

1. Мошенничество.

2. Создание, использование и распространение вредоносных компьютерных программ.

3. Кража данных.

4. Нарушение авторских прав.

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

КТ – 2.

Тема 4-5.

Тестовые задания с инструкцией по выполнению:

Тест 1.

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

Что такое киберпреступления экономического характера?

1. Преступления, связанные с кражей компьютерного оборудования.

2. Преступления, направленные на хищение финансовых средств, мошенничество, незаконное получение экономической выгоды с использованием цифровых технологий.

3. Преступления, совершаемые только в отношении государственных учреждений.

4. Нарушение авторских прав на программное обеспечение.

Какой из перечисленных примеров относится к киберпреступлениям экономического характера?

1. Кража ноутбука из офиса.

2. Фишинг с целью хищения данных банковских карт.

3. Порча имущества в общественном месте.

4. Нарушение правил дорожного движения.

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ или несколько.

Что такое фишинг в контексте экономических киберпреступлений?

1. Вид интернет-мошенничества с целью получения доступа к финансовым данным.

2. Программа для защиты от вирусов.

3. Метод шифрования данных.

4. Способ восстановления паролей.

Что такое криптоскам?

1. Легальная торговля криптовалютой.

2. Мошенничество, связанное с криптовалютами (фальшивые биржи, ICO, кошельки).

3. Майнинг криптовалюты на своём компьютере.

4. Хранение криптовалюты в банке.

Тест 3.

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

Какой из перечисленных методов относится к техническим мерам противодействия киберпреступности?

1. Обучение сотрудников.
2. Установка и обновление антивирусного ПО, межсетевых экранов.
3. Разработка законов.
4. Проведение опросов.

Какой из перечисленных способов является организационной мерой противодействия киберпреступности?

1. Установка антивируса.
2. Разработка политики информационной безопасности, обучение персонала, контроль доступа.
3. Взлом хакерских сайтов.
4. Использование сложных паролей.

Тест 4.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Какой из перечисленных методов относится к превентивным мерам противодействия киберпреступности?
1. Расследование уже совершённого преступления.
2. Установка систем обнаружения вторжений и анализ уязвимостей.
3. Наказание виновных лиц.
4. Восстановление данных после атаки.

Что такое мониторинг событий информационной безопасности?
1. Просмотр фильмов о хакерах.
2. Постоянное наблюдение за действиями в системе для выявления подозрительной активности.
3. Разработка программного обеспечения.
4. Проведение праздников в офисе.

Критерии оценивания тестовых заданий:

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

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

Для решения контрольных заданий обучающемуся разрешается использование нормативно-правовых актов.

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

6.1. Промежуточная аттестация (зачет) проводится с применением метода устного опроса.

6.2. Типовые оценочные материалы промежуточной аттестации

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

Тема 1. Понятие кибербезопасности. Основные риски и угрозы в области кибербезопасности. ПКс-2.1

1. Задания открытого типа.

1.1. Вопросы открытого типа:

1.Понятие кибербезопасности. Соотношение кибербезопасности и информационной безопасности.

2. Области кибербезопасности. Безопасность сетей. Безопасность приложений. Безопасность информации. Операционная безопасность.

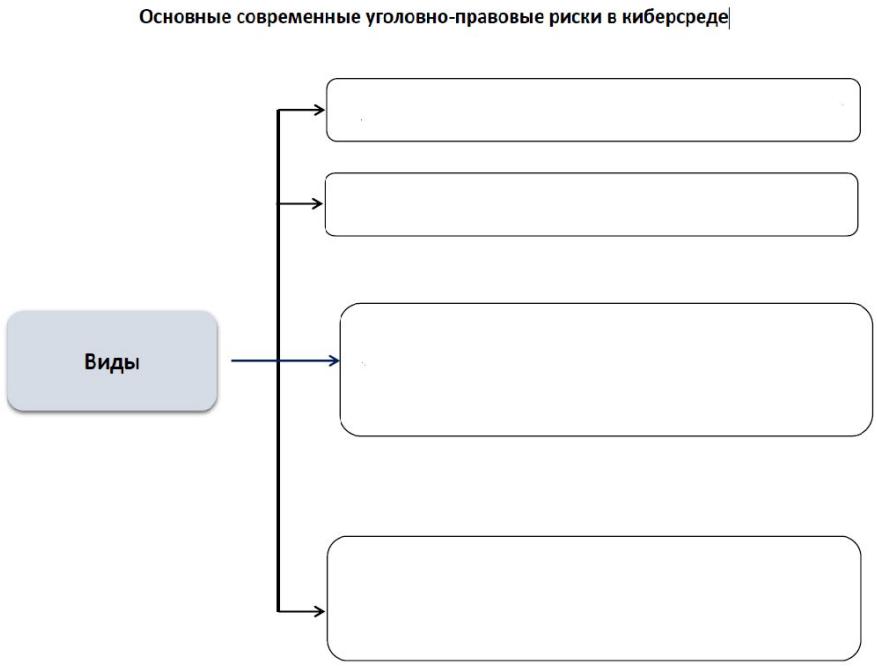
3. Международно-правовое регулирование кибербезопасности. Конвенция Совета Европы о компьютерных преступлениях.

4. Законодательство Российской Федерации в сфере кибербезопасности.

5. Основные риски кибербезопасности. Современные угрозы в области кибербезопасности.

1.2. Контрольные задания с ключами правильных ответов:

Задание 1. Составить схему «Основные современные уголовно-правовые риски в киберсреде»:



Задание 2. Составить сравнительную таблицу «Конвенция Организации Объединенных Наций против киберпреступности» и «Конвенция Совета Европы о киберпреступности»:

Критерий	**Конвенция ООН против киберпреступности**	**Конвенция Совета Европы о киберпреступности (Будапештская)**
Дата принятия		
Территориальный охват		
Цели		
Механизмы сотрудничества		
Актуальность		
Права человека		
Вступление в силу		
Организации-инициаторы		

2. Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Варианты ответов: а) верно б) неверно		
2.	Кибербезопасность находит применение в самых разных областях, от бизнес-сферы до		

	мобильных технологий. Варианты ответов: а) верно б) неверно		

3. Задания закрытого типа.

3.1. Тестовые задания.

Тестовые задания:

Тест 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое кибербезопасность?

1. Защита только компьютерных сетей.
2. Защита информации и информационных систем от угроз.
3. Использование антивирусов.
4. Хранение данных на флешке.

Какой из перечисленных факторов не относится к основным угрозам кибербезопасности?

1. Вирусы и вредоносное ПО.
2. Социальная инженерия.
3. Физическая кража компьютера.
4. Сильный пароль.

Тест 2. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое социальная инженерия в контексте кибербезопасности?

1. Метод взлома с помощью технических средств.
2. Манипуляция людьми с целью получения конфиденциальной информации.
3. Разработка антивирусных программ.
4. Создание защищённых сетей.

Какой из перечисленных принципов является основой кибербезопасности?

1. Открытость всех данных.
2. Конфиденциальность, целостность и доступность информации.
3. Использование только бесплатных программ.
4. Хранение всех данных на одном устройстве.

Тема 2. Понятие и виды киберпреступности. ПКс-2.2

1. Задания открытого типа.

1.1.Вопросы открытого типа:

1. Понятие киберпреступности. Соотношение киберпреступности и компьютерных преступлений.

2. Виды киберпреступлений. Противоправные деяния против конфиденциальности, доступности и целостности компьютерных систем и данных (несанкционированное вмешательство).

3. Действия, связанные с компьютерами (подлог, мошенничество). Противоправные поступки, связанные с контентом (содержанием) информации. Правонарушения в сфере авторских и смежных прав.

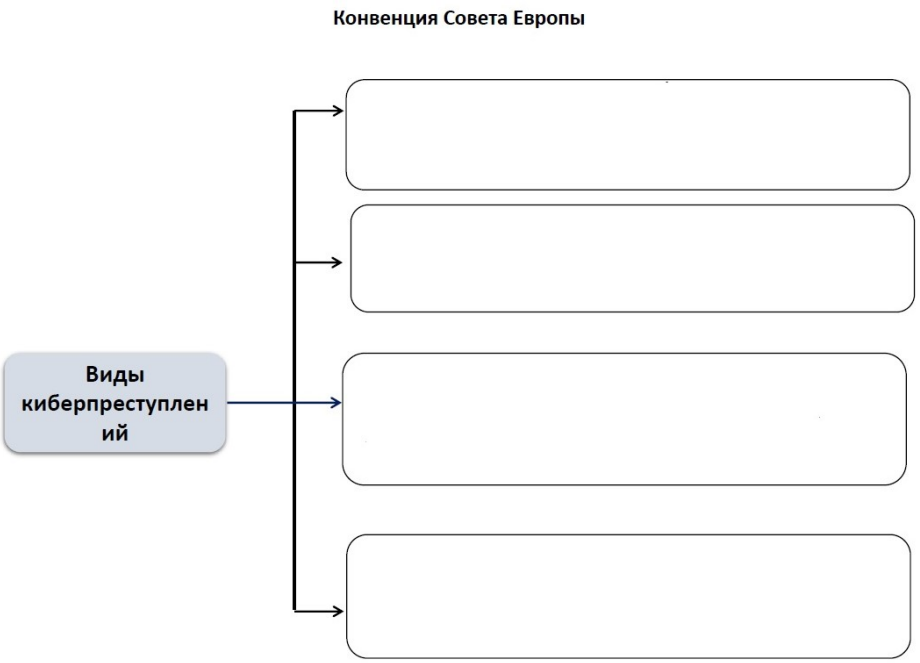
4. Основные современные уголовно-правовые риски в киберсреде. Промышленный шпионаж и иные посягательства на охраняемые законом тайны и персональные данные (ст. 137-138 УК РФ).

5. Киберпреступления, посягающие на личные права и государственные интересы.

1.2. Контрольные задания с ключами правильных ответов:

Задание 1.

Составить схему «Виды киберпреступлений, предусмотренных Конвенцией Совета Европы о киберпреступности»:



Задание 2. Составить таблицу «Основные виды противоправных поступков, связанных с контентом (содержанием) информации в цифровой среде»:

Вид противоправного поступка	**Характеристика**
Распространение запрещённого контента	
Оскорбление и клевета	
Нарушение авторских прав	

Разглашение персональных данных	
Фейковая информация и дезинформация	
Пропаганда и агитация, нарушающие закон	
Мошенничество с использованием контента	

2. Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Киберпреступность включает в себя «новые» преступления – те, которые стали возможными благодаря существованию информационно-коммуникационных технологий (ИКТ), – например, преступления, направленные против неприкосновенности частной жизни, конфиденциальности, целостности и доступности компьютерных данных и систем, а также традиционные преступления, совершению которых в той или иной степени способствуют ИКТ, включая правонарушения, связанные с использованием компьютерных средств, и правонарушения, связанные с содержанием компьютерных данных Варианты ответов: а) верно б) неверно		

2.	Хакерская атака – это термин, используемый для описания несанкционированного доступа к системам, сетям и данным. Варианты ответов: а) верно б) неверно		

Тестовые задания:

Тест 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое киберпреступность?

1. Любое преступление, совершённое с использованием компьютерных технологий или в сети Интернет.
2. Преступления, связанные только с кражей компьютеров.
3. Нарушение правил пользования компьютером.
4. Преступления, совершённые только в отношении государственных информационных систем.

Чем киберпреступность отличается от компьютерных преступлений?

1. Киберпреступность — это более широкое понятие, включающее преступления в цифровой среде, а компьютерные преступления — только те, где компьютер выступает объектом или инструментом.
2. Это синонимы.
3. Компьютерные преступления — это только взлом паролей.
4. Киберпреступность — это преступления против личности, а компьютерные — против государства.

Тест 2. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Какой из перечисленных примеров относится к киберпреступности?

1. Кража ноутбука из офиса.
2. Фишинг с целью хищения данных банковских карт.
3. Порча имущества в общественном месте.
4. Нарушение правил дорожного движения.

Что такое компьютерное преступление?

1. Преступление, совершённое исключительно с помощью компьютера или направленное на компьютерные системы.
2. Любое преступление, совершённое в интернете.
3. Преступление, связанное с нарушением авторских прав на программное обеспечение.
4. Преступление, совершённое только против государственных структур.

Тема 3. Преступления в сфере компьютерной информации. ПКс-2.1

1. Задания открытого типа.

1.1. Вопросы открытого типа:

1. Понятие компьютерных преступлений. Характеристика составов компьютерных преступлений.

2. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

3. Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272.1 УК РФ).

4. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

5. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

6. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).

7. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ).

6. Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции (ст. 274.3 УК РФ).

7. Организация деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации (ст. 274.4 УК РФ).

8. Организация деятельности по передаче информации, необходимой для регистрации и (или) авторизации пользователя сети "Интернет" для получения доступа к функциональным возможностям информационного ресурса (ст. 274.5 УК РФ).

1.2. Контрольные задания с ключами правильных ответов:

Задание 1.

Составить сравнительную таблицу «Основные виды преступлений в сфере компьютерной информации по Уголовному кодексу Российской Федерации»:

Вид преступления	**Характеристика**	**Примеры**	**Статья УК РФ**
Неправомерный доступ			
Создание и распространение вредоносных программ			
Нарушение правил эксплуатации			

Задание 2.

Решить задачу.

Задача

Гражданин Иванов, обладая навыками программирования, создал компьютерную программу, предназначенную для скрытого копирования паролей пользователей социальных сетей. Он разместил эту программу на интернет-форуме с инструкцией по её использованию, после чего программой воспользовались несколько человек, получив доступ к чужим аккаунтам.

Вопрос: Подлежит ли Иванов уголовной ответственности? Если да, то по какой статье УК РФ? Ответ обоснуйте.

2. Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Использование абонентского терминала пропуска трафика или виртуальной телефонной станции неуполномоченным лицом: Варианты ответов: а) допускается б) не допускается.		
2.	Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации относится к преступлениям в сфере компьютерной информации. Варианты ответов: а) верно б) не верно		

3. Задания закрытого типа.

3.1. Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое преступление в сфере компьютерной информации?

1. Любое нарушение правил работы с компьютером.
2. Уголовно наказуемое деяние, связанное с неправомерным доступом, использованием, распространением или уничтожением компьютерной информации.
3. Кража компьютерного оборудования.
4. Нарушение авторских прав на программное обеспечение.

Какой из перечисленных примеров относится к преступлению в сфере компьютерной информации?

1. Кража системного блока из офиса.
2. Неправомерный доступ к защищённой компьютерной информации.
3. Порча имущества в общественном месте.
4. Нарушение правил дорожного движения.

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ или несколько.

Что такое неправомерный доступ к компьютерной информации?

1. Доступ к информации с разрешения владельца.
2. Доступ к информации без права на это, с нарушением установленных правил.
3. Использование компьютера в личных целях.
4. Установка антивирусной программы.

Какой вид преступления связан с созданием и распространением вредоносных программ?

1. Мошенничество.
2. Создание, использование и распространение вредоносных компьютерных программ.
3. Кража данных.
4. Нарушение авторских прав.

Тема 4. Киберпреступления экономического характера. ПКс-2.3

1. Задания открытого типа.

1.1.Вопросы открытого типа:

1. Основные черты современно уголовного законодательства в сфере охраны экономических отношений. Уголовная политика в сфере охраны экономических отношений.
2. Характеристика экономических преступлений, совершаемых в киберпространстве. Классификация экономических преступлений.
3. Экономическое мошенничество.
4. Преступления в сфере предпринимательства.
5. Кредитные преступления.
6. Преступления в сфере конкуренции. Преступления на рынке ценных бумаг и финансовые преступления.
7. Преступления в сфере банкротства.
8. Служебные экономические преступления.
9. Преступления, совершаемые с использованием криптовалют и блокчейн технологий.
10. Неправомерное использование инсайдерской информации. Манипулирование рынком.

1.2. Контрольные задания с ключами правильных ответов:

Задание 1. Составить схему «Классификация киберпреступлений экономического характера».

Задание 2.

Решите задачу.

Задача.

Генеральный директор акционерного общества «ТехноСтрой» Петров, зная о тяжёлом финансовом положении компании, решил привлечь новых инвесторов. Для этого он опубликовал на официальном сайте общества и в СМИ заведомо ложный годовой отчёт, в котором указал прибыль в 50 миллионов рублей, хотя по факту компания понесла убытки в 10 миллионов рублей. На основании этих данных несколько инвесторов приобрели акции компании. Через месяц, когда истинное положение дел стало известно, акции компании резко упали в цене, а инвесторы понесли крупные убытки.

Вопрос: Должен ли Петров нести уголовную ответственность? Если да, то по какой статье УК РФ? Ответ обоснуйте.

2. Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Преступления с использованием криптовалют — это противоправные деяния, где цифровые активы выступают средством совершения преступления (хищение, фишинг, вымогательство) или его предметом (кража кошельков). Они часто связаны с мошенничеством, «инвестициями» в несуществующие проекты, отмыванием денег и наркоторговлей из-за анонимности. Варианты ответов: а)верно б) не верно		
2.	Преступления с использованием блокчейн-технологий — это незаконная деятельность (мошенничество, отмывание денег, наркоторговля), где криптовалюта выступает как предмет преступления или средство платежа. Используя анонимность и отсутствие посредников, преступники совершают кражи, вымогательства и трансграничные переводы преступных доходов. Варианты ответов: а) верно б) не верно		

3. Задания закрытого типа.

3.1. Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое киберпреступления экономического характера?

1. Преступления, связанные с кражей компьютерного оборудования.

2. Преступления, направленные на хищение финансовых средств, мошенничество, незаконное получение экономической выгоды с использованием цифровых технологий.

3. Преступления, совершаемые только в отношении государственных учреждений.

4. Нарушение авторских прав на программное обеспечение.

Какой из перечисленных примеров относится к киберпреступлениям экономического характера?

1. Кража ноутбука из офиса.

2. Фишинг с целью хищения данных банковских карт.

3. Порча имущества в общественном месте.

4. Нарушение правил дорожного движения.

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Что такое фишинг в контексте экономических киберпреступлений?

1. Вид интернет-мошенничества с целью получения доступа к финансовым данным.

2. Программа для защиты от вирусов.

3. Метод шифрования данных.

4. Способ восстановления паролей.

Что такое криптоскам?

1. Легальная торговля криптовалютой.

2. Мошенничество, связанное с криптовалютами (фальшивые биржи, ICO, кошельки).

3. Майнинг криптовалюты на своём компьютере.

4. Хранение криптовалюты в банке.

Тема 5. Противодействие киберпреступности. ПКс-2.1

1. Задания открытого типа.

1.1.Вопросы открытого типа:

1. Нормативно-правовая основа противодействия киберпреступности. Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий.

2. Противодействие распространению информации противоправного характера в сети "Интернет". Субъекты противодействия киберпреступности.

3. Кибердружины: понятие и функции.

4. Виктимологическая профилактика киберпреступлений. Реализация мер, направленных на повышение уровня цифровой и финансовой грамотности граждан.

5. Меры по снижению риска от посягательств в киберсфере.

6. Организация и проведение мероприятий по предупреждению вовлечения несовершеннолетних в противоправную деятельность в информационно-коммуникационной сфере.

1.2. Контрольные задания с ключами правильных ответов:

Задание 1. Охарактеризовать Концепцию государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий.

Задание 2. Составить таблицу «Меры по снижению риска от посягательств в киберсфере»:

Категория	**Описание и примеры**
Технические меры	
Организационные меры	
Контроль и мониторинг	
Процедурные меры	
Правовые меры	

2. Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Кибердружины относятся к субъектам противодействия киберпреступности. Варианты ответов: а) верно б) неверно		
2.	Реализация мер, направленных на повышение уровня цифровой и финансовой грамотности граждан, относится к виктимологической профилактике киберпреступности. Варианты ответов: а) верно б) неверно		

3. Задания закрытого типа.

3.1. Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Какой из перечисленных методов относится к техническим мерам противодействия киберпреступности?

1. Обучение сотрудников.

2. Установка и обновление антивирусного ПО, межсетевых экранов.
3. Разработка законов.
4. Проведение опросов.

Какой из перечисленных способов является организационной мерой противодействия киберпреступности?
1. Установка антивируса.
2. Разработка политики информационной безопасности, обучение персонала, контроль доступа.
3. Взлом хакерских сайтов.
4. Использование сложных паролей.

Тест 2.
Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные варианты ответа. Выбрать один верный ответ.

Какой из перечисленных методов относится к превентивным мерам противодействия киберпреступности?
1. Расследование уже совершённого преступления.
2. Установка систем обнаружения вторжений и анализ уязвимостей.
3. Наказание виновных лиц.
4. Восстановление данных после атаки.

Что такое мониторинг событий информационной безопасности?
1. Просмотр фильмов о хакерах.
2. Постоянное наблюдение за действиями в системе для выявления подозрительной активности.
3. Разработка программного обеспечения.
4. Проведение праздников в офисе.

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 студент 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	30-39

неточностями.	
Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.	20-29
Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	0-19

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

Для решения контрольных заданий обучающемуся разрешается использование нормативно-правовых актов

5. Оценочные материалы промежуточной аттестации по дисциплине Б1.В.ДЭ.05.01« Уголовно-правовые аспекты кибербезопасности»

5.1. Методы проведения зачета

Вопросы к зачету

1. Понятие кибербезопасности. Соотношение кибербезопасности и информационной безопасности.
2. Области кибербезопасности, их общая характеристика.
3. Международно-правовое регулирование кибербезопасности. Конвенция Совета Европы о компьютерных преступлениях.
4. Законодательство Российской Федерации в сфере кибербезопасности.
5. Основные риски кибербезопасности. Современные угрозы в области кибербезопасности.
6. Понятие киберпреступности. Соотношение киберпреступности и компьютерных преступлений.
7. Виды киберпреступлений, их общая характеристика.
8. Действия, связанные с компьютерами (подлог, мошенничество). Противоправные поступки, связанные с контентом (содержанием) информации. Правонарушения в сфере авторских и смежных прав.
9. Основные современные уголовно-правовые риски в киберсреде.

10. Киберпреступления, посягающие на личные права и государственные интересы.
11. Понятие компьютерных преступлений. Характеристика составов компьютерных преступлений.
12. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).
13. Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272.1 УК РФ).
14. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).
15. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).
16. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).
17. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ).
18. Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции (ст. 274.3 УК РФ).
19. Организация деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации (ст. 274.4 УК РФ).
20. Организация деятельности по передаче информации, необходимой для регистрации и (или) авторизации пользователя сети "Интернет" для получения доступа к функциональным возможностям информационного ресурса (ст. 274.5 УК РФ).
21. Основные черты современно уголовного законодательства в сфере охраны экономических отношений. Уголовная политика в сфере охраны экономических отношений.
22. Характеристика экономических преступлений, совершаемых в киберпространстве. Классификация экономических преступлений.
23. Экономическое мошенничество.
24. Преступления в сфере предпринимательства.
25. Кредитные преступления.
26. Преступления в сфере конкуренции. Преступления на рынке ценных бумаг и финансовые преступления.
27. Преступления в сфере банкротства.
28. Служебные экономические преступления.
29. Преступления, совершаемые с использованием криптовалют и блокчейн технологий.
30. Неправомерное использование инсайдерской информации. Манипулирование рынком.
31. Нормативно-правовая основа противодействия киберпреступности. Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий.
32. Противодействие распространению информации противоправного характера в сети "Интернет". Субъекты противодействия киберпреступности.
33. Кибердружины: понятие и функции.
34. Виктимологическая профилактика киберпреступлений.
35Реализация мер, направленных на повышение уровня цифровой и финансовой грамотности граждан.
36. Меры по снижению риска от посягательств в киберсфере.

37. Организация и проведение мероприятий по предупреждению вовлечения несовершеннолетних в противоправную деятельность в информационно-коммуникационной сфере.
38. Противоправные деяния против конфиденциальности, доступности и целостности компьютерных систем и данных (несанкционированное вмешательство).
39. Промышленный шпионаж и иные посягательства на охраняемые законом тайны и персональные данные (ст. 137-138 УК РФ).
40. Безопасность сетей и приложений. Понятие и общая характеристика, способы обеспечения.
41. Безопасность информации. Понятие и общая характеристика, способы обеспечения.
42. Операционная безопасность. Понятие и общая характеристика, способы обеспечения.

5.2. Оценочные материалы промежуточной аттестации

Компонент компетенции	Промежуточный / ключевой индикатор оценивания	Критерий оценивания
ПКс-2.1 Способен принимать законные и обоснованные решения в сфере осуществления юридической деятельности на основе развитого правового сознания	- обладает развитым правовым сознанием	- принимает законные решения в сфере осуществления юридической деятельности
	- аргументирует законность и обоснованность принятого решения	- соотносит конкретные правовые нормы в различных сферах правоприменительной деятельности
ПКс-2.2 Способен принимать законные и обоснованные решения в сфере осуществления юридической деятельности на основе развитого правового мышления	- обладает развитым правовым мышлением	- применяет основные принципы и законы развитого правового мышления в процессе принятия законного и обоснованного решения при осуществлении юридической деятельности
	- применяет основные принципы и законы развитого правового мышления в процессе принятия законного и обоснованного решения при осуществлении юридической деятельности	- принимает обоснованные решения в сфере осуществления юридической деятельности
ПКс-2.3 Способен принимать законные и обоснованные решения в сфере осуществления юридической деятельности на основе развитой	- обладает развитой правовой культурой	- учитывает в работе этические и межкультурные аспекты

Компонент компетенции	Промежуточный / ключевой индикатор оценивания	Критерий оценивания
правовой культуры	- организовывает порядок принятия законного и обоснованного решения в сфере осуществления юридической деятельности с учётом высокого уровня правовой культуры юриста	- принимает законные и обоснованные решения в сфере осуществления юридической деятельности на основе развитой правовой культуры юриста

Типовые оценочные средства промежуточной аттестации

Шкала оценивания

Критериями оценивания на зачете является демонстрация основных теоретических положений, в рамках осваиваемой компетенции, умение применять полученные знания на практике, овладение навыками анализа и систематизации информации.

Для дисциплин, формой промежуточной аттестации которых является зачет с оценкой, приняты следующие соответствия:

- 85-100% - «отлично» (5);
- 65-84% - «хорошо» (4);
- 64-55% - «удовлетворительно» (3);
- менее 55% - «неудовлетворительно» (2).

При оценивании результатов устного опроса используется следующая шкала оценок:

100% - 85% (отлично)	Этапы компетенции, предусмотренные образовательной программой, сформированы на высоком уровне. Свободное владение материалом, выявление межпредметных связей. Уверенное владение понятийным аппаратом дисциплины. Практические навыки профессиональной деятельности сформированы на высоком уровне. Способность к самостоятельному нестандартному решению практических задач
84% - 65% (хорошо)	Этапы компетенции, предусмотренные образовательной программой, сформированы достаточно. Детальное воспроизведение учебного материала. Практические навыки профессиональной деятельности в значительной мере сформированы. Присутствуют навыки самостоятельного решения практических задач с отдельными элементами творчества.
64% - 55% (удовлетворительно)	Этапы компетенции, предусмотренные образовательной программой, сформированы на минимальном уровне. Наличие минимально допустимого уровня в усвоении учебного материала, в т.ч. в самостоятельном решении практических задач. Практические навыки профессиональной деятельности сформированы не в полной мере.
менее 55% (неудовлетворительно)	Этапы компетенции, предусмотренные образовательной программой, не сформированы. Недостаточный уровень усвоения понятийного аппарата и наличие фрагментарных знаний по дисциплине. Отсутствие минимально допустимого уровня в самостоятельном решении практических задач.

	Практические навыки профессиональной деятельности не сформированы.

Фонды оценочных средств промежуточной аттестации по дисциплине представлены в приложении 1.

7. Методические материалы по освоению дисциплины Б1.В.ДЭ.05.01« Уголовно-правовые аспекты кибербезопасности»

Методические рекомендации по подготовке к практическому (семинарскому) занятию

Основной целью практического (семинарского) занятия является проверка глубины понимания студентом изучаемой темы, учебного материала и умения изложить его содержание ясным и четким языком, развитие самостоятельного мышления и творческой активности у студента, умения решать практические задачи. На практических (семинарских) занятиях предполагается рассматривать наиболее важные, существенные, сложные вопросы которые, наиболее трудно усваиваются студентами. При этом готовиться к практическому (семинарскому) занятию всегда нужно заранее. Подготовка к практическому (семинарскому) занятию включает в себя следующее:

- обязательное ознакомление с вопросами для устного опроса,
- изучение конспектов лекций, соответствующих разделов учебника, учебного пособия, содержания рекомендованных нормативных правовых актов;
- работа с основными терминами (рекомендуется их выучить);
- изучение дополнительной литературы по теме занятия, делая при этом необходимые выписки, которые понадобятся при обсуждении на семинаре;
- формулирование своего мнения по каждому вопросу и аргументированное его обоснование;
- запись возникших во время самостоятельной работы с учебниками и научной литературы вопросов, чтобы затем на семинаре получить на них ответы;
- обращение за консультацией к преподавателю.

Рекомендации по планированию и организации времени, необходимого на изучение дисциплины (модуля)

Структура времени, необходимого на изучение дисциплины

Форма изучения дисциплины	Время, затрачиваемое на изучение дисциплины, %
Изучение литературы, рекомендованной в учебной программе	40
Решение задач, практических упражнений и ситуационных примеров	40
Изучение тем, выносимых на самостоятельное рассмотрение	20
Итого	100

Методические рекомендации по работе с литературой

При работе с литературой необходимо обратить внимание на следующие вопросы. Основная часть материала изложена в учебниках, включенных в основной список литературы рабочей программы дисциплины. Основная и дополнительная литература предназначена для повышения качества знаний студента, расширения его

кругозора. При работе с литературой приоритет отдается первоисточникам (нормативным материалам, законам, кодексам и пр.).

При изучении дисциплины студентам следует обратить особое внимание на нормативно-правовые акты, регулирующие деятельность хозяйствующих субъектов в РФ.

Рекомендации по планированию и организации времени, необходимого на изучение дисциплины

Рекомендации по изучению методических материалов

Методические материалы по дисциплине Б1.В.ДЭ.05.01« Уголовно-правовые аспекты кибербезопасности» позволяют студенту оптимальным образом организовать процесс изучения данной дисциплины. Методические материалы по дисциплине призваны помочь студенту понять специфику изучаемого материала, а в конечном итоге – максимально полно и качественно его освоить. В первую очередь студент должен осознать предназначение методических материалов: структуру, цели и задачи. Для этого он знакомится с преамбулой, оглавлением методических материалов, говоря иначе, осуществляет первичное знакомство с ним. В разделе, посвященном методическим рекомендациям по изучению дисциплины, приводятся советы по планированию и организации необходимого для изучения дисциплины времени, описание последовательности действий студента («сценарий изучения дисциплины»), рекомендации по работе с литературой, советы по подготовке к экзамену и разъяснения по поводу работы с тестовой системой курса и над домашними заданиями. В целом данные методические рекомендации способны облегчить изучение студентами дисциплины и помочь успешно сдать экзамен. В разделе, содержащем учебно-методические материалы дисциплины, содержание практических занятий по дисциплине.

Рекомендации для подготовки к зачету

При подготовке к зачету студент внимательно просматривает вопросы, предусмотренные рабочей программой, и знакомиться с рекомендованной основной литературой. Основой для сдачи зачета студентом является изучение конспектов лекций, прослушанных в течение семестра, информация, полученная в результате самостоятельной работы в течение семестра.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2026. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588094
2. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588741 (дата обращения: 16.04.2026).

3. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/589902
4. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588515

8.2. Дополнительная литература

1. Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху : учебное пособие для вузов / О. А. Степанов. — Москва : Издательство Юрайт, 2026. — 103 с. — (Высшее образование). — ISBN 978-5-534-19963-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588068
2. Бессмертный, И. А. Искусственный интеллект. Введение в многоагентные системы : учебник для вузов / И. А. Бессмертный. — Москва : Издательство Юрайт, 2026. — 148 с. — (Высшее образование). — ISBN 978-5-534-20348-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/589921
3. 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, 2026. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583236
4. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Высшее образование). — ISBN 978-5-534-17866-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590420
5. Войниканис, Е. А. Правовое регулирование информационных отношений в сфере защиты информации с ограниченным доступом : учебник для вузов / Е. А. Войниканис ; под редакцией М. А. Федотова. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 50 с. — (Высшее образование). — ISBN 978-5-534-19364-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/589232
6. Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 352 с. — (Высшее образование). — ISBN 978-5-534-19386-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/586060
7. Компьютерные сети : учебник и практикум для вузов / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2026. — 515 с. — (Высшее образование). — ISBN 978-5-534-21452-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590190

8. Асмолов А.Г., Цветкова М.С., Янисов П.В. Цифровая социализация в культурно-исторической парадигме: изменяющийся ребенок в изменяющемся мире // Национальный психологический журнал. — 2018. — № 4(32). — С. 3-18.
9. Солдатова Г.В., Зотова Е.Ю., Чекалина А.И., Гостимская О.С. «Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об интернете». — М., 2011.
10. Рекомендации ФСТЭК России. Основы безопасности персональных данных при их обработке в информационных системах персональных данных. — М., 2022.
11. Национальный центр помощи пропавшим и пострадавшим детям, проект «КиберМосква». Методическое пособие «Основы цифровой гигиены». — М., 2023. — С. 15-22.
12. Казаков С.П., Олейников Я.С. Киберпреступность: методы противодействия. Учебное пособие. — М.: Проспект, 2021.
13. Расторгуев С.П. Информационная война. — М.: Академический проект, 2020.
14. Всемирная организация здравоохранения (ВОЗ). Информационный бюллетень о буллинге среди подростков (с учётом кибербуллинга), 2022.
15. Ищенко Е.П. Виртуальный криминал. / Е. П. Ищенко. — Москва : Проспект, 2024. — 232 с.

8.3. Нормативные правовые документы и иная правовая информация

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)
2. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174-ФЗ // Российская газета. – 2001. – 22 декабря (с посл. изм.).

3.Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (послед. ред.)

4. О прокуратуре Российской Федерации: Федеральный закон от 17 января 1992 г. N 2202-I (с посл. изм.).
5. О полиции: Федеральный закон Российской Федерации от 7 февраля 2011 года № 3-ФЗ (с посл. изм.).
6. О Следственном комитете Российской Федерации: Федеральный закон Российской Федерации от 28 декабря 2010 года № 403-ФЗ (с посл. изм.).
7. Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. N 144-ФЗ (с посл. изм.).
8. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с посл. изм.).

8.4. Интернет-ресурсы, справочные системы.

1. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) Официальный сайт: https://rkn.gov.ru/
2. Федеральная служба по финансовому мониторингу (Росфинмониторинг) Официальный сайт: https://www.fedsfm.ru/
3. Портал «Российская электронная школа» (РЭШ). Раздел «Уроки цифровой грамотности». Роскачество (rskrf.ru): разделы о цифровой безопасности и проверке приложений.

4. Бернская конвенция по охране литературных и художественных произведений 1886 года (http://www.wipo.int/treaties/en/text.jsp?file_id=283698).
5. Конвенция, учреждающая Всемирную организацию интеллектуальной собственности (ВОИС) 1967 года (http://www.wipo.int/publications/en/details.jsp?id=303&plang=EN).
6. Конвенция о киберпреступности 2001 года (Совет Европы) (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561).
7. Конвенция о предупреждении терроризма 2005 года (Европы) (https://www.coe.int/en/web/conventions/full-list/conventions/rms/09000016808c3f55).
8. Директива Совета 2008/114/ЕС от 8 декабря 2008 г. об определении и обозначении европейской критической инфраструктуры и об оценке необходимости усиления ее защиты (https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32008L0114&from=EN).
9. Закон о киберпреступлениях 2015 года (Ямайка) http://www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf).
10. Закон о киберпреступлениях 2015 года (Танзания) (https://rsf.org/sites/default/files/the_cyber_crime_act_2015.pdf)
11. Закон о предупреждении киберпреступности 2012 года (Республиканский закон №.10175; RA10175) (Флиппины) (https://www.lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html).
12. Федеральный закон №.2 от 2006 года о предупреждении преступлений в области информационных технологий (Объединенные Арабские Эмираты) (http://www.wipo.int/wipolex/en/details.jsp?id=13817).
13. Закон об информации и коммуникации (Кения) (http://kfcb.co.ke/wpcontent/uploads/2016/07/Kenya_Information_and_Communications_Act.pdf).
14. Международный пакт о гражданских и политических правах 1966 года (https://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf).

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

Материально-техническое обеспечение дисциплины включает в себя:

- лекционные аудитории, оборудованные видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном;
- помещения для проведения семинарских и практических занятий, оборудованные учебной мебелью.

Дисциплина поддержана соответствующими лицензионными программными продуктами: Microsoft Windows 7 Prof, Microsoft Office 2010, Kaspersky 8.2, СПС Гарант, СПС Консультант.

Программные средства обеспечения учебного процесса включают:

- программы презентационной графики (MS PowerPoint – для подготовки слайдов и презентаций);
- текстовые редакторы (MS WORD), MS ECXEL – для таблиц, диаграмм.

Вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

Помещения для самостоятельной работы обучающихся включают следующую оснащенность: столы аудиторные, стулья, доски аудиторные, компьютеры с подключением к локальной сети института (включая правовые системы) и Интернет.

Для изучения учебной дисциплины используются автоматизированная библиотечная информационная система и электронные библиотечные системы.