Автономная некоммерческая организация высшего образования
«Санкт-Петербургская юридическая академия»

УТВЕРЖДАЮ

Заведующий кафедрой
социально-гуманитарных дисциплин

_____ А.В. Долматов

«21» августа 2025 г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Специальность	40.05.04 Судебная и прокурорская деятельность
Специализация	Судебная деятельность
Форма обучения	Очная, заочная
Год начала подготовки	2025

Рассмотрена и одобрена на заседании
методического совета
«21» августа 2025 г.
протокол № 1

Рассмотрена на заседании кафедры
социально-гуманитарных дисциплин
«20» августа 2025 г.,
протокол № 6

Санкт-Петербург
2025

Разработал(и) д.п.н., профессор А.В. Долматов
(степень, звание, И.О.Фамилия)

Основы информационной безопасности в юридической деятельности

Оценочные материалы по дисциплине «Основы информационной безопасности в юридической деятельности» специальности 40.05.04 Судебная и прокурорская деятельность / Долматов А.В. – СПб.: АНО ВО СЮА, 2025.

Оценочные материалы по дисциплине «Основы информационной безопасности в юридической деятельности» подготовлены в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования Специалитет по специальности 40.05.04 Судебная и прокурорская деятельность, утвержденного приказом Министерства науки и высшего образования от 18 августа 2020 г. № 1058 и определяют структуру и содержание текущего контроля знаний и промежуточной аттестации.

© Долматов А.В., 2025.
© АНО ВО СЮА, 2025.

1.Компетенции обучающегося, формируемые в результате освоения дисциплины

1.1. Состав компетенций

Рабочей программой дисциплины «Основы информационной безопасности в юридической деятельности» предусмотрено формирование следующих компетенций:

Индекс	Формулировка:
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
ОПК-16	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

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

Код и наименование контролируемой компетенции	Наименование индикатора достижения компетенции	Перечень элементов компетенции	Технологии формирования компетенции	Средства и технологии оценки
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИД.1 Знает методы критического анализа, методы системного подхода; ИД.2 Знает методику разработки стратегических действий; ИД.3 Умеет идентифицировать проблемные ситуации, требующие критического анализа и выработки стратегии действий.	**Знает:** - нормативно-правовую базу, стандарты и системы менеджмента информационной безопасности, - методы и средства поиска, систематизации и обработки правовой информации в глобальных компьютерных сетях. - основные понятия и технологии обеспечения информационной безопасности, основные закономерности создания и функционирования информационных процессов в правовой сфере.	Занятия лекционного типа, Занятия семинарского типа, Самостоятельная работа	Устный опрос Типовые контрольные задания Электронное портфолио Зачет
		Умеет: - идентифицировать проблемные ситуации, организовывать и практически осуществлять защиту компьютерных сетей от вирусов и деструктивных воздействий, - применять полученные знания в области информационной безопасности в глобальных компьютерных сетях в юридической деятельности. - обеспечивать комплексную информационную безопасность организации, - применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов.		
		Владеет: -способностью эффективно работать с информацией в глобальных компьютерных сетях, - способами распознавания информационных угроз и методами их предотвращения, - навыками сбора,		

Код и наименование контролируемой компетенции	Наименование индикатора достижения компетенции	Перечень элементов компетенции	Технологии формирования компетенции	Средства и технологии оценки
		систематизации и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности. - способностью эффективно работать с информацией в глобальных компьютерных сетях, способами распознавания информационных угроз и методами их предотвращения, - навыками сбора, систематизации и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности.		
ОПК-16. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ИД-16.1. Знает классификационные признаки современных информационных технологий ИД-16.2. Умеет проводить отбор и анализ необходимых функциональных характеристик информационных технологий и систем для решения задач профессиональной деятельности; ИД-16.3. Использует современные программные средства информационных технологий для поиска, отбора и использования информации в профессиональной деятельности	**Знает:** - классификацию современных информационных систем и информационных технологий; - основные правила и подходы в работе с информационными технологиями, в том числе в юриспруденции; - принципы работы искусственного интеллекта и возможности его практического применения в юриспруденции.	Занятия лекционного типа, Занятия семинарского типа, Самостоятельная работа	Устный опрос Типовые контрольные задания Электронное портфолио Зачет
		Умеет: использовать аппаратное и программное обеспечение современных информационных систем и сетей в профессиональной деятельности		
		Владеет: навыками работы с прикладными программными продуктами, в том числе в сфере юриспруденции; с офисными пакетами программ и технологиями мультимедиа для решения задач профессиональной деятельности		

1.3. Перечень планируемых результатов обучения по дисциплине, формируемых в результате освоения дисциплины

Код и содержание компетенций	Индикаторы достижения компетенций	Планируемые результаты освоения дисциплины по элементам компетенций
УК-1 - способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИД.1 Знает методы критического анализа, методы системного подхода; ИД.2 Знает методику разработки стратегических действий; ИД.3 Умеет идентифицировать проблемные ситуации,	**УК-1 З1 Знать** – нормативно-правовую базу, стандарты и системы менеджмента информационной безопасности, **УК-1 З2 Знать –** методы и средства поиска, систематизации и обработки правовой информации в глобальных компьютерных сетях. **УК-1 З3 Знать** – основные понятия и технологии обеспечения информационной безопасности, основные закономерности создания и функционирования информационных процессов в правовой сфере.
		УК-1 У1 Уметь – идентифицировать проблемные ситуации,

Код и содержание компетенций	Индикаторы достижения компетенций	Планируемые результаты освоения дисциплины по элементам компетенций
	требующие критического анализа и выработки стратегии действий.	организовывать и практически осуществлять защиту компьютерных сетей от вирусов и деструктивных воздействий, **УК-1 У2 Уметь –** применять полученные знания в области информационной безопасности в глобальных компьютерных сетях в юридической деятельности **УК-1 У3 Уметь** – обеспечивать комплексную информационную безопасность организации **УК-1 У4 Уметь –** применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов
		УК-1 В1 Владеть – способностью эффективно работать с информацией в глобальных компьютерных сетях, **УК-1 В2 Владеть –** способами распознавания информационных угроз и методами их предотвращения, **УК-1 В3 Владеть –** навыками сбора, систематизации и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности. **УК-1 В4; Владеть** – основными методами, способами и средствами получения, хранения, переработки и защиты информации, **УК-1 В5 Владеть –** навыками работы с компьютером как средством управления информацией.
ОПК-16. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ИД-16.1. Знает классификационные признаки современных информационных технологий ИД-16.2. Умеет проводить отбор и анализ необходимых функциональных характеристик информационных технологий и систем для решения задач профессиональной деятельности; ИД-16.3. Использует современные программные средства информационных технологий для поиска, отбора и использования информации в профессиональной деятельности	**ОПК-16 З1 Знать –** классификацию современных информационных систем и информационных технологий; **ОПК-16 З2 Знать –** основные правила и подходы в работе с информационными технологиями, в том числе в юриспруденции; **ОПК-16 З3 Знать –** принципы работы искусственного интеллекта и возможности его практического применения в юриспруденции.
		ОПК-16 У1 Уметь – использовать аппаратное и программное обеспечение современных информационных систем и сетей в профессиональной деятельности
		ОПК-16 В1 Владеть – навыками работы с прикладными программными продуктами, в том числе в сфере юриспруденции; **ОПК-16 В2 Владеть –** навыками работы с офисными пакетами программ и технологиями мультимедиа для решения задач профессиональной деятельности

2. Паспорт оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации

Наименование темы	Контролируемая компетенция	Тип контроля	Вид контроля	Наименование оценочного средства	Показатели формирования компетенций
Тема 1. Основные понятия информационной безопасности в сфере юриспруденции	УК-1 способность работать с информацией в глобальных компьютерных сетях	Текущий	устный; письменный	устный опрос, типовые контрольные задания, электронное портфолио	**УК-1 З3 Знать** – основные понятия и технологии обеспечения информационной безопасности, основные закономерности создания и функционирования информационных процессов в правовой сфере. **ОПК-16 З1 Знать –** классификацию современных информационных систем и информационных технологий

Наименование темы	Контролируемая компетенция	Тип контроля	Вид контроля	Наименование оценочного средства	Показатели формирования компетенций
Тема 2. Технологии обеспечения информационной безопасности	ОПК-16 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	Текущий	устный; письменный	устный опрос, типовые контрольные задания, электронное портфолио	**УК-1 З3 Знать** – основные понятия и технологии обеспечения информационной безопасности, основные закономерности создания и функционирования информационных процессов в правовой сфере **УК-1 У1 Уметь** – организовывать и практически осуществлять защиту компьютерных сетей от вирусов и деструктивных воздействий, **УК-1 У3 Уметь** – обеспечивать комплексную информационную безопасность организации **УК-1У4 Уметь –** применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов **УК-1 В4 Владеть**– основными методами, способами и средствами получения, хранения, переработки и защиты информации, **УК-1 В5 Владеть -** навыками работы с компьютером как средством управления информацией **ОПК-16 З1 Знать** – классификацию современных информационных систем и информационных технологий; **ОПК-16 З2 Знать** – основные правила и подходы в работе с информационными технологиями, в том числе в юриспруденции
Тема 3. Нормативная правовая база, стандарты и системы менеджмента информационной безопасности		Текущий	устный; письменный	устный опрос, типовые контрольные задания, электронное портфолио	**УК-1 З1 Знать** – нормативно-правовую базу, стандарты и системы менеджмента информационной безопасности **УК-1 З2 Знать –** методы и средства поиска, систематизации и обработки правовой информации в глобальных компьютерных сетях. **УК-1 З3 Знать** – основные понятия и технологии обеспечения информационной безопасности, основные закономерности создания и функционирования информационных процессов в правовой сфере. **УК-1 У1 Уметь** – организовывать и практически осуществлять защиту компьютерных сетей от вирусов и деструктивных воздействий **ОПК-16 З1 Знать –** классификацию современных информационных систем и информационных технологий; **ОПК-16 У1 Уметь –** использовать аппаратное и программное обеспечение современных информационных систем и сетей в профессиональной деятельности
Тема 4. Основы защиты персональных данных		Текущий	устный; письменный	устный опрос, типовые контрольные задания, электронное портфолио	**УК-1 У1 Уметь** – организовывать и практически осуществлять защиту компьютерных сетей от вирусов и деструктивных воздействий, **УК-1 В4 Владеть**– основными методами, способами и средствами получения, хранения, переработки и защиты информации **УК-1 В5 Владеть**– навыками работы с компьютером как средством управления информацией. **ОПК-16 З3 Знать –** принципы работы искусственного интеллекта и возможности его практического применения в юриспруденции.
Тема 5. Обеспечение комплексной информационной безопасности организации		Текущий	устный; письменный	устный опрос типовые контрольные задания, электронное портфолио	**УК-1 У3 Уметь** – обеспечивать комплексную информационную безопасность организации **УК-1 У4 Уметь** – применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов. **УК-1 В1 Владеть**– способностью эффективно работать с информацией в глобальных

Наименование темы	Контролируемая компетенция	Тип контроля	Вид контроля	Наименование оценочного средства	Показатели формирования компетенций
					компьютерных сетях **УК-1 В2 Владеть –** способами распознавания информационных угроз и методами их предотвращения **УК-1 В3 Владеть –** навыками сбора, систематизации и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности **УК-1 В4 Владеть**– основными методами, способами и средствами получения, хранения, переработки и защиты информации **ОПК-16 З3 Знать** ¬– принципы работы искусственного интеллекта и возможности его практического применения в юриспруденции. **ОПК-16 В1 Владеть** – навыками работы с прикладными программными продуктами, в том числе в сфере юриспруденции; **ОПК-16 В2 Владеть** – навыками работы с офисными пакетами программ и технологиями мультимедиа для решения задач профессиональной деятельности
Тема 6. Защита компьютерных сетей от вирусов и деструктивных воздействий		Текущий	устный; письменный	устный опрос, типовые контрольные задания, электронное портфолио	**УК-1 У1 Уметь** – организовывать и практически осуществлять защиту компьютерных сетей от вирусов и деструктивных воздействий, **УК-1 У2 Уметь** – применять полученные знания в области информационной безопасности в глобальных компьютерных сетях в юридической деятельности. **УК-1 У3 Уметь** – обеспечивать комплексную информационную безопасность организации **УК-1 В1 Владеть**– способностью эффективно работать с информацией в глобальных компьютерных сетях **УК-1 В2 Владеть –** способами распознавания информационных угроз и методами их предотвращения **УК-1 В3 Владеть –** навыками сбора, систематизации и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности **УК-1 В4 Владеть**– основными методами, способами и средствами получения, хранения, переработки и защиты информации **ОПК-16 У1 Уметь** – использовать аппаратное и программное обеспечение современных информационных систем и сетей в профессиональной деятельности **ОПК-16 В1 Владеть** – навыками работы с прикладными программными продуктами, в том числе в сфере юриспруденции; **ОПК-16 В2 Владеть** – навыками работы с офисными пакетами программ и технологиями мультимедиа для решения задач профессиональной деятельности
Все темы дисциплины		промежуточный	устный	Зачет	**УК-1 З1 Знать** – нормативно-правовую базу, стандарты и системы менеджмента информационной безопасности, **УК-1 З2 Знать –** методы и средства поиска, систематизации и обработки правовой информации в глобальных компьютерных сетях. **УК-1 З3 Знать** – основные понятия и технологии обеспечения информационной безопасности, основные закономерности создания и

Наименование темы	Контролируемая компетенция	Тип контроля	Вид контроля	Наименование оценочного средства	Показатели формирования компетенций
					функционирования информационных процессов в правовой сфере
					УК-1 У1 Уметь – организовывать и практически осуществлять защиту компьютерных сетей от вирусов и деструктивных воздействий **УК-1 У2 Уметь –** применять полученные знания в области информационной безопасности в глобальных компьютерных сетях в юридической деятельности. **УК-1 У3 Уметь** – обеспечивать комплексную информационную безопасность организации **УК-1 У4 Уметь –** применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов **УК-1 В1 Владеть**– способностью эффективно работать с информацией в глобальных компьютерных сетях **УК-1 В2 Владеть –** способами распознавания информационных угроз и методами их предотвращения, **УК-1 В3 Владеть –** навыками сбора, систематизации и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности. **УК-1 В4 Владеть**– основными методами, способами и средствами получения, хранения, переработки и защиты информации **УК-1 В5 Владеть –** навыками работы с компьютером как средством управления информацией. **ОПК-16 З1 Знать –** классификацию современных информационных систем и информационных технологий; **ОПК-16 З2 Знать –** основные правила и подходы в работе с информационными технологиями, в том числе в юриспруденции; **ОПК-16 З3 Знать –** принципы работы искусственного интеллекта и возможности его практического применения в юриспруденции. **ОПК-16 У1 Уметь –** использовать аппаратное и программное обеспечение современных информационных систем и сетей в профессиональной деятельности **ОПК-16 В1 Владеть** – навыками работы с прикладными программными продуктами, в том числе в сфере юриспруденции; **ОПК-16 В2 Владеть –** навыками работы с офисными пакетами программ и технологиями мультимедиа для решения задач профессиональной деятельности

3. Оценочные средства для проведения текущего контроля с описанием показателей, критериев и шкалы оценивания

К оценочным средствам текущего контроля относятся:
- устный опрос;
- типовые контрольные задания;
- электронное портфолио.

Критерии оценивания:
- полнота ответов;

- степень осознанности, понимания изученного;
- языковое оформление ответа – четкость и правильность речи;
- степень самостоятельности выполнения действия;
- осознанность выполнения действия;
- выполнение заданий творческого уровня;
- креативность, коммуникативность;
- информационная компетентность.

Уровень освоения компетенций определяется в зависимости от критерия оценивания результатов обучения и демонстрирует успешность освоения компетенции.

Уровни сформированности компетенций

Повышенный уровень	Базовый уровень	Пороговый уровень	Недопустимый уровень
Компетенция сформирована. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка.	Компетенция сформирована. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	Компетенция сформирована. Демонстрируется недостаточный уровень самостоятельности практического навыка.	Компетенция не сформирована. Уровень самостоятельности практического навыка не демонстрируется.

Шкала оценивания и описание показателей оценивания **для типовых контрольных заданий,** с определением уровней сформированности

Бальная шкала оценивания	Описание показателей оценивания	Уровень сформированности компетенции
«отлично»	- задание выполнено правильно и в полном объеме, согласно предъявляемым требованиям; -проведен правильный анализ нормативно-правового материала; - сделаны аргументированные выводы; - проявлен творческий подход и демонстрация рациональных способов конкретной поставленной задачи; - самостоятельно и последовательно дает ответы на дополнительные вопросы.	Повышенный
«хорошо»	- задание выполнено правильно и в полном объеме, согласно предъявляемым требованиям; - проведен частичный анализ нормативно-правового материала; - сделаны слабо аргументированные выводы; - показаны знания в пределах изучаемой дисциплины; - допущены недочеты.	базовый
«удовлетворительно»	- задание выполнено не в полном объеме, согласно предъявляемым требованиям; - проведен частичный анализ нормативно-правового материала; - сделаны не достаточно аргументированные и полные выводы; - нарушена логика выполнения задания; - показаны не достаточные знания изучаемой дисциплины - допущены единичные существенные ошибки.	Пороговый
«неудовлетворительно»	- задание не выполнено; - выполнено не верно; - допущенные непосредственные ошибки с непосредственной помощью преподавателя.	недопустимый (компетенция не освоена)

Шкала оценивания и описание показателей оценивания **для устного опроса,** с определением уровней сформированности

Бальная шкала оценивания	Описание показателей оценивания	Уровень сформированности компетенции
«отлично»	- ответ раскрывает полностью суть и содержание рассматриваемой проблемы или отдельного вопроса; - ответы излагаются логично, последовательно и не требуют дополнительных пояснений; - делаются обоснованные выводы;	Повышенный

	- демонстрируются глубокие знания и свободное владение теоретическим материалом, точно используются термины; - ответ излагается грамотным языком	
«хорошо»	- ответ излагается уверенно, но не в полном объеме раскрывает суть, содержание и причинно-следственные связи; - демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; - допускает неточности при освещении основного содержания ответа, но исправляет их без наводящих вопросов преподавателя; - на вопросы дает точные и обоснованные ответы с небольшими поправками преподавателя.	базовый
«удовлетворительно»	- ответ раскрывает частично суть и содержание рассматриваемой проблемы или отдельного вопроса; - не полностью раскрываются причинно-следственные связи; - демонстрируются поверхностные знания пройденного материала; испытывает затруднения с выводами; - при недостаточном знании теоретического материала демонстрируется сформированность практических навыков и умений.	Пороговый
«неудовлетворительно»	- ответ не отражает суть и содержание рассматриваемой проблемы или отдельного вопроса; - отвечает непоследовательно и сбивчиво; - не может сделать выводы по изученному материалу; - демонстрирует полное незнание теоретического материала; допускает грубые ошибки в определениях и терминах; - допускает грубые ошибки при ответах или вовсе не отвечает	недопустимый (компетенция не освоена)

Шкала оценивания и описание показателей оценивания **электронного портфолио по дисциплине,** с определением уровней сформированности

Бальная шкала оценивания	Описание показателей оценивания	Уровень сформированности компетенции
«отлично»	Количество правильных выполненных заданий, представленных в портфолио 85 - 100% (в % от максимального количества заданий) с учетом следующих параметров: - полноты раскрытия вопроса; - соответствия содержанию; - достоверности информации; - грамотного компьютерного оформления (форматирование документов, оформление рисунков, таблиц, схем и т.д.); - выбора стратегий и творческого оформления презентаций: SmartArt, кластеры, интеллект-карты, схемы, графики и т.д.	Повышенный
«хорошо»	Количество правильных выполненных заданий, представленных в портфолио 71 - 80% (в % от максимального количества заданий) с учетом следующих параметров: - полноты раскрытия вопроса; - соответствия содержанию; - достоверности информации; - грамотного компьютерного оформления (форматирование документов, оформление рисунков, таблиц, схем и т.д.); - выбора стратегий и творческого оформления презентаций: SmartArt, кластеры, интеллект-карты, схемы, графики и т.д.	базовый
«удовлетворительно»	Количество правильных выполненных заданий, представленных в портфолио 50 - 70% (в % от максимального количества заданий) с учетом следующих параметров: - полноты раскрытия вопроса; - соответствия содержанию; - достоверности информации; - грамотного компьютерного оформления (форматирование документов, оформление рисунков, таблиц, схем и т.д.); - выбора стратегий и творческого оформления презентаций: SmartArt, кластеры, интеллект-карты, схемы, графики и т.д.	Пороговый
«неудовлетворительно»	Количество правильных выполненных заданий, представленных в портфолио менее 50% (в % от максимального количества заданий) с учетом следующих параметров:	недопустимый (компетенция не освоена)

Бальная шкала оценивания	Описание показателей оценивания	Уровень сформированности компетенции
	- полноты раскрытия вопроса; - соответствия содержанию; - достоверности информации; - грамотного компьютерного оформления (форматирование документов, оформление рисунков, таблиц, схем и т.д.); - выбора стратегий и творческого оформления презентаций: SmartArt, кластеры, интеллект-карты, схемы, графики и т.д.	

Содержание оценочных средств для текущего контроля успеваемости

Контрольные задания

Тема 1. Основные понятия информационной безопасности в сфере юриспруденции

Задание 1. Найти информацию и описать основные понятия, используемые в сфере информационной безопасности для включения в электронное Портфолио по дисциплине. Форма работы - индивидуальная**.**

Задание 2. Представить в графической форме (кластер)соотношение основных понятий информационной безопасности.

Информация для работы. Термин "кластер" происходит от английского "cluster" – рой, гроздь, груда, скопление.

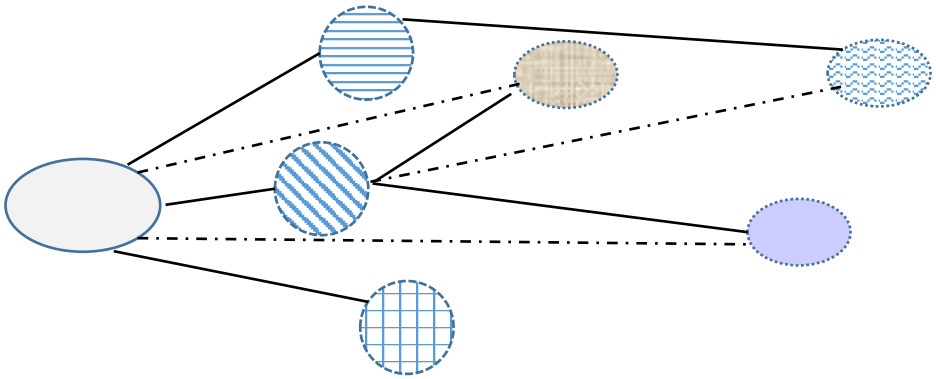
Построение кластеров позволяет выявить систему ключевых слов. С помощью кластеров можно в систематизированном виде представить большие объемы информации (ключевые слова, идеи).

Как составить кластеры

1. В центре кластеров, в главном овале – основная проблема, ключевое слово, понятие, фраза.

2. В овалах следующего уровня – слова, раскрывающие смысл ключевого.

Пример рисунка



Задание 3. Оформить материалы для электронного портфолио.

Тема 2. Технологии обеспечения информационной безопасности

*Задание 1***.**Провести поиск и анализ методов шифрования данных.

*Задание 2.*Раскрыть понятия: идентификации, аутентификации, аудита информационных систем.

*Задание 3.*Найти описание сертификации систем информационной безопасности.

*Задание 4.*Описать способ применения электронной подписи.

Задание 5. Оформить материалы для электронного портфолио.

Тема 3. Нормативная правовая база, стандарты и системы менеджмента информационной безопасности

*Задание 1***.**Найти описание международных стандартов в сфере менеджмента информационной безопасности.

Задание 2. Дать определение: риски информационной безопасности и управление ими.

Задание 3. Описать модель системы менеджмента информационной безопасности.

Задание 4.Разработать замысел организации системы информационной безопасности.

Задание 5. Составить перечень документации системы информационной безопасности.

*Задание*6. Оформить материалы для электронного портфолио.

Тема 4. Основы защиты персональных данных

Задание 1. Выделить виды и классификация информационных систем персональных данных.

Задание 2. Найти описание мер по защите персональных данных.

Задание 3. Разработка системы локальных актов по защите персональных данных.

*Задание*4. Оформить материалы для электронного портфолио.

Тема 5. Обеспечение комплексной информационной безопасности организации

Задание 1. Анализ и оценка угроз информационной безопасности.

Задание 2. Анализ систем комплексной информационной безопасности.

Задание 3. Разработка системы комплексной информационной безопасности организации.

*Задание*4. Оформить материалы для электронного портфолио.

Тема 6. Защита компьютерных сетей от вирусов и деструктивных воздействий

Задание 1. Провести анализ информации о видах вирусов и вредоносных воздействий.

Задание 2. Найти описание способов защиты от вирусов и вредоносных программ.

*Задание*3. Оформить материалы для электронного портфолио.

Требования к электронному портфолио по дисциплине «Основы информационной безопасности в юридической деятельности»

1. Название Электронное Портфолио ФИО студента …..группы по дисциплине «ОИБ в юридической деятельности»

2. Структура Портфолио соответствует темам в рабочей программе дисциплины и включает**:**

2.1.1. Презентацию «Содержание» с гиперссылками на выполненные работы.

2.2.1. Файлы и презентации (выполненные студентом практического задания).

Практические задания к электронному портфолио по темам дисциплины

Тема 1. Основные понятия информационной безопасности в сфере юриспруденции

*Задание 1.*Подготовить сообщение и презентацию по тематике занятия: «Основные понятия информационной безопасности. Конфиденциальность, целостность и доступность данных. Системный подход к обеспечению информационной безопасности».

Задание 2. Провести анализ перспектив применения информационных технологий в юридической деятельности.

Задание 3. Познакомиться со структурой, требованиями и оформить папку «Электронное Портфолио по дисциплине».

Тема 2. Технологии обеспечения информационной безопасности

Задание 1. Провести анализ перспектив применения телекоммуникационных, навигационных и геоинформационных технологий в юриспруденции

Задание 2. Провести анализ проблем нормативно-правовой базы в сфере телекоммуникаций.

*Задание 3.*Создать текстовой документ в формате word «Задачи и виды шифрования информации. Основные технологии разграничения доступа к информации.

*Задание 4.*Пополнить папку «Электронное Портфолио по дисциплине».

Тема 3. Нормативная правовая база, стандарты и системы менеджмента информационной безопасности

*Задание 1.*Провести анализ: нормативная правовая база информационной безопасности; основные законы в сфере информационной безопасности; нормативные документы по защите информации различного уровня; стандарты и системы менеджмента информационной безопасности; «Доктрина информационной безопасности России»; Международные стандарты в сфере менеджмента информационной безопасности программных продуктов необходимых для исследовательской деятельности юриста.

*Задание 2.*Провести исследование по направлениям: Модель системы менеджмента информационной безопасности. Риски информационной безопасности и управление ими. Документация системы информационной безопасности. Системы менеджмента информационной безопасности. Риски информационной безопасности и управление ими. Разработка системы мер по менеджменту информационной безопасности. Обсуждение, выбор электронных методик структурирования данных и оформления результатов. Пополнение Электронного портфолио по дисциплине.

Задание 3. Пополнить папку «Электронное Портфолио по дисциплине».

Тема 4. Основы защиты персональных данных

*Задание 1.*Провести анализ проблемы основ защиты персональных данных. Определить виды персональных данных в соответствии с существующей нормативной правовой базой.

Задание 2. Подготовить сообщение и презентацию по проблематике «Виды и классификация информационных систем персональных данных и возможности их применения в юридической деятельности»

*Задание 3.*Определить основные мероприятия по защите персональных данных и организации защиты персональных данных.

*Задание 4.*Пополнить папку «Электронное Портфолио по дисциплине».

Тема 5. Обеспечение комплексной информационной безопасности организации

*Задание 1.*Сформулировать основные проблемы обеспечения комплексной информационной безопасности организации, управления системой комплексной безопасности организации, совершенствования систем информационной безопасности и системы комплексной информационной безопасности организации.

Задание 2. Провести анализ и оценка угроз информационной безопасности. Анализ систем комплексной информационной безопасности. Разработка системы комплексной информационной безопасности организации.

*Задание 3.*Пополнить папку «Электронное Портфолио по дисциплине».

Тема 6. Защита компьютерных сетей от вирусов и деструктивных воздействий

*Задание 1.*Провести самостоятельный поиск и анализ возможностей вирусов и вредоносных воздействий в юридических информационно-справочных системах с использованием официальных сайтов министерств и ведомств РФ, системы **Гарант** в сети интернет и обучающих пособий.

Задание 2. Провести анализ способов защиты от вирусов и вредоносных программ по юридической проблематике в сети Интернет.

Задание 3. Завершение работы над **Электронным портфолио** и оформление документов и системы гиперссылок на источники; презентация результатов работы **в электронном виде**; оценивание электронного Портфолио.

Вопросы для устного опроса

Тема 1. Основные понятия информационной безопасности в сфере юриспруденции

1. Кратко охарактеризовать основные понятия информационной безопасности.
2. Раскрыть значение информатизации судов общей юрисдикции и Судебного департамента.
3. Описать информационные технологии в реальной и виртуальной жизни.
4. Привести примеры и обоснование необходимости использования информационных технологий безопасности в профессиональной деятельности юриста.

Тема 2. Технологии обеспечения информационной безопасности

1. Перечислить нормативно-правовую базу информационной безопасности.
2. Разработать рекомендации по мотивированию сотрудников соблюдать политику информационной безопасности в юридической деятельности.
3. Разработать систему мер обеспечения безопасности использования информационных технологий в законотворчестве.

Тема 3. Нормативная правовая база, стандарты и системы менеджмента информационной безопасности

1. Разработать программу аудита информационной безопасности и перспектив информатизации в различных сферах юридической деятельности на основе актуальной нормативно-правовой базы.

2. Осуществить планирование правового регулирования безопасности сети «Интернет».
3. Перечислить основные сервисы обеспечения информационной безопасности в деятельности юриста.

Тема 4. Основы защиты персональных данных

1. Разработать таблицу «Правовые методы обеспечения безопасности информации».
2. Описать виды и категории персональных данных
3. Раскрыть возможности информационных систем персональных данных
4. Обосновать основы защиты персональных данных.
5. Рассмотреть классификацию информационных систем персональных данных.

Тема 5. Обеспечение комплексной информационной безопасности организации

1. Разработать методику безопасного использования офисных программ в юридической деятельности.
2. Описать Internet/Intranet–технологии и технологическая эволюция корпоративных информационных систем.
3. Автоматизированные аналитико-статистические информационные системы.

Тема 6. Защита компьютерных сетей от вирусов и деструктивных воздействий

1. Привести примеры и обоснование понятия «безопасность: информационная, национальная, личная».
2. Внутренний и внешний документооборот в Арбитражных судах.
3. Описать особенности графической, табличной и качественной обработка криминальной информации.

4. Оценочные средства для проведения промежуточного контроля с описанием показателей, критериев и шкалы оценивания

К оценочным средствам промежуточной аттестации относятся:

- зачет, предполагающий воспроизведение (изложение) теоретического материала по дисциплине.

Критерии оценивания:

- полнота ответов;
- степень осознанности, понимания изученного;
- языковое оформление ответа – четкость и правильность речи;
- степень самостоятельности выполнения действия;
- осознанность выполнения действия;
- выполнение заданий творческого уровня;
- креативность, коммуникативность;
- информационная компетентность.

Уровень освоения компетенций определяется в зависимости от критерия оценивания результатов обучения и демонстрирует успешность освоения компетенции.

Оцениваемая компетенция	Показатели формирования компетенций	Наименование Темы	Содержание оценочных средств (Перечень вопросов теста к зачету)
УК-1 ОПК-16	УК-1 З3 ОПК-16 З1	**Тема 1.** Основные понятия информационной безопасности в сфере юриспруденции	1. Основные требованиями к информации с точки зрения ее безопасности. 2. Основные виды деструктивных воздействий в компьютерных сетях. 3. Значимые для пользователей характеристики современных криптографических систем. 4. Основная особенность асимметричных криптосистем. 5. Сущность аутентификации пользователя.
	УК-1 З3 УК-1 У1 УК-1 У3 УК-1У4 УК-1 В4 УК-1 В5 ОПК-16 З1 ОПК-16 З2	**Тема 2.** Технологии обеспечения информационной безопасности.	6. Основные технические каналы утечки информации. 7. Основные методы обеспечения информационной безопасности. 8. Основной показатель криптографической стойкости систем шифрования. 9. Основные цели применения асимметричных криптосистемы. 10. Сущность процедуры аутентификации пользователя. 11. Основные принципы политики информационной безопасности организации. 12. Типовой состав универсального защитного программного комплекса информационных систем персональных данных. 13. Основной способ аутентификации дистрибутивов программных продуктов.
	УК-1 З1 УК-1 З2 УК-1 З3 УК-1 У1 ОПК-16 З1 ОПК-16 У1	**Тема 3.** Нормативная правовая база, стандарты и системы менеджмента информационной безопасности.	14. Юридические действия руководителя организации до начала обработки персональных данных. 15. Основные проблемы установки криптографического оборудования в узлах провайдеров интернет. 16. Основные виды угроз информационным системам персональных данных актуальные для судебных органов. 17. Электронная подпись. 18. Процедура применения электронной подписи.
	УК-1 У1 УК-1 В4 УК-1 В5 ОПК-16 З3	**Тема 4.** Основы защиты персональных данных.	19. Перечень необходимых документов, регламентирующих обработку персональных данных (ПД) в образовательной организации. 20. Группы категорий персональных данных. 21. Основные типы угроз информационным системам персональных данных образовательных организаций. 22. Обработка персональных данных граждан РФ.
	УК-1 У3 УК-1 У4 УК-1 В1 УК-1 В2 УК-1 В3 УК-1 В4 ОПК-16 З3	**Тема 5.** Обеспечение комплексной информационной безопасности организации.	23. Основной метод аутентификации электронных документов. 24. Основное отличие симметричных и асимметричных криптосистем. 25. Основное отличие криптосистем временной и гарантированной стойкости. 26. Основные типы угроз программного

Оцениваемая компетенция	Показатели формирования компетенций	Наименование Темы	Содержание оценочных средств (Перечень вопросов теста к зачету)
	ОПК-16 В1 ОПК-16 В22		обеспечения информационных систем объектов критической инфраструктуры. 27. Основная проблема операционных систем с зашифрованным ядром. 28. Основные методы разграничения доступа к информации.
	УК-1 У1 УК-1 У2 УК-1 У3 УК-1 В1 УК-1 В2 УК-1 В3 УК-1 В4 ОПК-16 У1 ОПК-16 В1 ОПК-16 В2	**Тема 6.** Защита компьютерных сетей от вирусов и деструктивных воздействий.	29. Принцип обнаружения вирусов методом эвристического анализа. 30. Метод сигнатурного обнаружения вирусов. 31. Выявление новых неизвестных вирусов и вредоносных программ. 32. Какие виды операционных систем необходимо использовать в целях исключения возможности программных закладок в критически важных информационных системах. 33. Организация защищенного канала передачи информации в публичной сети. 34. Минимальные требования к надежному паролю. 35. Наиболее надежный способ организации защищенного канала в публичной сети.

Уровни сформированности компетенций

Повышенный уровень	Базовый уровень	Пороговый уровень	Недопустимый уровень
Компетенция сформирована. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка.	Компетенция сформирована. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	Компетенция сформирована. Демонстрируется недостаточный уровень самостоятельности практического навыка.	Компетенция не сформирована. Уровень самостоятельности практического навыка не демонстрируется.

Шкала оценивания и описание показателей оценивания **для зачета,** с определением уровней сформированности

Бинарная шкала оценивания	Описание показателей оценивания	Уровень сформированности компетенции
«зачтено»	- в полном объеме излагает учебный материал; - допускает несущественные ошибки и исправляет их самостоятельно или после указания на них преподавателем; - при изложении пройденных разделов подчеркивает существенные признаки изученного предмета; - выделяет причинно-следственные связи; формулирует выводы и обобщает материал.	Повышенный
«не зачтено»	- не может выделить существенные признаки изученного предмета; - затрудняется при выявлении причинно-следственных связей и формулировке выводов; - при ответах на вопросы преподавателя допускает грубые ошибки или вовсе не отвечает на них; - демонстрирует полное незнание пройденного материала.	недопустимый (компетенция не освоена)

Перечень вопросов для проведения промежуточной аттестации (зачет)

1. Основные требованиями к информации с точки зрения ее безопасности.
2. Основные виды деструктивных воздействий в компьютерных сетях.
3. Значимые для пользователей характеристики современных криптографических систем.
4. Основная особенность асимметричных криптосистем.
5. Сущность аутентификации пользователя.
6. Какие виды операционных систем необходимо использовать в целях исключения возможности программных закладок в критически важных информационных системах.
7. Юридические действия руководителя организации до начала обработки персональных данных.
8. Перечень необходимых документов, регламентирующих обработку персональных данных (ПД) в образовательной организации.
9. Группы категорий персональных данных.
10. Основные типы угроз информационным системам персональных данных образовательных организаций.
11. Основные принципы политики информационной безопасности организации.
12. Типовой состав универсального защитного программного комплекса информационных систем персональных данных.
13. Основной способ аутентификации дистрибутивов программных продуктов.
14. Принцип обнаружения вирусов методом эвристического анализа.
15. Метод сигнатурного обнаружения вирусов.
16. Организация защищенного канала передачи информации в публичной сети.
17. Минимальные требования к надежному паролю.
18. Наиболее надежный способ организации защищенного канала в публичной сети.
19. Основные технические каналы утечки информации.
20. Основные методы обеспечения информационной безопасности.
21. Основной показатель криптографической стойкости систем шифрования.
22. Основные цели применения асимметричных криптосистемы.
23. Сущность процедуры аутентификации пользователя.
24. Основные проблемы установки криптографического оборудования в узлах провайдеров интернет.
25. Основные виды угроз информационным системам персональных данных актуальные для судебных органов.
26. Электронная подпись.
27. Процедура применения электронной подписи.
28. Выявление новых неизвестных вирусов и вредоносных программ.
29. Обработка персональных данных граждан РФ.
30. Основной метод аутентификации электронных документов.
31. Основное отличие симметричных и асимметричных криптосистем.
32. Основное отличие криптосистем временной и гарантированной стойкости.
33. Основные типы угроз программного обеспечения информационных систем объектов критической инфраструктуры.
34. Основная проблема операционных систем с зашифрованным ядром.
35. Основные методы разграничения доступа к информации.

ЗАДАНИЯ ОТКРЫТОГО ТИПА, ПРЕДУСМАТРИВАЮЩИЕ РАЗВЕРНУТЫЙ ОТВЕТ ОБУЧАЮЩЕГОСЯ

Вопрос	Ответ
1. Основные требованиями к информации с точки зрения ее безопасности.	Основные требования: конфиденциальность, доступность, целостность информации.
2. Основные виды деструктивных воздействий в компьютерных сетях.	Внедрение вирусов и вредоносных программ, хакерские атаки, взлом аккаунтов, хищение паролей и конфиденциальной информации.
3. Значимые для пользователей характеристики современных криптографических систем.	Криптографическая стойкость, алгоритм шифрования, вид и сложность ключа.
4. Основная особенность асимметричных криптосистем.	В асимметричных криптосистемах используются различные, но математически связанные ключи шифрования и дешифрования. Один из них открытый, другой секретный. Это позволяет существенно уменьшить количество ключей при сетевом обмене.
5. Сущность аутентификации пользователя.	Аутентификация пользователя предполагает подтверждение личности физического лица.
6. Какие виды операционных систем необходимо использовать в целях исключения возможности программных закладок в критически важных информационных системах.	В целях исключения возможности программных закладок в критически важных информационных системах необходимо использовать операционные системы с открытым машинным кодом.
7. Юридические действия руководителя организации до начала обработки персональных данных.	Юридические действия руководителя организации до начала обработки персональных данных включают: уведомление Роскомнадзора, приведение внутренней нормативной базы в соответствие с требованиями закона.
8. Перечень необходимых документов, регламентирующих обработку персональных данных (ПД) в образовательной организации.	Положение об обработке ПД, согласия на обработку ПД обучающихся и работников, приказ руководителя о назначении ответственного за защиту ПД, дополнения в должностные инструкции сотрудников.
9. Группы категорий персональных данных.	Выделяют следующие группы категорий персональных данных: специальные, биометрические, общедоступные, иные.
10. Основные типы угроз информационным системам персональных данных образовательных организаций.	Угрозы, не связанные с недокументированными (недекларированными) возможностями системного и прикладного программного обеспечения.
11. Основные принципы политики информационной безопасности организации.	Использование комплексного подхода к обеспечению безопасности, баланс возможного ущерба от реализации угрозы и затрат на ее предотвращение, использование средств, которые при отказе переходят в состояние максимальной

	защиты, предоставление каждому сотруднику минимального уровня привилегий на доступ к данным.
12. Типовой состав универсального защитного программного комплекса информационных систем персональных данных.	Типовой состав универсального защитного программного комплекса включает: антивирусный модуль, межсетевой экран, средство обнаружения вторжений, хакерских атак.
13. Основной способ аутентификации дистрибутивов программных продуктов.	Основным способом аутентификации дистрибутивов программных продуктов является: использование односторонних функций шифрования и цифровых сертификатов.
14. Принцип обнаружения вирусов методом эвристического анализа.	Эвристический анализ позволяет обнаруживать вирусы по несанкционированным действиям программ.
15. Метод сигнатурного обнаружения вирусов.	Метод сигнатурного обнаружения вирусов заключается в обнаружении вирусов на основе сравнения их кодов с кодами вирусной базы.
16. Организация защищенного канала передачи информации в публичной сети.	Защищенный канал передачи информации организуется применением шифрования с установкой шифрующего оборудования в организациях или у провайдеров.
17. Минимальные требования к надежному паролю.	Минимальные требования к надежному паролю включают: не смысловой, не менее 8 символов: цифр и букв латинского алфавита в различном регистре.
18. Наиболее надежный способ организации защищенного канала в публичной сети.	Установка криптографического оборудования в филиалах организации, однако для этого необходимо получить лицензию ФСБ, соблюдать режим секретности и оформить нужную форму допуска персоналу, обслуживающему оборудование.
19. Основные технические каналы утечки информации.	Основными техническими каналами утечки информации являются: виброакустический, электромагнитный, логический сетевой.
20. Основные методы обеспечения информационной безопасности.	Основными методами обеспечения информационной безопасности являются: разграничение доступа к информации, шифрование.
21. Основной показатель криптографической стойкости систем шифрования.	Основным показателем криптографической стойкости систем шифрования является необходимое для подбора ключа время.
22. Основные цели применения асимметричных криптосистемы.	Асимметричных криптосистемы стали применяться в целях сокращения количества секретных ключей шифрования и дешифрования в информационных сетях.
23. Сущность процедуры аутентификации пользователя.	Процедура аутентификации пользователя заключается в подтверждении личности физического лица;
24. Основные проблемы установки криптографического	Незащищенным остается канал связи между организацией и провайдером. У провайдера есть

оборудования в узлах провайдеров интернет.	доступ к информации. Организация должна полагаться на благонадежность провайдера.
25. Основные виды угроз информационным системам персональных данных актуальные для судебных органов.	Угрозы, не связанные с недокументированными (недекларированными) возможностями системного и прикладного программного обеспечения.
26. Электронная подпись.	Электронный документ, зашифрованный специальной программой с использованием секретного ключа электронной подписи.
27. Процедура применения электронной подписи.	Электронный документ зашифровывается специальной программой с использованием секретного ключа – это и есть электронная подпись (ЭП). Она передается корреспонденту вместе с самим электронным документом. Корреспондент с помощью специальной программы и соответствующего открытого ключа дешифрует ЭП и полученный файл сравнивается с документом, при их полном совпадении документ аутентичен.
28. Выявление новых неизвестных вирусов и вредоносных программ.	Выявление новых неизвестных вирусов и вредоносных программ осуществляется за счет применения эвристического анализа.
29. Обработка персональных данных граждан РФ.	Обработка персональных данных граждан РФ должна осуществляться на серверах, расположенных на территории РФ. Необходимо согласие физического лица на обработку. Предусмотрена трансграничная передача персональных данных в ряде случаев.
30. Основной метод аутентификации электронных документов.	Использование электронной подписи.
31. Основное отличие симметричных и асимметричных криптосистем.	В симметричных криптосистемах используются одинаковые ключи шифрования и дешифрования. В асимметричных криптосистемах используются различные, но математически связанные ключи шифрования и дешифрования.
32. Основное отличие криптосистем временной и гарантированной стойкости.	Компьютерный подбор ключа и вскрытие шифра криптосистем временной стойкости возможно за обозримое время (минуты, часы). Для криптосистем гарантированной стойкости это невозможно за обозримый период (тысячи лет).
33. Основные типы угроз программного обеспечения информационных систем объектов критической инфраструктуры.	Угрозы, связанные с недокументированными (недекларированными) возможностями специального и прикладного программного обеспечения.
34. Основная проблема операционных систем с зашифрованным ядром.	Проблема операционных систем с зашифрованным ядром заключается в возможности наличия программных закладок и недекларированных (недокументированных) возможностей.
35. Основные методы разграничения доступа к	Основные методы разграничения доступа к информации: авторизация с применением паролей

информации.	или мандатов, аутентификация.

Лист учета изменений

Нижний колонтитул оценочных материалов содержит указания на номер и дату версии документа (Например, Версия 1.1 от 09.2021 г.).

Актуализация (непосредственное внесение изменений) текста (части текста) на любой из страниц оценочных материалов осуществляется путем замены всей страницы. Соответственно изменяется номер и дата версии соответствующей страницы.

Информация о внесении изменений (замене листов) вносится в Таблицу учета изменений. Дата последней версии характеризует современность всего документа.

Выпуск новой редакции документа взамен предыдущей осуществляется при накоплении изменений более 20 % от объема общего содержания документа.

Таблица учета изменений

Стр.	Дата последней версии	№ и дата документа, регламентирующего внесение изменений	Дата внесения изменений	Подпись исполнителя