Лебедева Екатерина Александровна
Подписано цифровой подписью: Лебедева Екатерина Александровна
Дата: 2026.06.25 14:40:16 +03'00'

Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.02 Правовая защита от киберугроз и инцидентов (Incident Response)
(индекс, наименование дисциплины в соответствии с учебным планом)

40.04.01 "Юриспруденция"
(код, наименование направления подготовки)

Правовое обеспечение использования искусственного интеллекта
(наименование образовательной программы)

Очная форма обучения
(форма обучения)

Год набора – 2026
Нижний Новгород, 2026 г.

Автор(ы)-составитель(и) РПД:

Калинина Евгения Валерьевна, доктор юридических наук, доцент, заведующая кафедрой гражданского и международного права

Заведующий кафедрой:

Калинина Евгения Валерьевна, доктор юридических наук, доцент, заведующая кафедрой гражданского и международного права

Рабочая программа дисциплины Б1.В.02 «Правовая защита от киберугроз и инцидентов (Incident Response)» одобрена на заседании кафедры гражданского и международного права

протокол № 6 от «4» марта 2026 г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы
2. Объем и место дисциплины в структуре образовательной программы
3. Содержание и структура дисциплины
4. Типы оценочных материалов, показатели, критерии, шкалы оценивания
5. Формы аттестации и типовые оценочные материалы для текущего контроля успеваемости обучающихся
6. Формы промежуточной аттестации по дисциплине, типы оценочных материалов, показатели, критерии, шкалы оценивания
7. Методические материалы по освоению дисциплины
8. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»
9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

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

Дисциплина Б1.В.02 «Правовая защита от киберугроз и инцидентов (Incident Response)» обеспечивает формирование у обучающихся следующих профессиональных компетенций:

ОТФ/ТФ и реквизиты ПС *(при наличии)*	**Код компетенции**	**Наименование компетенции**	**Код индикатора достижения компетенций**	**Наименование индикатора достижения компетенций**	**Образовательный результат**
	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК-1.1	Определяет стратегию действий на основе критического анализа и системного подхода	ИУК-1.1 З-1 (Incident Response). Знает: методы системного анализа киберинцидентов как комплексных проблемных ситуаций, включающих технологические, правовые и организационные аспекты; принципы разработки стратегий реагирования на инциденты и восстановления после атак в условиях неопределенности. ИУК-1.1 У-1 (Incident Response). Умеет: выявлять структурные элементы киберинцидента (вектор атаки, затронутые активы, пострадавшие субъекты, нарушенные нормы права); разрабатывать и обосновывать стратегические варианты действий по правовой защите и минимизации последствий инцидента.
ОТФ С/7 Правовое обеспечение охраны и защиты прав на РИД и СИ ТФ С/01.7 Правовое обеспечение охраны, осуществления прав на РИД и СИ, а также распоряжения этими правами и	**ПКс-ИИ-3 (проф. спец.)**	Способен представлять интересы клиентов в спорах, связанных с причинением вреда решениями ИИ, защитой интеллектуальных прав на AI-модели и данные, а также в административных процедурах, связанных с регулированием инновационны	ИПКс-ИИ-3.2	Разрабатывает и реализует правовую стратегию защиты интересов клиента при расследовании инцидентов, связанных с ИИ (утечка данных, дискриминационные решения, причинение вреда), включая взаимодействие с органами власти и подготовку	ИПКс-ИИ-3.2 З-1 (Incident Response). Знает: административные процедуры и полномочия регуляторов (Роскомнадзор, ФСТЭК, ФАС, прокуратура) при расследовании инцидентов, связанных с утечками данных и сбоями в работе ИИ-систем; требования к содержанию планов исправительных мероприятий и уведомлений об инцидентах. ИПКс-ИИ-3.2 У-1 (Incident Response). Умеет: выстраивать коммуникацию с регуляторами в ходе расследования инцидента; разрабатывать и представлять структурированные документы (позиции, пояснения, планы устранения нарушений), направленные на минимизацию правовых последствий и

их защиты ТФ С/02.7 Информационное и аналитическое сопровождение мероприятий по защите прав на ИС, в том числе за рубежом (40.001 Специалист по патентоведению утв. приказом Министерства труда и социальной защиты РФ от 21.10.2021 № 748н)		х технологий		структурированных документов, определяющих шаги по устранению причин выявленных несоответствий, ошибок или жалоб, направленных на предотвращение их повторения в будущем.	предотвращение повторения инцидентов, с учетом технических возможностей клиента.
	ПКо ОС-2 (проф. обяз.)	Способен представлять интересы физических и юридических лиц в судах и органах исполнительной власти, оказывая эффективную профессиональную помощь и защиту физических и юридических лиц в сфере бизнеса	ИПКо ОС-2.1	Демонстрирует знание порядка судебного, досудебного и внесудебного производства, умеет составлять процессуальные акты, собирать и представлять сведения, имеющие доказательственное значение при разрешении правового конфликта в сфере бизнеса	ИПКо ОС-2.1 З-1 (Incident Response). Знает: процессуальные особенности доказывания по делам, связанным с киберинцидентами и утечками данных (фиксация факта инцидента, сбор и оформление электронных доказательств, привлечение экспертов). ИПКо ОС-2.1 У-1 (Incident Response). Умеет: формировать правовую позицию по защите интересов клиента, пострадавшего от кибератаки (или обвиняемого в нарушении требований к защите данных); готовить процессуальные документы (иски, жалобы, ходатайства) и взаимодействовать с правоохранительными и надзорными органами при расследовании инцидентов.

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

Общая трудоемкость дисциплины составляет 144 а.ч. (4 з.е.)

Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся: 3 сем. - лекции – 14 а.ч., лабораторные работы – 2 ч., практические занятия – 40 а.ч., самостоятельная работа – 79 а.ч., зачет с оценкой – контактная работа на аттестацию в период экзаменационных сессий – 9 часов.

Дисциплина *«Правовая защита от киберугроз и инцидентов (Incident Response)»* относится к дисциплинам части, формируемой участниками образовательных отношений. Изучается на очной форме обучения - на 2 курсе.

Для освоения дисциплины «*Правовая защита от киберугроз и инцидентов (Incident Response)»* обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения дисциплин *«Информационное право» и «Информационные технологии в юридической деятельности»*.

Форма промежуточной аттестации в соответствии с учебным планом:

Очная форма обучения – зачет с оценкой.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и (или) разделов		Объем дисциплины, ак.час											Форма текущего контроля успеваемости, промежуточной аттестации
		ВСЕГО	Контактная работа обучающихся с преподавателем по видам учебных занятий						Период промежуточной аттестации (сессия)			Самостоятельная работа		
			Период теоретического обучения											
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Кат тэк	Контроль	СРкр	СРэк	СР
			Л	ВЛ	ЛР	ПЗ								
Тема 1.	Введение в правовое обеспечение кибербезопасности и Incident Response	12	1	0	0	4	0	0	0	0		0	0	7	Устный опрос, Ситуационная задача
Тема 2.	Организационно-правовые основы формирования CSIRT	14	2	0	0	4	0	0	0	0		0	0	8	Устный опрос, Ситуационная задача
Тема 3.	Правовые аспекты	14	2	0	0	4	0	0	0	0		0	0	8	Устный опрос,

	выявления киберугроз и оценки рисков (Legal Risk Assessment)													Ситуационная задача
Тема 4.	Международное сотрудничество и юрисдикционные аспекты	14	2	0	0	4	0	0	0	0	0	0	8	Устный опрос, Ситуационная задача
Тема 5.	Правовые режимы защиты информации и их влияние на реагирование	14	2	0	0	4	0	0	0	0	0	0	8	Устный опрос, Ситуационная задача
Тема 6.	Процессуальные основы сбора цифровых доказательств (Digital Forensics)	14	2	0	0	4	0	0	0	0	0	0	8	Устный опрос, Ситуационная задача
Тема 7.	Взаимодействие с правоохранительными органами и регуляторами	12	0	0	0	4	0	0	0	0	0	0	8	Устный опрос, Ситуационная задача
Тема 8.	Юридическая ответственность за киберинциденты	14	2	0	0	4	0	0	0	0	0	0	8	Устный опрос, Ситуационная задача
Тема 9.	Правовое обеспечение этапов сдерживания, ликвидации и восстановления	12	0	0	0	4	0	0	0	0	0	0	8	Устный опрос, Ситуационная задача
Тема 10.	Compliance и совершенствование системы реагирования	15	1	0	2	4	0	0	0	0	0	0	8	Устный опрос, Ситуационная задача
Промежуточная аттестация		9								9				Зачет с оценкой
Итого		144	14	0	2	40	0	0	0	9	0	0	79	

Используемые сокращения:

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

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.

СРэк – самостоятельная работа на подготовку к экзамену.СР – самостоятельная работа в семестре на подготовку к учебным занятиям.

3.2 Содержание дисциплины

Раздел 1. Теоретико-правовые основы реагирования на инциденты

Тема 1. Введение в правовое обеспечение кибербезопасности и Incident Response. УК-1.1

Понятие киберугрозы и инцидента информационной безопасности: правовая дефиниция и соотношение понятий.

Источники правового регулирования: международные стандарты (ISO/IEC 27035, NIST), российское законодательство (ФЗ «О безопасности», Доктрина ИБ РФ).

Национальное законодательство в сфере противодействия киберпреступности (гл. 28 УК РФ, КоАП РФ).

Роль права в управлении жизненным циклом инцидента: от обнаружения до извлечения уроков.

Тема 2. Организационно-правовые основы формирования CSIRT (Команды реагирования). ПКо ОС-2.1

Понятие и правовой статус CSIRT (Computer Security Incident Response Team) в корпоративной структуре.

Разработка локальных нормативных актов: Политика управления инцидентами, Регламент взаимодействия CSIRT.

Разграничение ответственности между IT-отделом, службой безопасности и юридическим департаментом.

Трудовые отношения и конфиденциальность: обязательства сотрудников CSIRT о неразглашении (NDA).

Тема 3. Правовые аспекты выявления киберугроз и оценки рисков (Legal Risk Assessment). ПКс-ИИ-3.1

Категорирование активов и их правовая защита (государственная тайна, коммерческая тайна, персональные данные).

Правовая основа риск-ориентированного подхода (ФЗ-№184 «О техническом регулировании», стандарты ЦБ РФ).

Идентификация угроз: фишинг, DDoS-атаки, утечки данных — правовые последствия.

Обязанность уведомления регуляторов (Роскомнадзор, ЦБ РФ, ФСТЭК) о фактах инцидентов.

Тема 4. Международное сотрудничество и юрисдикционные аспекты в Incident Response. УК-1.1

Трансграничный характер киберугроз: коллизионные вопросы и определение применимого права.

Международные договоры (Будапештская конвенция о киберпреступности) и позиция РФ.

Взаимодействие с зарубежными CERT/CSIRT при расследовании инцидентов.

Правовые ограничения при передаче данных через границу (трансграничная передача персональных данных).

Раздел 2. Процессуальные и практические аспекты расследования

Тема 5. Правовые режимы защиты информации и их влияние на реагирование. ПКо ОС-2.1

Правовой режим персональных данных (ФЗ-152): требования к обработке и последствия утечек.

Защита коммерческой тайны (ФЗ-98) в ходе расследования инцидентов.

Обеспечение безопасности критической информационной инфраструктуры (ФЗ-187).

Лицензирование и сертификация в области ИБ как превентивная мера.

Тема 6. Процессуальные основы сбора цифровых доказательств (Digital Forensics). ПКс-ИИ-3.1

Понятие электронного доказательства и его юридическая сила (УПК РФ, ГПК РФ).

Порядок фиксации инцидента: составление актов, протоколы осмотра места происшествия.

Применение ACPO Good Practice Guide и российских методик при работе с доказательствами.

Обеспечение цепочки хранения (Chain of Custody) и невмешательства в цифровую информацию.

Тема 7. Взаимодействие с правоохранительными органами и регуляторами. ПКо ОС-2.1

Порядок подачи заявления о киберпреступлении в правоохранительные органы.

Правовой статус специалиста и эксперта при расследовании компьютерных инцидентов.

Судебная компьютерно-техническая экспертиза: назначение, вопросы эксперту, оценка заключения.

Взаимодействие с ЦБ РФ при инцидентах в кредитно-финансовой сфере.

Тема 8. Юридическая ответственность за киберинциденты. УК-1.1

Уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание вредоносных программ (ст. 273 УК РФ).

Административная ответственность за нарушение требований по защите информации (КоАП РФ).

Гражданско-правовая ответственность: возмещение убытков, компенсация морального вреда.

Дисциплинарная ответственность сотрудников, допустивших инцидент.

Тема 9. Правовое обеспечение этапов сдерживания, ликвидации и восстановления. ПКо ОС-2.1

Правовые аспекты изоляции пораженных сегментов сети и временного ограничения доступа.

Защита прав третьих лиц при ликвидации последствий атаки.

Восстановление данных: лицензионная чистота ПО и регламенты резервного копирования.

Претензионная и исковая работа с контрагентами, пострадавшими от инцидента.

Тема 10. Compliance и совершенствование системы реагирования. ПКс-ИИ-3.1

Аудит системы реагирования на инциденты: правовые критерии оценки эффективности.

Разработка Post-Incident Report и корректирующие мероприятия.

Тенденции развития законодательства об ИИ и Big Data в контексте Incident Response.

Страхование киберрисков как механизм защиты и компенсации.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.02 «Правовая защита от киберугроз и инцидентов (Incident Response)» входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляют фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

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

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

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

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

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

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

4.4. Типы заданий, сценарии выполнения, критерии оценивания

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

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

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

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

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

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

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

5.1. В ходе реализации дисциплины Б1.В.02 «Правовая защита от киберугроз и инцидентов (Incident Response)» используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Устный опрос, ситуационная задача, тестирование.

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

Раздел 1. Теоретико-правовые основы реагирования на инциденты

Тема 1. Введение в правовое обеспечение кибербезопасности и Incident Response. УК-1.1

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;

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

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

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Понятие киберугрозы и инцидента информационной безопасности: правовая дефиниция и соотношение понятий.
2. Источники правового регулирования: международные стандарты (ISO/IEC 27035, NIST), российское законодательство (ФЗ «О безопасности», Доктрина ИБ РФ).
3. Национальное законодательство в сфере противодействия киберпреступности (гл. 28 УК РФ, КоАП РФ).
4. Роль права в управлении жизненным циклом инцидента: от обнаружения до извлечения уроков.

Ситуационные задачи.

Задача 1.

В организации ООО «Альфа» произошло событие: сотрудник отдела кадров по ошибке отправил файл с персональными данными всех сотрудников (зарплатные ведомости, паспортные данные) в открытый чат в мессенджере вместо личного сообщения коллеге. Информация находилась в открытом доступе 15 минут, пока сообщение не было удалено. За это время файл никто не скачал.

Можно ли данное событие квалифицировать как инцидент информационной безопасности? Какие правовые последствия это может повлечь?

Задача 2.

Системный администратор обнаружил в логах сервера многократные попытки подбора пароля к учетной записи директора (брутфорс-атака). Атака была заблокирована средствами защиты, несанкционированного доступа не произошло.

Является ли это событие инцидентом? Должна ли организация сообщать о нем в какие-либо органы?

Тема 2. Организационно-правовые основы формирования CSIRT (Команды реагирования). ПКо ОС-2.1

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;

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

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

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Понятие и правовой статус CSIRT (Computer Security Incident Response Team) в корпоративной структуре.

2. Разработка локальных нормативных актов: Политика управления инцидентами, Регламент взаимодействия CSIRT.

3. Разграничение ответственности между IT-отделом, службой безопасности и юридическим департаментом.

4. Трудовые отношения и конфиденциальность: обязательства сотрудников CSIRT о неразглашении (NDA).

Ситуационные задачи.

Задача 1.

В организации создана неформальная группа из системных администраторов, которые по звонку коллег помогают разбираться со сбоями и вирусами. Никаких документов, регламентирующих их деятельность, не существует. При серьезной атаке шифровальщика никто из них не взял на себя ответственность за координацию действий, в результате время простоя увеличилось.

Какие правовые риски выявила данная ситуация? Какие документы необходимо разработать?

Задача 2.

Сотрудник CSIRT М. при расследовании инцидента скопировал на личную флешку базу данных клиентов для удобного анализа дома. Флешка была утеряна в транспорте. В результате произошла утечка персональных данных.

Какие правовые последствия наступят для М. и для организации? Какие документы были нарушены?

Тема 3. Правовые аспекты выявления киберугроз и оценки рисков (Legal Risk Assessment). ПКс-ИИ-3.1

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;

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

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

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Категорирование активов и их правовая защита (государственная тайна, коммерческая тайна, персональные данные).
2. Правовая основа риск-ориентированного подхода (ФЗ-№184 «О техническом регулировании», стандарты ЦБ РФ).
3. Идентификация угроз: фишинг, DDoS-атаки, утечки данных — правовые последствия.
4. Обязанность уведомления регуляторов (Роскомнадзор, ЦБ РФ, ФСТЭК) о фактах инцидентов.

Ситуационные задачи.

Задача 3.1.
Интернет-магазин собирает персональные данные клиентов (ФИО, адрес, телефон) для доставки товаров. Магазин использует простую форму сбора на сайте без подтверждения согласия (стоит заранее проставленная галочка). Произошла утечка базы данных. *Какие нарушения в части получения согласия допустил магазин? Как это повлияет на правовую оценку инцидента?*

Задача 3.2.
Банк (субъект КИИ) оценивая риски, решил не внедрять дополнительную защиту для своей автоматизированной банковской системы, посчитав угрозу DDoS-атак маловероятной, хотя регулятор (ЦБ РФ) рекомендовал усилить защиту. Через месяц произошла мощная DDoS-атака, которая парализовала работу отделений на сутки.
Правильно ли банк оценил риски с правовой точки зрения? Какие правовые последствия наступят?

Тема 4. Международное сотрудничество и юрисдикционные аспекты в Incident Response. УК-1.1

Подготовка к практическому занятию:

- внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;
- подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;
- понять, что осталось неясными и постараться получить на них ответ заранее;
- готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Трансграничный характер киберугроз: коллизионные вопросы и определение применимого права.
2. Международные договоры (Будапештская конвенция о киберпреступности) и позиция РФ.
3. Взаимодействие с зарубежными CERT/CSIRT при расследовании инцидентов.
4. Правовые ограничения при передаче данных через границу (трансграничная передача персональных данных).

Ситуационные задачи.

Задача 4.1.
Российская компания использует облачный сервис американской компании (серверы находятся в США) для хранения персональных данных своих российских клиентов. Произошел инцидент: из-за уязвимости в облачном сервисе данные российских клиентов стали общедоступны в интернете.
К юрисдикции какой страны относится расследование этого инцидента? Какое право будет применяться к ответственности оператора (российской компании)?

Задача 4.2.
Российский хакер взломал сервер немецкой компании и похитил данные. Ущерб был причинен немецкой компании. Хакер был задержан в России.
Будет ли он привлечен к ответственности в России? Если да, то по какой статье и на основании каких норм?

Раздел 2. Процессуальные и практические аспекты расследования

Тема 5. Правовые режимы защиты информации и их влияние на реагирование. ПКо ОС-2.1

Подготовка к практическому занятию:

- внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;
- подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;
- понять, что осталось неясными и постараться получить на них ответ заранее;
- готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Правовой режим персональных данных (ФЗ-152): требования к обработке и последствия утечек.
2. Защита коммерческой тайны (ФЗ-98) в ходе расследования инцидентов.
3. Обеспечение безопасности критической информационной инфраструктуры (ФЗ-187).
4. Лицензирование и сертификация в области ИБ как превентивная мера.

Ситуационные задачи:

Задача 1.
В больнице (медицинское учреждение, оператор ПДн особой категории) произошла утечка электронных медицинских карт пациентов. Выяснилось, что доступ к системе был возможен по стандартному паролю, который не менялся 5 лет. Средства защиты информации не сертифицированы.

Какие требования ФЗ-152 и подзаконных актов нарушены? Как это повлияет на размер ответственности?

Задача 2.
Компания разработала новый уникальный алгоритм. Информация об алгоритме была размечена грифом «Коммерческая тайна» и лежала в общедоступной сетевой папке, к которой имели доступ все сотрудники отдела разработки. Специального приказа о введении режима коммерческой тайны и перечня сведений не было. Алгоритм был похищен конкурентом через скомпрометированный аккаунт уборщицы, имевшей доступ в офис.
Сможет ли компания защитить свои права и привлечь конкурента к ответственности за нарушение коммерческой тайны?

Тема 6. Процессуальные основы сбора цифровых доказательств (Digital Forensics). ПКс-ИИ-3.1

Подготовка к практическому занятию:

- внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;
- подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;
- понять, что осталось неясными и постараться получить на них ответ заранее;
- готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Понятие электронного доказательства и его юридическая сила (УПК РФ, ГПК РФ).
2. Порядок фиксации инцидента: составление актов, протоколы осмотра места происшествия.
3. Применение ACPO Good Practice Guide и российских методик при работе с доказательствами.
4. Обеспечение цепочки хранения (Chain of Custody) и невмешательства в цифровую информацию.

Ситуационные задачи.

Задача 1.
Системный администратор, обнаружив следы взлома, для анализа запустил антивирусную проверку на том же сервере (запись на диск), скопировал подозрительные файлы в другую папку на этом же сервере, а затем сделал их zip-архив и отправил начальнику по электронной почте.
Оцените действия администратора с точки зрения правил сбора цифровых доказательств. Какие ошибки допущены?

Задача 2.

Следователь изъял ноутбук подозреваемого. Для осмотра он привлек специалиста, который включил ноутбук и начал просматривать файлы через штатную операционную систему. Адвокат заявил протест.
Прав ли адвокат? Как следовало поступить?

Тема 7. Взаимодействие с правоохранительными органами и регуляторами. ПКо ОС-2.1

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;

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

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

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Порядок подачи заявления о киберпреступлении в правоохранительные органы.
2. Правовой статус специалиста и эксперта при расследовании компьютерных инцидентов.
3. Судебная компьютерно-техническая экспертиза: назначение, вопросы эксперту, оценка заключения.
4. Взаимодействие с ЦБ РФ при инцидентах в кредитно-финансовой сфере.

Ситуационные задачи.

Задача 1.
Банк обратился в полицию с заявлением о хищении 1 млн рублей со счетов клиентов через взлом системы ДБО. Следователь попросил предоставить логи серверов и рабочие станции сотрудников. Банк отказался выдать рабочие станции, сославшись на то, что там содержится банковская тайна и тайна иных клиентов.
Правомерен ли отказ банка? Как должен поступить следователь?

Задача 2.
По делу о DDoS-атаке на сайт госоргана назначена компьютерно-техническая экспертиза. Следователь поставил перед экспертом вопрос: «Кто совершил атаку?». Эксперт дал заключение, где указал имя конкретного человека.
Будет ли такое заключение иметь доказательственную силу?

Тема 8. Юридическая ответственность за киберинциденты. УК-1.1

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

- подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;
- понять, что осталось неясными и постараться получить на них ответ заранее;
- готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:
Вопросы для устного опроса:

1. Уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание вредоносных программ (ст. 273 УК РФ).
2. Административная ответственность за нарушение требований по защите информации (КоАП РФ).
3. Гражданско-правовая ответственность: возмещение убытков, компенсация морального вреда.
4. Дисциплинарная ответственность сотрудников, допустивших инцидент.

Ситуационные задачи.

Задача 1.
Начальник IT-отдела дал указание подчиненному скопировать базу данных клиентов конкурента для анализа. Подчиненный взломал защиту и скопировал данные. Начальник обещал заплатить подчиненному премию за это. Полиция задержала обоих. *Кто и какую ответственность понесет? Есть ли здесь соучастие?*

Задача 2.
Сотрудник уволился из компании и на следующий день разместил в своем блоге слайды с презентации нового продукта, над которым работал, сопроводив их критическими комментариями. В трудовом договоре было условие о неразглашении коммерческой тайны, с которым сотрудник был ознакомлен.
Какие виды ответственности могут быть применены к бывшему сотруднику?

Тема 9. Правовое обеспечение этапов сдерживания, ликвидации и восстановления. ПКо ОС-2.1

Подготовка к практическому занятию:
- внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;
- подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;
- понять, что осталось неясными и постараться получить на них ответ заранее;
- готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:
Вопросы для устного опроса:
1. Правовые аспекты изоляции пораженных сегментов сети и временного ограничения доступа.
2. Защита прав третьих лиц при ликвидации последствий атаки.

3. Восстановление данных: лицензионная чистота ПО и регламенты резервного копирования.
4. Претензионная и исковая работа с контрагентами, пострадавшими от инцидента.

Ситуационные задачи.

Тема 10. Compliance и совершенствование системы реагирования. ПКс-ИИ-3.1

Подготовка к практическому занятию:

- внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;
- подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;
- понять, что осталось неясными и постараться получить на них ответ заранее;
- готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:
Вопросы для устного опроса:
1. Аудит системы реагирования на инциденты: правовые критерии оценки эффективности.
2. Разработка Post-Incident Report и корректирующие мероприятия.
3. Тенденции развития законодательства об ИИ и Big Data в контексте Incident Response.
4. Страхование киберрисков как механизм защиты и компенсации.

Ситуационные задачи.

Задача 1.
Аудит системы реагирования на инциденты выявил, что 70% инцидентов в компании связаны с фишинговыми письмами. При этом обучение сотрудников проводилось один раз три года назад в виде рассылки памятки по электронной почте.
Какие корректирующие мероприятия (на основе риск-ориентированного подхода) следует предложить по итогам Post-Incident Report?

Задача 2.
Компания застраховала киберриски. Произошел инцидент: утечка данных из-за атаки на веб-сервер. Страховая компания запросила Post-Incident Report, акты внутреннего расследования и подтверждение, что все необходимые обновления безопасности (патчи) были установлены своевременно. Выяснилось, что критическое обновление, закрывающее уязвимость, через которую проникли хакеры, не было установлено, так как администратор «забыл».
Выплатит ли страховая компания возмещение?

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

Максимальное количество баллов за любой тип работ в рамках КТ составляет 100

(сто) баллов.

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

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

Формула расчета результата контрольной точки:

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

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

КТ – 1.

Тема 1-10.

Доклад.

Тематика докладов:

Раздел 1. Теоретико-правовые основы реагирования на инциденты

Тема 1. Введение в правовое обеспечение кибербезопасности и Incident Response. УК-1.1

1. Понятие киберугрозы и инцидента информационной безопасности: правовая дефиниция и соотношение понятий.
2. Источники правового регулирования: международные стандарты (ISO/IEC 27035, NIST), российское законодательство (ФЗ «О безопасности», Доктрина ИБ РФ).
3. Национальное законодательство в сфере противодействия киберпреступности (гл. 28 УК РФ, КоАП РФ).
4. Роль права в управлении жизненным циклом инцидента: от обнаружения до извлечения уроков.

Тема 2. Организационно-правовые основы формирования CSIRT (Команды реагирования). ПКо ОС-2.1

5. Понятие и правовой статус CSIRT (Computer Security Incident Response Team) в корпоративной структуре.
6. Разработка локальных нормативных актов: Политика управления инцидентами, Регламент взаимодействия CSIRT.
7. Разграничение ответственности между IT-отделом, службой безопасности и юридическим департаментом.
8. Трудовые отношения и конфиденциальность: обязательства сотрудников CSIRT о неразглашении (NDA).

Тема 3. Правовые аспекты выявления киберугроз и оценки рисков (Legal Risk Assessment). ПКс-ИИ-3.1

9. Категорирование активов и их правовая защита (государственная тайна, коммерческая тайна, персональные данные).

10. Правовая основа риск-ориентированного подхода (ФЗ-№184 «О техническом регулировании», стандарты ЦБ РФ).

11. Идентификация угроз: фишинг, DDoS-атаки, утечки данных — правовые последствия.

12. Обязанность уведомления регуляторов (Роскомнадзор, ЦБ РФ, ФСТЭК) о фактах инцидентов.

Тема 4. Международное сотрудничество и юрисдикционные аспекты в Incident Response. УК-1.1

13. Трансграничный характер киберугроз: коллизионные вопросы и определение применимого права.

14. Международные договоры (Будапештская конвенция о киберпреступности) и позиция РФ.

15. Взаимодействие с зарубежными CERT/CSIRT при расследовании инцидентов.

16. Правовые ограничения при передаче данных через границу (трансграничная передача персональных данных).

Раздел 2. Процессуальные и практические аспекты расследования

Тема 5. Правовые режимы защиты информации и их влияние на реагирование. ПКо ОС-2.1

17. Правовой режим персональных данных (ФЗ-152): требования к обработке и последствия утечек.

18. Защита коммерческой тайны (ФЗ-98) в ходе расследования инцидентов.

19. Обеспечение безопасности критической информационной инфраструктуры (ФЗ-187).

20. Лицензирование и сертификация в области ИБ как превентивная мера.

Тема 6. Процессуальные основы сбора цифровых доказательств (Digital Forensics). ПКс-ИИ-3.1

21. Понятие электронного доказательства и его юридическая сила (УПК РФ, ГПК РФ).

22. Порядок фиксации инцидента: составление актов, протоколы осмотра места происшествия.

23. Применение ACPO Good Practice Guide и российских методик при работе с доказательствами.

24. Обеспечение цепочки хранения (Chain of Custody) и невмешательства в цифровую информацию.

Тема 7. Взаимодействие с правоохранительными органами и регуляторами. ПКо ОС-2.1

25. Порядок подачи заявления о киберпреступлении в правоохранительные органы.

26. Правовой статус специалиста и эксперта при расследовании компьютерных инцидентов.

27. Судебная компьютерно-техническая экспертиза: назначение, вопросы эксперту, оценка заключения.

28. Взаимодействие с ЦБ РФ при инцидентах в кредитно-финансовой сфере.

Тема 8. Юридическая ответственность за киберинциденты. УК-1.1

29. Уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание вредоносных программ (ст. 273 УК РФ).

30. Административная ответственность за нарушение требований по защите информации (КоАП РФ).

31. Гражданско-правовая ответственность: возмещение убытков, компенсация морального вреда.

32. Дисциплинарная ответственность сотрудников, допустивших инцидент.

Тема 9. Правовое обеспечение этапов сдерживания, ликвидации и восстановления. ПКо ОС-2.1

33. Правовые аспекты изоляции пораженных сегментов сети и временного ограничения доступа.
34. Защита прав третьих лиц при ликвидации последствий атаки.
35. Восстановление данных: лицензионная чистота ПО и регламенты резервного копирования.
36. Претензионная и исковая работа с контрагентами, пострадавшими от инцидента.

Тема 10. Compliance и совершенствование системы реагирования. ПКс-ИИ-3.1

37. Аудит системы реагирования на инциденты: правовые критерии оценки эффективности.
38. Разработка Post-Incident Report и корректирующие мероприятия.
39. Тенденции развития законодательства об ИИ и Big Data в контексте Incident Response.
40. Страхование киберрисков как механизм защиты и компенсации.

Методические рекомендации по подготовке доклада.

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

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

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

Критерии оценивания доклада:

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

Логика изложения	0-20	Чёткая последовательность изложения, логические связи между частями текста, аргументы подтверждают выводы
Оригинальность	0-20	Уникальный подход к теме, нестандартные решения, инновационные идеи, собственная позиция автора
Итого максимально:	100	

КТ – 2.

Темы 1-10
Устный опрос:

Вопросы для опроса:

№ п.п.	Содержание вопроса
1.	Понятие киберугрозы и инцидента информационной безопасности: правовая дефиниция и соотношение понятий.
2.	Источники правового регулирования: международные стандарты (ISO/IEC 27035, NIST), российское законодательство (ФЗ «О безопасности», Доктрина ИБ РФ).
3.	Национальное законодательство в сфере противодействия киберпреступности (гл. 28 УК РФ, КоАП РФ).
4.	Понятие и правовой статус CSIRT (Computer Security Incident Response Team) в корпоративной структуре.
5.	Разработка локальных нормативных актов: Политика управления инцидентами, Регламент взаимодействия CSIRT.
6.	Трудовые отношения и конфиденциальность: обязательства сотрудников CSIRT о неразглашении (NDA).
7.	Категорирование активов и их правовая защита (государственная тайна, коммерческая тайна, персональные данные).
8.	Правовая основа риск-ориентированного подхода (ФЗ-№184 «О техническом регулировании», стандарты ЦБ РФ).
9.	Идентификация угроз: фишинг, DDoS-атаки, утечки данных — правовые последствия.
10.	Трансграничный характер киберугроз: коллизионные вопросы и определение применимого права.
11.	Международные договоры (Будапештская конвенция о киберпреступности) и позиция РФ.
12.	Взаимодействие с зарубежными CERT/CSIRT при расследовании инцидентов.
13.	13. Правовые ограничения при передаче данных через границу (трансграничная передача персональных данных).
14.	14. Правовой режим персональных данных (ФЗ-152): требования к обработке и последствия утечек.
15.	Защита коммерческой тайны (ФЗ-98) в ходе расследования инцидентов.
16.	Обеспечение безопасности критической информационной инфраструктуры (ФЗ-187).
17.	Лицензирование и сертификация в области ИБ как превентивная мера.

18.	Понятие электронного доказательства и его юридическая сила (УПК РФ, ГПК РФ).
19.	Порядок фиксации инцидента: составление актов, протоколы осмотра места происшествия.
20.	Порядок подачи заявления о киберпреступлении в правоохранительные органы.
21.	Правовой статус специалиста и эксперта при расследовании компьютерных инцидентов.
22.	Судебная компьютерно-техническая экспертиза: назначение, вопросы эксперту, оценка заключения.
23.	Уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание вредоносных программ (ст. 273 УК РФ).
24.	Административная ответственность за нарушение требований по защите информации (КоАП РФ).
25.	Гражданско-правовая ответственность: возмещение убытков, компенсация морального вреда.
26.	Защита прав третьих лиц при ликвидации последствий атаки.
27.	Восстановление данных: лицензионная чистота ПО и регламенты резервного копирования.
28.	Аудит системы реагирования на инциденты: правовые критерии оценки эффективности.
29.	Тенденции развития законодательства об ИИ и Big Data в контексте Incident Response.
30.	Страхование киберрисков как механизм защиты и компенсации.

Критерии оценивания опроса:

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

КТ – 3.

Темы 1-10

Тестирование

1. Что понимается под инцидентом информационной безопасности в соответствии с правовыми подходами?

1. Потенциальная возможность нарушения безопасности информации
2. Любое событие, которое привело к фактическому нарушению безопасности информации (конфиденциальности, целостности, доступности)
3. Наличие уязвимости в программном обеспечении
4. Проведение плановых работ по обновлению систем защиты

2. Какой международный стандарт содержит рекомендации по управлению инцидентами информационной безопасности?

1. ISO 9001
2. ISO/IEC 27035
3. PCI DSS
4. COBIT 5

3. Что означает аббревиатура CSIRT?

1. Computer Security Incident Response Team
2. Central Security Information Response Tool
3. Cyber Systems Incident Reporting Team
4. Corporate Security Intelligence and Response Team

4. Какой локальный нормативный акт определяет цели, задачи и общие принципы реагирования на инциденты в организации?

1. Должностная инструкция системного администратора
2. Политика управления инцидентами информационной безопасности
3. Правила внутреннего трудового распорядка
4. Устав организации

5. К какой категории информации предъявляются наиболее строгие требования по защите в соответствии с ФЗ-152?

1. Общедоступная информация
2. Коммерческая тайна
3. Персональные данные
4. Служебная информация ограниченного распространения

6. В каком нормативном акте реализован риск-ориентированный подход при определении уровня защищенности персональных данных?

1. ФЗ-184 «О техническом регулировании»
2. Постановление Правительства РФ № 1119
3. Уголовный кодекс РФ
4. Трудовой кодекс РФ

7. Какова позиция Российской Федерации в отношении Будапештской конвенции о киберпреступности?

1. Россия является полноправным участником и ратифицировала конвенцию
2. Россия подписала, но не ратифицировала конвенцию, развивая собственные механизмы сотрудничества
3. Россия категорически отвергает конвенцию и не участвует в ней
4. Россия вышла из конвенции в 2022 году

8. При каком условии допустима трансграничная передача персональных данных в страну, не обеспечивающую адекватной защиты прав субъектов?

1. При любых обстоятельствах
2. При наличии письменного согласия субъекта персональных данных
3. Если это решит оператор

4. При уведомлении Роскомнадзора

9. Какой федеральный закон устанавливает правовой режим персональных данных?

1. ФЗ-149 «Об информации...»
2. ФЗ-152 «О персональных данных»
3. ФЗ-98 «О коммерческой тайне»
4. ФЗ-187 «О безопасности КИИ»

10. Какое условие является обязательным для признания информации коммерческой тайной в суде?

1. Наличие грифа «Коммерческая тайна» на документах
2. Введение в организации режима коммерческой тайны (перечень, гриф, учет доступа)
3. Желание руководителя
4. Наличие патента

11. В каком кодексе РФ закреплено, что документы, полученные в электронной форме, могут признаваться письменными доказательствами?

1. Только в УПК РФ
2. Только в ГПК РФ и АПК РФ
3. Во всех процессуальных кодексах (УПК, ГПК, АПК, КАС)
4. Только в КоАП РФ

12. Какой документ составляется следователем при осмотре места происшествия по факту киберинцидента?

1. Акт внутреннего расследования
2. Протокол осмотра места происшествия
3. Экспертное заключение
4. Справка об инциденте

13. Куда подается заявление о киберпреступлении в Российской Федерации?

1. Только в прокуратуру
2. В территориальный орган МВД России (полицию)
3. В Роскомнадзор
4. В ФСБ России (по любому киберпреступлению)

14. Кто назначает судебную компьютерно-техническую экспертизу?

1. Только суд
2. Следователь или суд (на основании постановления/определения)
3. Руководитель организации-заявителя
4. Эксперт по собственной инициативе

15. Какое наказание предусмотрено ч. 1 ст. 273 УК РФ за создание вредоносных компьютерных программ?

1. Только штраф
2. Только обязательные работы
3. Лишение свободы на срок до 4 лет
4. Административный арест

16. Какая статья КоАП РФ устанавливает ответственность за нарушение порядка обработки персональных данных?

1. Ст. 13.11
2. Ст. 13.12
3. Ст. 13.13
4. Ст. 13.14

17. Обязана ли организация уведомлять третьих лиц (контрагентов), если инцидент затронул их данные?

1. Нет, это внутреннее дело организации
2. Да, в разумных пределах, не нарушая конфиденциальность расследования
3. Только по требованию суда

4. Только если третьи лица сами запросят информацию

18. Какое требование предъявляется к программному обеспечению, используемому для восстановления данных из резервных копий?

1. Оно должно быть бесплатным
2. Оно должно быть лицензионным
3. Оно должно быть только российским
4. Оно должно быть одобрено ФСБ

19. Какая тенденция в законодательстве об ИИ влияет на Incident Response?

1. Полный запрет на использование ИИ
2. Необходимость учета «прозрачности» алгоритмов при расследовании инцидентов с участием ИИ
3. Отмена всех требований к ИИ
4. Передача всех функций реагирования ИИ

20. Какие расходы могут покрываться полисом киберстрахования?

1. Только штрафы регуляторов
2. Только упущенная выгода
3. Расходы на расследование, юридические услуги, выплаты пострадавшим, убытки от простоя
4. Только затраты на новое оборудование

Критерии оценивания тестовых заданий:

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

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

Для ответа на вопросы студенту разрешается использование нормативно-правовых актов.

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

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

6.2. Типовые оценочные материалы промежуточной аттестации

Типовые проверочные задания для самоподготовки обучающегося к промежуточной

аттестации:

Раздел 1. Теоретико-правовые основы реагирования на инциденты

Тема 1. Введение в правовое обеспечение кибербезопасности и Incident Response. УК-1.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Понятие киберугрозы и инцидента информационной безопасности: правовая дефиниция и соотношение понятий.
2.	Источники правового регулирования: международные стандарты (ISO/IEC 27035, NIST), российское законодательство (ФЗ «О безопасности», Доктрина ИБ РФ).
3.	Национальное законодательство в сфере противодействия киберпреступности (гл. 28 УК РФ, КоАП РФ).
4.	Роль права в управлении жизненным циклом инцидента: от обнаружения до извлечения уроков.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Соотношение понятий «киберугроза» и «инцидент информационной безопасности» наиболее точно определяется как: а) это синонимичные понятия, обозначающие одно и то же; б) киберугроза — это реализованный инцидент, а инцидент — потенциальная возможность; в) киберугроза — это потенциальная возможность нарушения безопасности, а инцидент — факт реализации этой возможности; г) инцидент — это всегда следствие киберугрозы, но киберугроза не всегда ведет к		

	инциденту.		
2.	К источникам правового регулирования в сфере противодействия киберугрозам в Российской Федерации относятся: а) только Уголовный кодекс РФ и КоАП РФ; б) Доктрина информационной безопасности РФ, ФЗ «Об информации...», глава 28 УК РФ, а также подзаконные акты ФСТЭК и ФСБ; в) исключительно международные договоры и конвенции; г) только локальные нормативные акты коммерческих организаций.		

3. Задания закрытого типа.

Тестовые задания.

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.

Записать только цифру выбранного варианта ответа.

1. Что понимается под инцидентом информационной безопасности в соответствии с правовыми подходами?

5. Потенциальная возможность нарушения безопасности информации
6. Любое событие, которое привело к фактическому нарушению безопасности информации (конфиденциальности, целостности, доступности)
7. Наличие уязвимости в программном обеспечении
8. Проведение плановых работ по обновлению систем защиты

2. Какой международный стандарт содержит рекомендации по управлению инцидентами информационной безопасности?

5. ISO 9001
6. ISO/IEC 27035
7. PCI DSS
8. COBIT 5

3. Какая глава Уголовного кодекса РФ устанавливает ответственность за преступления в сфере компьютерной информации?

1. Глава 21
2. Глава 24

3. Глава 28
4. Глава 30

4. На каком этапе жизненного цикла инцидента право играет ключевую роль в обеспечении законности сбора доказательств?

1. Только на этапе обнаружения
2. Только на этапе ликвидации
3. На всех этапах, но особенно на этапе расследования (сбор доказательств)
   Только на этапе извлечения уроков

Тема 2. Организационно-правовые основы формирования CSIRT (Команды реагирования). ПКо ОС-2.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Понятие и правовой статус CSIRT (Computer Security Incident Response Team) в корпоративной структуре.
2.	Разработка локальных нормативных актов: Политика управления инцидентами, Регламент взаимодействия CSIRT.
3.	Разграничение ответственности между IT-отделом, службой безопасности и юридическим департаментом.
4.	Трудовые отношения и конфиденциальность: обязательства сотрудников CSIRT о неразглашении (NDA).

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Правовой статус CSIRT в корпоративной структуре закрепляется: а) устным распоряжением руководителя IT-отдела; б) приказом о создании подразделения, Положением о CSIRT и должностными инструкциями сотрудников; в) записью в трудовой книжке сотрудника; г) протоколом общего собрания акционеров.		
2.	Сотрудник CSIRT при приеме на работу подписывает обязательство о неразглашении (NDA). Это необходимо для:		

	а) соблюдения требований трудового законодательства об испытательном сроке; б) юридического закрепления обязанности сохранять конфиденциальность информации, ставшей известной в ходе реагирования на инциденты; в) получения доступа к сети Интернет; г) оформления пропуска в офис.		

3. Задания закрытого типа.

Тестовые задания.

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.

Записать только цифру выбранного варианта ответа.

1. Что означает аббревиатура CSIRT?

5. Computer Security Incident Response Team
6. Central Security Information Response Tool
7. Cyber Systems Incident Reporting Team
8. Corporate Security Intelligence and Response Team

2. Какой локальный нормативный акт определяет цели, задачи и общие принципы реагирования на инциденты в организации?

5. Должностная инструкция системного администратора
6. Политика управления инцидентами информационной безопасности
7. Правила внутреннего трудового распорядка
8. Устав организации

3. Какое подразделение в организации обычно отвечает за правовую квалификацию инцидента и взаимодействие с регуляторами?

1. IT-отдел
2. Служба безопасности
3. Юридический департамент
4. Отдел кадров

4. Какой документ регулирует обязательства сотрудника о неразглашении информации, полученной в ходе работы в CSIRT?

1. Трудовой договор (в части NDA)
2. Заявление о приеме на работу
3. График отпусков

4. Положение о премировании

Тема 3. Правовые аспекты выявления киберугроз и оценки рисков (Legal Risk Assessment). ПКс-ИИ-3.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Категорирование активов и их правовая защита (государственная тайна, коммерческая тайна, персональные данные).
2.	Правовая основа риск-ориентированного подхода (ФЗ-№184 «О техническом регулировании», стандарты ЦБ РФ).
3.	Идентификация угроз: фишинг, DDoS-атаки, утечки данных — правовые последствия.
4.	Обязанность уведомления регуляторов (Роскомнадзор, ЦБ РФ, ФСТЭК) о фактах инцидентов.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Категорирование информационных активов организации (выделение государственной тайны, коммерческой тайны, персональных данных) необходимо для: а) определения стоимости активов для бухгалтерского учета; б) применения адекватных правовых режимов защиты и корректной квалификации последствий инцидента; в) повышения заработной платы сотрудникам; г) украшения отчетности.		
2.	Риск-ориентированный подход в ФЗ-152 «О персональных данных» означает: а) одинаковые требования ко всем операторам независимо от объема данных; б) зависимость объема требований к защите от возможного вреда субъектам персональных данных;		

	в) полную свободу оператора в выборе мер защиты; г) обязанность страховать все риски.		

3. Задания закрытого типа.

Тестовые задания.

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.

Записать только цифру выбранного варианта ответа.

1. К какой категории информации предъявляются наиболее строгие требования по защите в соответствии с ФЗ-152?

5. Общедоступная информация
6. Коммерческая тайна
7. Персональные данные
8. Служебная информация ограниченного распространения

2. В каком нормативном акте реализован риск-ориентированный подход при определении уровня защищенности персональных данных?

5. ФЗ-184 «О техническом регулировании»
6. Постановление Правительства РФ № 1119
7. Уголовный кодекс РФ
8. Трудовой кодекс РФ

3. Какие правовые последствия могут наступить для организации в результате утечки персональных данных?

1. Только административная ответственность
2. Только гражданско-правовая ответственность
3. Административная, гражданско-правовая и репутационная ответственность
4. Только дисциплинарная ответственность сотрудников

4. В какой срок оператор обязан уведомить Роскомнадзор о факте утечки персональных данных?

1. В течение 72 часов
2. В течение 24 часов
3. В течение 7 дней
4. В течение 3 дней с момента окончания расследования

Тема 4. Международное сотрудничество и юрисдикционные аспекты в Incident Response. УК-1.1

1. Задания открытого типа.

№	Вопрос

п.п.	
1.	Трансграничный характер киберугроз: коллизионные вопросы и определение применимого права.
2.	Международные договоры (Будапештская конвенция о киберпреступности) и позиция РФ.
3.	Взаимодействие с зарубежными CERT/CSIRT при расследовании инцидентов.
4.	Правовые ограничения при передаче данных через границу (трансграничная передача персональных данных).

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	При трансграничной кибератаке, когда атакующий находился в стране А, серверы — в стране Б, а пострадавший (российская компания) — в РФ, применимое право (согласно ст. 11 УК РФ) будет определяться: а) по праву страны А (местонахождение атакующего); б) по праву страны Б (местонахождение серверов); в) по праву РФ, так как вредные последствия наступили на территории РФ; г) по международному праву.		
2.	Российская организация (оператор ПДн) в ходе расследования инцидента хочет передать зарубежному партнеру логи, содержащие персональные данные европейских клиентов. Страна партнера не входит в перечень стран с адекватной защитой. Это возможно: а) всегда, так как это необходимо для расследования; б) только с письменного согласия каждого субъекта персональных данных, чьи данные передаются; в) по устному запросу партнера; г) без каких-либо		

	ограничений.		

3. Задания закрытого типа.

Тестовые задания.

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.

Записать только цифру выбранного варианта ответа.

1. Какой принцип определения применимого права закреплен в ст. 11 УК РФ для случаев киберпреступлений?

1. Принцип гражданства атакующего
2. Принцип территориальности (место совершения преступления или наступления последствий)
3. Принцип большинства голосов
4. Принцип lex mercatoria

2. Какова позиция Российской Федерации в отношении Будапештской конвенции о киберпреступности?

5. Россия является полноправным участником и ратифицировала конвенцию
6. Россия подписала, но не ратифицировала конвенцию, развивая собственные механизмы сотрудничества
7. Россия категорически отвергает конвенцию и не участвует в ней
8. Россия вышла из конвенции в 2022 году

3. В каком формате чаще всего осуществляется оперативный обмен технической информацией с зарубежными CERT?

1. Через официальные дипломатические ноты
2. Через международные объединения типа FIRST на основе меморандумов
3. Через Интерпол
4. Через ООН

4. При каком условии допустима трансграничная передача персональных данных в страну, не обеспечивающую адекватной защиты прав субъектов?

5. При любых обстоятельствах
6. При наличии письменного согласия субъекта персональных данных
7. Если это решит оператор
8. При уведомлении Роскомнадзора

Раздел 2. Процессуальные и практические аспекты расследования

Тема 5. Правовые режимы защиты информации и их влияние на реагирование. ПКо ОС-2.1

1. Задания открытого типа.

№ п.п.	Вопрос

1.	Правовой режим персональных данных (ФЗ-152): требования к обработке и последствия утечек.
2.	Защита коммерческой тайны (ФЗ-98) в ходе расследования инцидентов.
3.	Обеспечение безопасности критической информационной инфраструктуры (ФЗ-187).
4.	Лицензирование и сертификация в области ИБ как превентивная мера.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	В результате инцидента произошла утечка базы данных клиентов (ФИО, паспортные данные, телефоны). Организация не получила письменного согласия на обработку паспортных данных. В отношении организации: а) никаких последствий не будет, так как утечка — это случайность; б) может быть применена административная ответственность по ст. 13.11 КоАП РФ за обработку ПДн без согласия и за их разглашение; в) ответственность наступит только для технического директора; г) дело будет передано в суд присяжных.		
2.	Организация, являющаяся субъектом КИИ, не уведомила ФСТЭК об инциденте, приведшем к отказу системы управления технологическим процессом. Это деяние: а) не является нарушением, так как можно уведомить позже; б) является административным правонарушением (ст. 13.12.1 КоАП РФ), а при наличии тяжких последствий может содержать признаки уголовного преступления (ст. 274.1 УК РФ);		

	в) влечет только дисциплинарную ответственность; г) наказывается лишением свободы до 15 лет в любом случае.		

3. Задания закрытого типа.

Тестовые задания.

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.

Записать только цифру выбранного варианта ответа.

1. Какой федеральный закон устанавливает правовой режим персональных данных?

5. ФЗ-149 «Об информации...»
6. ФЗ-152 «О персональных данных»
7. ФЗ-98 «О коммерческой тайне»
8. ФЗ-187 «О безопасности КИИ»

Правильный ответ: 2

2. Какое условие является обязательным для признания информации коммерческой тайной в суде?

5. Наличие грифа «Коммерческая тайна» на документах
6. Введение в организации режима коммерческой тайны (перечень, гриф, учет доступа)
7. Желание руководителя
8. Наличие патента

Правильный ответ: 2

3. На какие объекты распространяется действие ФЗ-187 «О безопасности критической информационной инфраструктуры РФ»?

1. На все коммерческие организации
2. На государственные органы и компании оборонной, банковской, энергетической сфер (субъекты КИИ)
3. Только на объекты Минобороны
4. На организации, работающие с персональными данными

Правильный ответ: 2

4. Кто выдает лицензии на деятельность по технической защите конфиденциальной информации?

1. Минцифры
2. Роскомнадзор
3. ФСТЭК России
4. Роспатент

Тема 6. Процессуальные основы сбора цифровых доказательств (Digital Forensics). ПКс-ИИ-3.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Понятие электронного доказательства и его юридическая сила (УПК РФ, ГПК РФ).
2.	Порядок фиксации инцидента: составление актов, протоколы осмотра места происшествия.
3.	Применение ACPO Good Practice Guide и российских методик при работе с доказательствами.
4.	Обеспечение цепочки хранения (Chain of Custody) и невмешательства в цифровую информацию.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Системный администратор компании при осмотре жесткого диска (оригинала) на предмет поиска вредоносного ПО вносит изменения в служебные области файловой системы. С точки зрения компьютерной криминалистики: а) это допустимо, если изменения незначительны; б) это недопустимо, нарушен принцип неизменности данных (работы только с копиями); в) это допустимо, если есть разрешение начальника; г) это обязательно для ускорения поиска.		
2.	Следователь при осмотре компьютера изъял системный блок и передал его эксперту без составления акта приема-передачи, не зафиксировав контрольные суммы (хэши). В суде адвокат заявил ходатайство об исключении доказательства. Суд, скорее всего: а) не примет во внимание это заявление; б) признает доказательство недопустимым, так как нарушена цепочка хранения		

	(Chain of Custody); в) назначит повторную экспертизу; г) вынесет частное определение следователю.		

3. Задания закрытого типа.

Тестовые задания.

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.

Записать только цифру выбранного варианта ответа.

1. В каком кодексе РФ закреплено, что документы, полученные в электронной форме, могут признаваться письменными доказательствами?

5. Только в УПК РФ
6. Только в ГПК РФ и АПК РФ
7. Во всех процессуальных кодексах (УПК, ГПК, АПК, КАС)
8. Только в КоАП РФ

2. Какой документ составляется следователем при осмотре места происшествия по факту киберинцидента?

5. Акт внутреннего расследования
6. Протокол осмотра места происшествия
7. Экспертное заключение
8. Справка об инциденте

3. Какой из принципов ACPO Good Practice Guide требует работы только с копиями данных, а не с оригиналами?

1. Принцип компетентности
2. Принцип неизменности данных
3. Принцип цепочки хранения
4. Принцип ответственности

4. Что означает понятие «цепочка хранения» (Chain of Custody) в компьютерной криминалистике?

1. Физическое хранение серверов в сейфе
2. Документированная история перемещения и работы с цифровым носителем или данными
3. Шифрование данных при передаче
4. Резервное копирование информации

Тема 7. Взаимодействие с правоохранительными органами и регуляторами. ПКо ОС-2.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Порядок подачи заявления о киберпреступлении в правоохранительные органы.
2.	Правовой статус специалиста и эксперта при расследовании компьютерных инцидентов.
3.	Судебная компьютерно-техническая экспертиза: назначение, вопросы эксперту, оценка заключения.
4.	Взаимодействие с ЦБ РФ при инцидентах в кредитно-финансовой сфере.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Организация обнаружила, что неизвестные взломали сервер и похитили базу данных. Для возбуждения уголовного дела юрист организации должен подать заявление в полицию. Что необходимо приложить к заявлению для повышения шансов на возбуждение дела? а) ничего, полиция разберется сама; б) акт внутреннего расследования, логи, скриншоты, объяснения сотрудников, расчет предполагаемого ущерба; в) только копию паспорта директора; г) гарантийное письмо об оплате услуг полиции.		
2.	В ходе расследования уголовного дела следователь назначает компьютерно-техническую экспертизу. Эксперт дает заключение, в котором указывает на наличие вредоносного ПО. Следователь: а) обязан принять заключение как истину; б) должен оценить заключение в совокупности с другими доказательствами, проверив его полноту и обоснованность; в) обязан назначить повторную экспертизу; г) не имеет права читать		

	заключение без понятых.		

3. Задания закрытого типа.

Тестовые задания.

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.

Записать только цифру выбранного варианта ответа.

1. Куда подается заявление о киберпреступлении в Российской Федерации?

5. Только в прокуратуру
6. В территориальный орган МВД России (полицию)
7. В Роскомнадзор
8. В ФСБ России (по любому киберпреступлению)

2. Чем отличается статус специалиста от статуса эксперта в уголовном процессе?

1. Специалист проводит исследование и дает заключение, эксперт помогает в ходе следствия
2. Эксперт назначается для проведения исследования и дает заключение, специалист помогает в обнаружении и изъятии
3. Ничем, это одно и то же лицо
4. Эксперт привлекается только защитой, специалист — только обвинением

3. Кто назначает судебную компьютерно-техническую экспертизу?

5. Только суд
6. Следователь или суд (на основании постановления/определения)
7. Руководитель организации-заявителя
8. Эксперт по собственной инициативе

4. В какой орган обязаны сообщать об инцидентах организации кредитно-финансовой сферы?

1. В Роскомнадзор
2. В ФСТЭК
3. В Центральный банк РФ (ФинЦЕРТ)
4. В Минфин

Тема 8. Юридическая ответственность за киберинциденты. УК-1.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание вредоносных программ (ст. 273 УК РФ).
2.	Административная ответственность за нарушение требований по защите информации (КоАП РФ).
3.	Гражданско-правовая ответственность: возмещение убытков, компенсация

	морального вреда.
4.	Дисциплинарная ответственность сотрудников, допустивших инцидент.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Программист создал вредоносную программу для скрытого майнинга криптовалюты, но еще не успел ее распространить. Он был задержан. Подлежит ли он уголовной ответственности по ст. 273 УК РФ? а) нет, так как нет последствий (никто не пострадал); б) да, так как состав преступления по ст. 273 УК РФ является формальным (достаточно самого факта создания); в) да, но только как покушение; г) нет, это административное правонарушение.		
2.	В результате халатных действий сотрудника (не установил обновление безопасности) произошло заражение шифровальщиком, что привело к простою производства и убыткам в 5 млн рублей. Сотрудник может быть привлечен: а) только к уголовной ответственности; б) к дисциплинарной ответственности (вплоть до увольнения), а также возможно взыскание материального ущерба в ограниченном размере (если нет оснований для полной материальной ответственности); в) только к административной ответственности; г) ни к какой, так как он действовал в интересах		

	компании.		

3. Задания закрытого типа.

Тестовые задания.

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.

Записать только цифру выбранного варианта ответа.

1. Какое наказание предусмотрено ч. 1 ст. 273 УК РФ за создание вредоносных компьютерных программ?

5. Только штраф
6. Только обязательные работы
7. Лишение свободы на срок до 4 лет
8. Административный арест

2. Какая статья КоАП РФ устанавливает ответственность за нарушение порядка обработки персональных данных?

5. Ст. 13.11
6. Ст. 13.12
7. Ст. 13.13
8. Ст. 13.14

3. В соответствии со ст. 15 ГК РФ убытки включают в себя:

1. Только реальный ущерб
2. Только упущенную выгоду
3. Реальный ущерб и упущенную выгоду
4. Только моральный вред

4. По какому основанию ТК РФ возможно увольнение сотрудника за разглашение данных, ставших известными в связи с инцидентом?

1. За прогул (пп. «а» п. 6 ст. 81)
2. За разглашение охраняемой законом тайны (пп. «в» п. 6 ст. 81)
3. За появление на работе в нетрезвом виде (пп. «б» п. 6 ст. 81)
4. За неисполнение трудовых обязанностей (ст. 192)

Тема 9. Правовое обеспечение этапов сдерживания, ликвидации и восстановления. ПКо ОС-2.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Правовые аспекты изоляции пораженных сегментов сети и временного ограничения доступа.

2.	Защита прав третьих лиц при ликвидации последствий атаки.
3.	Восстановление данных: лицензионная чистота ПО и регламенты резервного копирования.
4.	Претензионная и исковая работа с контрагентами, пострадавшими от инцидента.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	В ходе отражения DDoS-атаки администратор принял решение вручную отключить от сети сервер с критической базой данных, чтобы сохранить ее целостность. Простой сервера длился 6 часов, что привело к срыву поставок клиентам. Оцените правомерность действий администратора. а) действия неправомерны, так как любое отключение должно быть оформлено приказом руководителя; если приказа не было, администратор может нести дисциплинарную ответственность за простой; б) действия абсолютно правомерны в любой ситуации; в) действия правомерны, если они соответствуют утвержденному регламенту реагирования или администратор действовал в состоянии крайней необходимости (ст. 2.7 КоАП), но факт и причины отключения должны быть задокументированы постфактум; г) действия незаконны и влекут уголовную ответственность.		
2.	После восстановления системы из резервной копии выяснилось, что используемое для восстановления ПО не имеет лицензии (взято с торрента), так как		

	лицензионный ключ был утерян при атаке. Какие риски возникают у организации? а) никаких, главное — восстановить данные; б) риск привлечения к административной ответственности по ст. 7.12 КоАП РФ за использование нелицензионного ПО; в) риск уголовной ответственности по ст. 146 УК РФ при определенных условиях; г) верны варианты б и в.		

3. Задания закрытого типа.

Тестовые задания.

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.

Записать только цифру выбранного варианта ответа.

1. Чем должно быть оформлено решение об изоляции сегмента сети для придания ему законности?

1. Устным распоряжением администратора
2. Внутренним распорядительным актом (приказом) с указанием причин
3. Решением общего собрания работников
4. Ничем не оформляется

2. Обязана ли организация уведомлять третьих лиц (контрагентов), если инцидент затронул их данные?

5. Нет, это внутреннее дело организации
6. Да, в разумных пределах, не нарушая конфиденциальность расследования
7. Только по требованию суда
8. Только если третьи лица сами запросят информацию

3. Какое требование предъявляется к программному обеспечению, используемому для восстановления данных из резервных копий?

5. Оно должно быть бесплатным
6. Оно должно быть лицензионным
7. Оно должно быть только российским
8. Оно должно быть одобрено ФСБ

4. Что обязан сделать контрагент, прежде чем обратиться в суд с иском о возмещении убытков от инцидента?

1. Обратиться в СМИ
2. Соблюсти претензионный порядок (направить претензию)
3. Получить справку из полиции

4. Ничего, можно сразу подавать иск

Тема 10. Compliance и совершенствование системы реагирования. ПКс-ИИ-3.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Аудит системы реагирования на инциденты: правовые критерии оценки эффективности.
2.	Разработка Post-Incident Report и корректирующие мероприятия.
3.	Тенденции развития законодательства об ИИ и Big Data в контексте Incident Response.
4.	Страхование киберрисков как механизм защиты и компенсации.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	По итогам внешнего аудита системы реагирования на инциденты аудиторы выявили, что в организации отсутствует утвержденный Регламент взаимодействия CSIRT с юридическим отделом, а сроки уведомления Роскомнадзора об утечках не соблюдаются. Это свидетельствует о: а) высоком уровне зрелости системы; б) несоответствии (non-compliance) требованиям законодательства и локальных актов, что требует разработки корректирующих мероприятий; в) незначительных недостатках, не требующих исправления; г) необходимости уволить IT-директора.		
2.	Страховая компания отказала в выплате по полису киберстрахования, мотивируя это тем, что инцидент произошел из-за того, что		

	организация не установила критическое обновление безопасности, о котором было известно за 3 месяца до атаки. Отказ страховщика: а) неправомерен, страхование покрывает все риски; б) правомерен, если в договоре страхования есть условие об исключении случаев, вызванных грубой неосторожностью или невыполнением обязательных требований по защите (непринятием разумных мер); в) неправомерен, страховая обязана платить всегда; г) может быть оспорен только в уголовном порядке.		

3. Задания закрытого типа.

Тестовые задания.

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.

Записать только цифру выбранного варианта ответа.

1. Что является целью аудита системы реагирования на инциденты?

1. Поиск виновных в инцидентах
2. Проверка соответствия системы требованиям законодательства и внутренним регламентам
3. Наказание сотрудников CSIRT
4. Сокращение бюджета на ИБ

2. Какой документ обязательно составляется по итогам расследования каждого значимого инцидента и содержит рекомендации по улучшению?

1. Акт списания оборудования
2. Post-Incident Report (Отчет по итогам инцидента)
3. Докладная записка на сотрудника
4. Пресс-релиз для СМИ

3. Какая тенденция в законодательстве об ИИ влияет на Incident Response?

5. Полный запрет на использование ИИ
6. Необходимость учета «прозрачности» алгоритмов при расследовании инцидентов с участием ИИ
7. Отмена всех требований к ИИ
8. Передача всех функций реагирования ИИ

4. Какие расходы могут покрываться полисом киберстрахования?

5. Только штрафы регуляторов
6. Только упущенная выгода
7. Расходы на расследование, юридические услуги, выплаты пострадавшим, убытки от простоя
8. Только затраты на новое оборудование

6.3. Критерии и шкала оценивания на основе БРС.

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок	40
Дан развернутый ответ на поставленный вопрос, где обучающийся демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.	30-39
Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.	20-29
Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. обучающийся не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	0-19

6.4. Для решения практических заданий обучающемуся разрешается использование нормативно-правовых актов.

7. Методические материалы по освоению дисциплины

Подготовка к лекциям.

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

Самостоятельная работа на лекции.

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

Подготовка к практическим занятиям.

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

должен проявиться в способности обучающегося свободно ответить на теоретические вопросы практического занятия, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Структура практического занятия:

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

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

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

Работа с литературными источниками.

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

Вопросы для самостоятельной подготовки к лекционным и практическим занятиям:

1. Понятие киберугрозы и инцидента информационной безопасности: правовая дефиниция и соотношение понятий.
2. Источники правового регулирования: международные стандарты (ISO/IEC 27035,

NIST), российское законодательство (ФЗ «О безопасности», Доктрина ИБ РФ).
3. Национальное законодательство в сфере противодействия киберпреступности (гл. 28 УК РФ, КоАП РФ).
4. Роль права в управлении жизненным циклом инцидента: от обнаружения до извлечения уроков.
5. Понятие и правовой статус CSIRT (Computer Security Incident Response Team) в корпоративной структуре.
6. Разработка локальных нормативных актов: Политика управления инцидентами, Регламент взаимодействия CSIRT.
7. Разграничение ответственности между IT-отделом, службой безопасности и юридическим департаментом.
8. Трудовые отношения и конфиденциальность: обязательства сотрудников CSIRT о неразглашении (NDA).
9. Категорирование активов и их правовая защита (государственная тайна, коммерческая тайна, персональные данные).
10. Правовая основа риск-ориентированного подхода (ФЗ-№184 «О техническом регулировании», стандарты ЦБ РФ).
11. Идентификация угроз: фишинг, DDoS-атаки, утечки данных — правовые последствия.
12. Обязанность уведомления регуляторов (Роскомнадзор, ЦБ РФ, ФСТЭК) о фактах инцидентов.
13. Трансграничный характер киберугроз: коллизионные вопросы и определение применимого права.
14. Международные договоры (Будапештская конвенция о киберпреступности) и позиция РФ.
15. Взаимодействие с зарубежными CERT/CSIRT при расследовании инцидентов.
16. Правовые ограничения при передаче данных через границу (трансграничная передача персональных данных).
17. Правовой режим персональных данных (ФЗ-152): требования к обработке и последствия утечек.
18. Защита коммерческой тайны (ФЗ-98) в ходе расследования инцидентов.
19. Обеспечение безопасности критической информационной инфраструктуры (ФЗ-187).
20. Лицензирование и сертификация в области ИБ как превентивная мера.
21. Понятие электронного доказательства и его юридическая сила (УПК РФ, ГПК РФ).
22. Порядок фиксации инцидента: составление актов, протоколы осмотра места происшествия.
23. Применение ACPO Good Practice Guide и российских методик при работе с доказательствами.
24. Обеспечение цепочки хранения (Chain of Custody) и невмешательства в цифровую информацию.
25. Порядок подачи заявления о киберпреступлении в правоохранительные органы.
26. Правовой статус специалиста и эксперта при расследовании компьютерных инцидентов.
27. Судебная компьютерно-техническая экспертиза: назначение, вопросы эксперту, оценка заключения.
28. Взаимодействие с ЦБ РФ при инцидентах в кредитно-финансовой сфере.
29. Уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание вредоносных программ (ст. 273 УК РФ).
30. Административная ответственность за нарушение требований по защите информации (КоАП РФ).
31. Гражданско-правовая ответственность: возмещение убытков, компенсация морального вреда.
32. Дисциплинарная ответственность сотрудников, допустивших инцидент.

33. Правовые аспекты изоляции пораженных сегментов сети и временного ограничения доступа.
34. Защита прав третьих лиц при ликвидации последствий атаки.
35. Восстановление данных: лицензионная чистота ПО и регламенты резервного копирования.
36. Претензионная и исковая работа с контрагентами, пострадавшими от инцидента.
37. Аудит системы реагирования на инциденты: правовые критерии оценки эффективности.
38. Разработка Post-Incident Report и корректирующие мероприятия.
39. Тенденции развития законодательства об ИИ и Big Data в контексте Incident Response.
40. Страхование киберрисков как механизм защиты и компенсации.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Вавилин, Е. В. Гражданско-правовая защита интересов государства в реалиях цифровой трансформации общественных отношений : монография / Е. В. Вавилин, В. А. Бабаков. – Москва : Статут, 2025. - 426 с. – ISBN 978-5-8354-2102-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2240011 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. - Йошкар-Ола : Поволжский государственный технологический университет, 2020. - 154 с. - ISBN 978-5-8158-2165-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1894130 (дата обращения: 07.06.2026). – Режим доступа: по подписке

3. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2024. — 602 с. — DOI 10.12737/1942679. - ISBN 978-5-16-018253-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1942679 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

4. Родичев, Ю. А. Безопасность инфокоммуникаций: стандартизация, измерения соответствия и подготовка кадров : учебное пособие для вузов / Ю. А. Родичев, П. И. Симонов, Ю. А. Кубанков. - Москва : Горячая линия-Телеком, 2020. - 160 с. - ISBN 978-5-9912-0706-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1911622 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

8.2. Дополнительная литература

1. Wong, H. Cyber Security : Law and Guidance / H. Wong. — 2nd ed. — London : Bloomsbury Professional, 2025. — ISBN 9781526528131. (Практическое руководство по праву кибербезопасности, содержащее детальные чек-листы для реагирования на инциденты, анализ требований к уведомлению об инцидентах безопасности, вопросы ответственности работников и защиты организаций после утечек данных).

2. Криминологическая характеристика и предупреждение отдельных видов киберпреступлений // Вестник Московского университета МВД России имени В.Я. Кикотя. — 2025. (Научная статья, анализирующая современные тенденции киберпреступности, категории преступлений в информационно-телекоммуникационном пространстве и проблемы совершенствования законодательства с учетом особенностей цифровой среды).

3. Калашников, И. В., Калашникова, Л. Н. Криминологическая характеристика и прогнозирование отдельных видов киберпреступлений, совершаемых в информационно-

телекоммуникационном пространстве на территории Российской Федерации // Криминологический журнал. — 2024. — № 2. (Исследование, посвященное криминологической характеристике киберпреступлений и вопросам их прогнозирования).

8.3. Нормативные правовые документы и иная правовая информация

Российская Федерация

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». (Базовый закон, определяющий принципы обеспечения безопасности КИИ, права и обязанности субъектов КИИ, включая обязанность информировать ФСБ России о компьютерных инцидентах).
2. Приказ ФСБ России от 25.12.2025 № 547 «Об утверждении Порядка информирования ФСБ России о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации и иных информационных ресурсов Российской Федерации...» (Зарегистрирован в Минюсте России 30.12.2025 № 84871). (Ключевой нормативный акт, вступающий в силу с 30 января 2026 года. Устанавливает новый порядок информирования ФСБ России обо всех компьютерных атаках и инцидентах, реагирования на них и принятия мер по ликвидации последствий. Распространяется не только на субъекты КИИ, но и на государственные органы, унитарные предприятия, учреждения, фонды, госкорпорации. Признает утратившим силу ранее действовавший Приказ ФСБ России от 19.06.2019 № 282) .
3. Уголовный кодекс Российской Федерации (глава 28 «Преступления в сфере компьютерной информации»). (Статьи 272–274.1, устанавливающие ответственность за неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и иные преступления в сфере компьютерной информации).
4. Кодекс Российской Федерации об административных правонарушениях (статьи 13.11–13.13). (Ответственность за нарушение законодательства о персональных данных, нарушение правил защиты информации и иные правонарушения в области информации).
5. Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации». (Утрачивает силу с 30.01.2026 в связи с изданием Приказа № 547, однако может использоваться для сравнительного анализа изменений в регулировании) .
6. Указание Банка России от 25.11.2022 № 6315-У «О порядке информирования Банка России о компьютерных атаках и компьютерных инцидентах, реагирования на них и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении объектов информационной инфраструктуры Банка России». (Ведомственный акт, регулирующий порядок реагирования на инциденты в финансовой сфере).
7. Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка взаимодействия Федеральной службы по техническому и экспортному контролю, территориальных органов Федеральной службы по техническому и экспортному контролю, федеральных органов исполнительной власти, уполномоченных в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и субъектов критической информационной инфраструктуры Российской Федерации по вопросам обмена информацией о компьютерных инцидентах». (Регулирует взаимодействие с ФСТЭК России по вопросам компьютерных инцидентов).

Международное и зарубежное регулирование

1. Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR). (Содержит требования к уведомлению о нарушениях безопасности персональных данных — breach notification).
2. Directive (EU) 2022/2555 (NIS 2 Directive). (Обновленная директива ЕС о безопасности сетевых и информационных систем, устанавливающая расширенные требования к реагированию на инциденты и отчетности для широкого круга организаций).

8.4. Интернет-ресурсы

1. Официальный интернет-портал правовой информации (www.pravo.gov.ru). (Гарантированный источник опубликования федеральных законов и ведомственных актов, включая Приказ ФСБ России № 547).

2. СПС «КонсультантПлюс» (www.consultant.ru). (Профессиональная справочная система, содержащая актуальные редакции документов, включая новейший Приказ ФСБ России № 547 от 25.12.2025, судебную практику по делам о киберпреступлениях, комментарии и аналитические обзоры) .

3. СПС «Гарант» (www.garant.ru). (Альтернативная справочная система с широким набором документов по информационной безопасности и реагированию на инциденты).

4. Официальный сайт ФСБ России (www.fsb.ru). (Информация о деятельности Национального координационного центра по компьютерным инцидентам (НКЦКИ), методические материалы по реагированию на компьютерные атаки).

5. Портал государственных услуг Российской Федерации (www.gosuslugi.ru/cybersecurity). (Раздел по кибербезопасности, содержащий информационно-разъяснительные материалы для граждан и организаций).

6. Официальный сайт МВД России (мвд.рф/mvd/structure1/Upravlenija/ubk). (Информация о деятельности Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий, статистика и профилактические материалы).

7. Официальный сайт ФСТЭК России (fstec.ru). (Нормативные и методические документы по технической защите информации и противодействию техническим разведкам).

8. Сайт Альянса в сфере искусственного интеллекта (a-ai.ru) и РОЦИТ (rocit.ru). (Информационно-разъяснительные материалы по кибербезопасности, аналитика инцидентов, рекомендации по защите).

9. Национальный институт стандартов и технологий США (NIST) — Cybersecurity Framework (www.nist.gov/cyberframework). (Международно признанный стандарт по управлению киберрисками и реагированию на инциденты).

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

9.1. Материально-техническая база

Перечень материально-технического обеспечения:

1. Учебные аудитории, оборудованные для проведения учебных занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, коллоквиумов, мероприятий текущего контроля и промежуточной аттестации, в том числе мультимедийным оборудованием для демонстрации электронных презентаций и аудио- и видеоматериалов;

2. Компьютерные классы для выполнения групповых тестовых и иных

заданий, а также для самостоятельной работы обучающихся оснащенные компьютерной техникой и обеспечением доступа к сети «Интернет» и доступа в электронную информационно- образовательную среду организации;

3. Специализированные аудитории и лаборатории;

4. Библиотека с обеспечением печатными изданиями или электронно-библиотечная система обеспечивающая доступ к электронным изданиям (электронная библиотека);

5. Читальный зал;

6. Технические средства обучения: персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV и др.

9.2. Информационные технологии, программное обеспечение:

При осуществлении образовательного процесса по дисциплине используется информационные технологии и программное обеспечение:

1. Современная операционная система.
2. Kaspersky Endpoint Security (или аналог).
3. Средство просмотра файлов формата pdf.
4. Современные офисные средства (текстовые и табличные редакторы, средстваработы с презентационными материалами и т.д.).
5. Архиватор 7-Zip.
6. Система дистанционного обучения.
7. Автоматизированная библиотечная система.

9.3. Информационные справочные системы:

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