

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Андрей Драгомирович Хлутков  
Должность: директор  
Дата подписания: 21.05.2026 11:27:30  
Уникальный программный ключ:  
880f7c07c583b07b775f6604a630281b13ca9fd2

Приложение 4  
к образовательной программе

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Б1.В.10 Основы информационной безопасности в таможенных органах**  
(индекс, наименование дисциплины в соответствии с учебным планом)

**38.05.02 Таможенное дело**  
(код, наименование направления подготовки)

**Таможенные операции и таможенный контроль**  
(наименование образовательной программы)

**очная/заочная**  
(формы обучения)

Год набора – 2026

Санкт-Петербург

**Автор(ы)-составитель(и) РПД:**

Орел Максим Николаевич, преподаватель кафедры таможенного администрирования

**Заведующий кафедрой:**

Гетман Анастасия Геннадьевна, д-р экон. наук, доц., заведующий кафедрой таможенного администрирования

Рабочая программа дисциплины Б1.В.10 Основы информационной безопасности в таможенных органах одобрена на заседании кафедры таможенного администрирования факультета безопасности и таможни РАНХиГС Санкт-Петербург

Протокол № 9 от 30 апреля 2026 года

## СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы
2. Объем и место дисциплины в структуре образовательной программы
3. Содержание и структура дисциплины
4. Типы оценочных материалов, показатели и критерии их оценивания
5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам
6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине
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.10 Основы информационной безопасности в таможенных органах обеспечивает формирование у обучающихся следующих универсальных, общепрофессиональных и профессиональных компетенций\*:

ОТФ/ТФ и реквизиты ПС  <i>(при наличии)</i> **	Код компетенц ии **	Наименован ие Компетенции  **	Код индикатора достижения компетенций **	Наименован ие индикатора достижения компетенций  **	Образователь ный результат  **
В/01.6 - Определение стоимостей движимого имущества (включая машины и оборудование, отдельные машины и единицы оборудования, являющиеся изделиями машиностроител ьного производства или аналогичные им, группы (множества, совокупности) машин и оборудования, части машин и оборудования вместе или по отдельности, иное движимое имущество), а также работ и услуг, связанных с машинами, оборудованием, иным движимым имуществом, за исключением уникального и представленного в единичных образцах движимого имущества, подлежащих	ПКо ОС-3	Способен применять современные информационно аналитические системы в практической деятельности таможенных органов и участников ВЭД	ПКо ОС-3.2	Демонстрирует умения работать с информационны ми программными средствами и, применяемыми в подразделениях таможенных органов и участников ВЭД, критически оценивать возможности информационны х программных средств для решения профессиональн ых задач. Применяет современные информационны е технологии и программные средства при решении задач профессиональн ой деятельности таможенных органов и участников ВЭД	ПКо ОС-3.2. 3-3  Знает особенности информационны х процессов в таможенной сфере и основы повышения эффективности их работы; -информационн ые процессы и ресурсы информацию с целью выявления новых вызовов и угроз, пресечения противоправных деяний в таможенной сфере  ПКо ОС-3.2. У-3  Умеет правильно выявить угрозы информационног о взаимодействия в работе таможенных органов; -самостоятельно определять требования по безопасности информации программных средств

<p>государственной регистрации воздушных и морских судов, судов внутреннего плавания, космических объектов, извлеченных (добытых из недр) полезных ископаемых и сырья, культурных ценностей (относящихся к движимому имуществу), работ и услуг, связанных с ними;</p> <p>В/02.6 - Определение стоимостей недвижимого имущества, прав, работ и услуг, связанных с объектами недвижимости, за исключением месторождений полезных ископаемых, участков недр и прав, связанных с ними, особо охраняемых территорий и объектов, памятников архитектуры и объектов культурного наследия (относящихся к недвижимому имуществу), работ, услуг и прав, связанных с ними;</p> <p>В/03.6 - Определение стоимостей организаций (включая акции, паи в паевых фондах производственных кооперативов, доли в уставном</p>					<p>информационных систем и информационных технологий в таможенных органах; правильно получать юридически значимую таможенную информацию</p>
---	--	--	--	--	---

<p>(складочном) капитале, имущественные комплексы организации или его части как обособленного имущества действующего бизнеса), за исключением организаций добывающих отраслей, многопрофильных холдингов (включая акции, доли в уставном (складочном) капитале, имущественные комплексы организации или их части как обособленное имущество действующего бизнеса), кредитных и некредитных финансовых организаций, транснациональных организаций (включая акции, доли в уставном (складочном) капитале, имущественные комплексы или их части как обособленное имущество действующего бизнеса); С/01.7 - Определение стоимостей уникального и представленного в единичных образцах движимого имущества, подлежащих государственной регистрации воздушных и морских судов, судов внутреннего плавания,</p>					
--	--	--	--	--	--

<p>космических объектов, извлеченных (добытых из недр) полезных ископаемых и сырья, культурных ценностей (относящихся к движимому имуществу), работ и услуг, связанных с ними;</p> <p>С/02.7 -  Определение стоимостей месторождений полезных ископаемых, участков недр и прав, связанных с ними, особо охраняемых территорий и объектов, памятников архитектуры и объектов культурного наследия (относящихся к недвижимому имуществу), работ, услуг и прав, связанных с ними;</p> <p>С/03.7 -  Определение стоимостей организаций добывающих отраслей, многопрофильных холдингов (включая акции, доли в уставном (складочном) капитале, имущественные комплексы организации или их части как обособленное имущество действующего бизнеса), за исключением кредитных и некредитных финансовых</p>					
---	--	--	--	--	--

<p>организаций, транснациональн ых организаций (включая акции, доли в уставном (складочном) капитале, имущественные комплексы или их части как обособленное имущество действующего бизнеса); С/04.7 - Определение стоимостей нематериальных активов и интеллектуально й собственности; D/01.8 - Определение стоимостей кредитных и некредитных финансовых организаций, транснациональн ых организаций (включая акции, доли в уставном (складочном) капитале, имущественные комплексы или их части как обособленное имущество действующего бизнеса); D/02.8 - Экспертиза (проверка) итогового документа об определении стоимостей; D/04.8 - Методологическа я и исследовательска я деятельность в области определения стоимостей</p> <p>08.025 Специалист по оценочной деятельности Приказ</p>					
---	--	--	--	--	--

Министерства труда и социальной защиты Российской Федерации от 26 ноября 2018 г. № 742н					
--	--	--	--	--	--

\* Дисциплина может формировать компетенцию полностью или частично.

\*\* Должно соответствовать Приложению 1 к образовательной программе

## **2. Объем и место дисциплины в структуре образовательной программы**

### **Объем дисциплины**

Общая трудоемкость дисциплины по учебному плану составляет 2 зачетные единицы или 72 академических часов/54 астрономических часов.

Дисциплина реализуется частично с применением дистанционных образовательных технологий (далее – ДОТ).

Доступ к системе дистанционных образовательных технологий осуществляется каждым обучающимся самостоятельно с любого устройства на портале: <https://lms.ranepa.ru/>. Пароль и логин к личному кабинету/профилю предоставляется студенту в деканате.

Для очной формы обучения трудоемкость контактной работы с преподавателем составляет 34 ч. (из них: лекции – 14 ч., практические занятия – 16 ч.), самостоятельная работа – 38 ч. 4 часа-контроль

Для заочной формы обучения трудоемкость контактной работы с преподавателем составляет 10 ч. (из них: лекции – 4 ч., практические занятия – 6 ч.), контроль – 4 ч., самостоятельная работа – 58 ч.

### **Место дисциплины в структуре ОП ВО**

Дисциплина Б1.В.10 Основы информационной безопасности в таможенных органах осваивается на 5 курсе (9 семестр) очной формы и 6 курсе (12 семестр) заочной формы обучения.

Учебная дисциплина базируется на знаниях, полученных на дисциплинах: Информатика, Информационные таможенные технологии, Анализ бизнес-процессов в таможенном деле.

Знания, умения и навыки, полученные при изучении дисциплины, используются студентами при подготовке и сдаче государственного экзамена.

Формой промежуточной аттестации в соответствии с учебным планом является зачет.

### 3. Содержание и структура дисциплины

#### 3.1. Структура дисциплины

##### Очная форма обучения

№ п/п	Наименование тем и (или) разделов	ВС ЕГ О	Объем дисциплины, ак.час										Форма текущего контроля успеваемости, промежуточной аттестации		
			Контактная работа обучающихся с преподавателем по видам учебных занятий							Самостоятельная работа					
			Период теоретического обучения				Период промежуточной аттестации (сессия)			СРкр	СРэк	СР			
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ					Кат тэк	К о н т р о л ь
			Л	ВЛ	ЛР	ПЗ									
Тема 1	Информационная безопасность в современной системе таможенных органов	16	2	0	0	4	0	0	0	0	0	0	10	Т, ПЗ	
Тема 2	Система правового обеспечения	18	4	0	0	4	0	0	0	0	0	0	10	Т, УО	

	защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов													
Тема 3	Понятие и структура информационной безопасности. Характер и формы угроз. Каналы утечки информации в таможенных органах. Формы обеспечения информационной безопасности ЕАИС. Средства управления защитой информации в таможенных органах.	19	4	0	0	4	0	0	0	0	0	0	11	Т, Д
Тема 4	Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности таможенного органа	19	4	0	0	4	0	0	0	0	0	0	11	Т, УО
Промежуточная аттестация														<b>Зачет</b>

<b>Итого</b>		72	14	0	0	16	0	0		4	0	0	38	
--------------	--	----	----	---	---	----	---	---	--	---	---	---	----	--

*Используемые сокращения:*

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

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

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

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

СРэк – самостоятельная работа на подготовку к экзамену.

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

УО – устный опрос.

ПЗ – практическое задание.

Д – доклад.

Т – тестирование.

### 3.1. Структура дисциплины

#### Заочная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕ ГО	Объем дисциплины, ак.час		Форма текущего контроля успеваемости, промежуточной аттестации	
			Контактная работа обучающихся с преподавателем по видам учебных занятий			Самостоятельная работа
			Период теоретического обучения	Период промежуточной аттестации (сессия)		

			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Кат тЭК	К о н т р о л ь	СРкр	СРЭК	СР	
			Л	ВЛ	ЛР	ПЗ									
Тема 1	Информационная безопасность в современной системе таможенных органов	16	0	0	0	1	0	0	0	0	0	0	0	15	Т, ПЗ
Тема 2	Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов	19	2	0	0	2	0	0	0	0	0	0	0	15	Т, УО
Тема 3	Понятие и структура информационной безопасности. Характер и формы угроз. Каналы утечки информации в таможенных органах. Формы	15	0	0	0	1	0	0	0	0	0	0	0	14	Т, Д

	обеспечения информационной безопасности ЕАИС. Средства управления защитой информации в таможенных органах.													
Тема 4	Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности таможенного органа	18	2	0	0	2	0	0	0	0	0	0	14	Т, УО
Промежуточная аттестация														<b>Зачет</b>
<b>Итого</b>		72	4	0	0	6	0	0		4	0	0	58	

*Используемые сокращения:*

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

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

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

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

СРэк – самостоятельная работа на подготовку к экзамену.

СР – самостоятельная работа в семестре на подготовку к учебным занятиям;

УО – устный опрос.

ПЗ – практическое задание.

Д – доклад.

Т – тестирование.



## 3.2. Содержание дисциплины

### **Тема 1. Информационная безопасность в современной системе таможенных органов. ПКo OC-3.2.**

Понятие и предмет информационной безопасности, и ее место в системе обеспечения национальной безопасности. Объекты информационной безопасности: личность, общество, государство, - особенности каждого из объектов. Информация и информационные системы как объекты правового регулирования в сфере обеспечения информационной безопасности. Право и законодательство в сфере обеспечения информационной безопасности. Подразделения, обеспечивающие информационную безопасность в таможенных органах.

### **Тема 2. Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов. ПКo OC-3.2.**

Направления государственной политики РФ в сфере информатизации и информационной безопасности личности, общества, государства, таможенные органы России. Концепция национальной безопасности и Доктрина информационной безопасности России. Развитие информационных технологий и обеспечение безопасности в таможенных органах России. Национальные интересы России в информационной сфере: для личности, общества и государства, таможенных органах.

### **Тема 3. Понятие и структура информационной безопасности. Характер и формы угроз. Каналы утечки информации в таможенных органах. Формы обеспечения информационной безопасности ЕАИС. Средства управления защитой информации в таможенных органах. ПКo OC-3.2.**

Характеристика основных угроз в информационной сфере для личности, общества и государства, таможенных органах России. Классификация угроз информационной безопасности на различных уровнях управления таможенных органов.

Сравнительный анализ возможностей по нейтрализации угроз информационной безопасности в России и развитых зарубежных странах. Модели прогнозирования и нейтрализации угроз информационной безопасности и их применение.

### **Тема 4. Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности таможенного органа. ПКo OC-3.2.**

Структура нормативного правового обеспечения Российской Федерации в области информационной безопасности. Международная

нормативная правовая база по вопросам информационной безопасности. Международные стандарты обеспечения информационного обмена. Структура внутреннего нормативного правового обеспечения информационной безопасности в ЕАЭС, таможенных органах ЕАЭС и России. Разрабатываемые в таможенных органах России документы по вопросам информационной безопасности. Понятие государственной тайны.

Критерии отнесения информации к государственной тайне. Доступ и допуск к государственной тайне, категории допуска. Порядок засекречивания и рассекречивания информации, отнесенной к государственной тайне. Служебная тайна. Понятие служебной тайны и критерии охраноспособности прав на нее.

#### **4. Типы оценочных материалов, показатели и критерии оценивания**

4.1. Оценочные материалы по дисциплине Б1.В.10 Основы информационной безопасности в таможенных органах входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляет фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

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

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

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

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

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

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

#### 4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	<ol style="list-style-type: none"> <li>1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.</li> <li>2. Внимательно прочитать предложенные варианты ответа.</li> <li>3. Выбрать один верный ответ.</li> <li>4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).</li> </ol>	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	<ol style="list-style-type: none"> <li>1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов.</li> <li>2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д.</li> <li>3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов.</li> <li>4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).</li> </ol>	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	<ol style="list-style-type: none"> <li>1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.</li> <li>2. Внимательно прочитать предложенные варианты ответа.</li> <li>3. Выбрать несколько правильных ответов.</li> <li>4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).</li> </ol>	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	<ol style="list-style-type: none"> <li>1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.</li> </ol>	Ответ считается верным, если правильно указана вся последовательность цифр

		<p>2. Внимательно прочитать предложенные варианты ответа.</p> <p>3. Построить верную последовательность из предложенных элементов.</p> <p>4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).</p>	
<p>Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора</p>	<p>Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа</p>	<p>1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.</p> <p>2. Внимательно прочитать предложенные варианты ответа.</p> <p>3. Выбрать один верный ответ.</p> <p>4. Записать только номер (или букву) выбранного варианта ответа.</p> <p>5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).</p>	<p>Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа</p>
<p>Задание открытого типа с развернутым ответом</p>	<p>Прочитайте текст и запишите развернутый обоснованный ответ</p>	<p>1. Внимательно прочитать текст задания и понять суть вопроса.</p> <p>2. Продумать логику и полноту ответа.</p> <p>3. Записать ответ, используя четкие компактные формулировки.</p> <p>4. В случае расчетной задачи, записать решение и ответ</p>	<p>Ответ считается верным:</p> <p>1. Отсутствие фактических ошибок.</p> <p>2. Раскрытие объема используемых понятий (полнота ответа).</p> <p>3. Обоснованность ответа (наличие аргументов).</p> <p>4. Логическая последовательность излагаемого материала.</p>

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением 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			E	P/ Passed
0-54	Неудовлетворительно	Не зачтено	F	F/Failed

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

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

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

5.1. В ходе реализации дисциплины используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Т – тестирование, УО – устный опрос, ПЗ – практическое задание,  
Д – доклад.

### Тема 1. Информационная безопасность в современной системе таможенных органов. ПКo OC-3.2.

#### Тестовые задания:

Тест 1.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Обладатель информации имеет право:

- а) защищать от незаконного использования информации, способами в рамках закона;
- б) использовать информацию по своему усмотрению;
- в) использовать конфиденциальную инф другого обладателя без его ведома;
- г) разрешать или ограничивать доступ к информации.

Тест 2.

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

Внимательно прочитайте предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

По степени функциональности информационные системы бывают:

- а) геоинформационные, финансовые, кадровые;
- б) производственные, документальные, финансовые, кадровые;
- в) фактографические, документальные, геоинформационные;
- г) производственные, маркетинговые, финансовые, кадровые.

Тест 3.

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

Внимательно прочитайте предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Ключи электронной подписи — это:

- а) уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;
- б) уникальная последовательность символов, предназначенная для создания электронной подписи;
- в) шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;
- г) программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

Практическое задание:

### Задание 1.

Сотрудник компании периодически использует слабые пароли для доступа к корпоративным ресурсам, что создает угрозу для безопасности данных.

Какие шаги предпринять для усиления информационной безопасности в данной ситуации?

### Задание 2.

В организации возник случайный сбой в системе безопасности, из-за которого несколько сотрудников получили несанкционированный доступ к данным, которые им не требовались для выполнения рабочих обязанностей.

Какие меры по обеспечению информационной безопасности следует принять?

### Задание 3.

В офисе компании один из сотрудников случайно утратил флеш-накопитель, на которой хранились конфиденциальные данные клиентов.

Какие шаги по обеспечению информационной безопасности необходимо предпринять, чтобы минимизировать угрозы утечки данных?

**Тема 2. Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов. ПКО ОС-3.2.**

### Тестовые задания:

#### Тест 1.

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

Внимательно прочитайте предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

По степени функциональности информационные системы бывают:

- а) геоинформационные, финансовые, кадровые;
- б) производственные, документальные, финансовые, кадровые;
- в) фактографические, документальные, геоинформационные;
- г) производственные, маркетинговые, финансовые, кадровые.

#### Тест 2.

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

Внимательно прочитайте предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Защита информации – это...

- а) комплекс мероприятий, направленных на обеспечение информационной безопасности;
- б) процесс разработки структуры базы данных в соответствии с требованиями пользователей;
- в) небольшая программа для выполнения определенной задачи.

Тест 3.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Правовое обеспечение безопасности информации делится?

- а) международно-правовые нормы;
- б) национально-правовые нормы;
- в) все ответы правильные.

Вопросы для устного опроса:

1. Назовите объекты информационной безопасности.
2. Назовите подразделения, обеспечивающие информационную безопасность в таможенных органах Российской Федерации.
3. Какая существует Международная нормативная правовая база по вопросам информационной безопасности?
4. Назовите классификацию угроз информационной безопасности на различных уровнях управления таможенных органов Российской Федерации.
5. Перечислите критерии отнесения информации к государственной тайне?

**Тема 3. Понятие и структура информационной безопасности. Характер и формы угроз. Каналы утечки информации в таможенных органах. Формы обеспечения информационной безопасности ЕАИС. Средства управления защитой информации в таможенных органах. ПКo ОС-3.2.**

Тестовые задания:

Тест 1.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Виды электронных подписей:

а) простая электронная подпись (ПЭП) — это подпись, которая создаётся с помощью средств электронной связи и позволяет подтвердить авторство электронного документа, но не обладает высокой степенью защиты;

б) неквалифицированная электронная подпись (НЭП) — это электронная подпись, которая создаётся с использованием криптографических средств и позволяет подтвердить авторство и целостность документа, но не всегда соответствует требованиям законодательства для юридически значимого документооборота;

в) квалифицированная электронная подпись (КЭП) — это электронная подпись, которая соответствует требованиям законодательства и обладает высоким уровнем защиты. Она позволяет подтвердить авторство, целостность и неизменность документа, а также может использоваться для юридически значимого документооборота;

г) усиленная электронная подпись — это вид электронной подписи, который включает в себя неквалифицированную и квалифицированную электронные подписи. Усиленная подпись обеспечивает более высокий уровень защиты по сравнению с простой электронной подписью.

Тест 2.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Что такое лицензия?

а) документ, подтверждающий право на занятие определённой деятельностью;

б) разрешение на въезд в страну;

в) сертификат на покупку товаров;

г) документ, подтверждающий личность владельца.

Тест 3.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Что относится к правовой защите информации?

- а) лицензии;
- б) патенты;
- в) разрешения;
- г) свидетельства.

Тематика докладов:

1. Информационная безопасность таможенных органов Российской Федерации и Евразийского экономического союза.
2. Направления развития информационных таможенных технологий.
3. Характеристика форм обеспечения информационной безопасности Единая автоматизированная информационная система ФТС России.
4. Анализа информационных рисков и управление ими.
5. Коммерческая тайна. Понятие и правовое регулирование.
6. Служебная тайна. Понятие и правовое регулирование.
7. Роль и место информационно-технической безопасности в работе таможенного органа.

**Тема 4. Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности таможенного органа. ПКo OC-3.2.**

Тестовые задания:

Тест 1.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Обладатель информации имеет право:

- а) защищать от незаконного использования информации, способами в рамках закона;
- б) использовать информацию по своему усмотрению;
- в) использовать конфиденциальную инф другого обладателя без его ведома;
- г) разрешать или ограничивать доступ к информации.

### Тест 2.

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

Внимательно прочитайте предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Какие действия включает в себя обработка персональных данных?

- а) только сбор персональных данных;
- б) сбор и хранение персональных данных;
- в) сбор, хранение, распространение и использование персональных данных без согласия субъекта;
- г) сбор, систематизация, хранение, использование, распространение, а также иные действия с персональными данными.

### Тест 3.

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

Внимательно прочитайте предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Какие виды ключей электронной подписи существуют?

- а) открытый ключ;
- б) закрытый ключ;
- в) общий ключ;
- г) публичный ключ.

### Вопросы для устного опроса:

1. Объекты информационной безопасности: личность, общество, государство, - особенности каждого из объектов.

2. Право и законодательство в сфере обеспечения информационной безопасности.

3. Направления государственной политики РФ в сфере информатизации и информационной безопасности личности, общества, государства, таможенные органы России?

4. Структура нормативного правового обеспечения Российской Федерации в области информационной безопасности?

5. Классификация угроз информационной безопасности на различных уровнях управления таможенных органов?

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

## 6.2.

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 студент	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,15	15
КТ 2	100	0,15	15
КТ 3	100	0,15	15
КТ 4	100	0,15	15
Итого:	x	0,6	60

Формула расчета результата контрольной точки:

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

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

### **КТ-1**

#### **Тема 1.**

Тестирование (Т).

Практическое задание (ПЗ).

### **КТ-2**

#### **Тема 2.**

Тестирование (Т).

Устный опрос (УО).

### **КТ-3**

#### **Тема 3.**

Тестирование (Т).

Доклад (Д).

**КТ-4**

**Тема 4.**

Тестирование (Т).

Устный опрос (УО).

Для каждой формы текущего контроля успеваемости обучающихся в рамках КТ определены критерии оценивания результатов выполнения задания.

1. *Критерии оценивания тестирования (Т):*

Критерии оценки	Диапазон баллов	Описание критерия
<i>Количество правильных ответов</i>	<i>0</i>	<i>Количество правильных ответов менее 55%</i>
	<i>25</i>	<i>Количество правильных ответов от 55% до 64%</i>
	<i>50</i>	<i>Количество правильных ответов от 65% до 74%</i>
	<i>75</i>	<i>Количество правильных ответов от 75% до 84%</i>
	<i>100</i>	<i>Количество правильных ответов от 85% до 100%</i>
Итого максимально:	100	

2. *Критерии оценивания практических заданий (ПЗ):*

Критерии оценки	Диапазон баллов	Описание критерия
<i>Качество правильных ответов</i>	<i>0-54</i>	<i>У обучающегося отсутствуют ответы на большинство вопросов задачи, задание не выполнено или выполнено не верно.</i>
	<i>55-64</i>	<i>Обучающимся допущены отдельные ошибки при выполнении задания</i>
	<i>65-84</i>	<i>Обучающимся в целом задание выполнено, имеются отдельные неточности или недостаточно полные ответы, не содержащие ошибок.</i>
	<i>85-100</i>	<i>Обучающимся задание выполнено без ошибок и в полном объеме.</i>
Итого максимально:	100	

3. Критерии оценивания устного опроса (УО):

Критерии оценки	Диапазон баллов	Описание критерия
<i>Качество правильных ответов</i>	0-54	<i>Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.</i>
	55-64	<i>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.</i>
	65-84	<i>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.</i>
	85-100	<i>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.</i>

Итого максимально:	100	
--------------------	-----	--

#### 4. Критерии оценивания доклада (Д):

Критерии оценки	Диапазон баллов	Описание критерия
<i>Содержание и раскрытие темы</i>	<i>0-20</i>	<i>Детальное, последовательное описание всех этапов с конкретными примерами</i>
<i>Грамотность изложения</i>	<i>0-20</i>	<i>Соблюдены все правила грамматики, орфографии и пунктуации</i>
<i>Стилистика</i>	<i>0-20</i>	<i>Единый стиль изложения, точные формулировки, уместное использование терминов, лаконичность</i>
<i>Логика изложения</i>	<i>0-20</i>	<i>Чёткая последовательность изложения, логические связи между частями текста, аргументы подтверждают выводы</i>
<i>Оригинальность</i>	<i>0-20</i>	<i>Уникальный подход к теме, нестандартные решения, инновационные идеи, собственная позиция автора</i>
Итого максимально:	100	

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий.

Для решения практических заданий, тестовых заданий студенту разрешается использование калькулятора; программ для работы с электронными таблицами для обработки, анализа и визуализации данных.

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

6.1. Промежуточная аттестация проводится в форме **зачета**.

Зачет может проводиться с применением следующих методов (средств):

- устный ответ на вопросы билета;
- письменный ответ на вопросы билета.

При реализации промежуточной аттестации с применением ДОТ:

- устно с прокторингом – в форме ответа на вопросы билета;
- письменно с прокторингом – в форме ответа на вопросы билета.

6.2. Типовые оценочные материалы промежуточной аттестации.

### **Вопросы для подготовки к зачету:**

1. Понятие и предмет информационной безопасности.
2. Роль информационной безопасности в обеспечении национальной безопасности государства.
3. Интересы личности, общества и государства в информационной сфере.
4. Конституционное закрепление и охрана информационных прав граждан.
5. Право на неприкосновенность частной жизни, личной и семейной тайны.
6. Информация: понятие, виды, свойства.
7. Информационные процессы, информационные ресурсы: понятие, значение.
8. Соотношение понятий безопасность и информационная безопасность.
9. Уровни обеспечения безопасности: личностный, гражданское общество, государственный.
10. Разработка и принятие Концепции национальной безопасности и Доктрины информационной безопасности России.
11. Понятие источника угрозы национальной безопасности, информационной безопасности и их разновидности.
12. Принципы обеспечения информационной безопасности.
13. Основные задачи, функции и стандарты обеспечения информационной безопасности.
14. Защита информации: понятие, принципы, система.
15. Персональные данные. Понятие, правовое регулирование.
16. Понятие и правовая основа обеспечения информационной безопасности системе таможенных органов.
17. Формы информационного обеспечения деятельности таможенных органов.
18. Объекты обеспечения информационной безопасности таможенных органов.
19. Информационное обеспечение деятельности таможенных органов государств-членов Евразийского экономического союза.
20. Характер и формы угроз.
21. Виды «нарушителей» режима защиты информации, модели их действий.
22. Потенциальный (вероятный) нарушитель информационной безопасности таможенных органов Российской Федерации.
23. Система информационной безопасности ФТС России: подразделения обеспечения информационной безопасности предприятия: состав, структура и функции.

24. Основные нормативные правовые и руководящие документы, касающиеся вопросов соблюдения государственной тайны и их содержание.
25. Основные нормативные правовые и руководящие документы, касающиеся вопросов соблюдения коммерческой тайны и их содержание.
26. Содержание процессов лицензирования и сертификации.
27. Организация мероприятий по обеспечению информационной безопасности таможенных органов.
28. Создание и обеспечение защищенного электронного документооборота в таможенных органах.
29. Способы и средства защиты информации от утечки по техническим каналам в автоматизированных информационных системах.
30. Понятие и содержание криптографии, основные методы, применяемые участниками ВЭД и таможенными органами.
31. Электронная подпись (понятие, содержание процесса использования электронной подписи, проблемы), использование электронной подписи участниками ВЭД и таможенными органами.
32. Методы и приемы информационно-психологического воздействия на должностных лиц.
33. Алгоритмы информационно-психологической защиты.
34. Использование интернет-технологий и обеспечение информационной безопасности.
35. Основные технологии построения защищенных информационных систем.
36. Формы контроля состояния технической защиты информации.
37. Информационно-аналитические средства, используемые при разработке и принятии решения по информационной безопасности таможенных органов.
38. Коммерческая тайна. Понятие и правовое регулирование.
39. Банковская тайна. Понятие и правовое регулирование.
40. Профессиональная тайна. Понятие и правовое регулирование.
41. Служебная тайна. Понятие и правовое регулирование.
42. Понятие государственной тайны.
43. Доступ и допуск к государственной тайне, категории допуска.
44. Порядок засекречивания и рассекречивания информации, отнесенной к государственной тайне. Предварительное засекречивание.
45. Ответственность за нарушение порядка обращения с информацией, составляющей государственную тайну.
46. Основные виды деятельности по защите информации, подлежащие лицензированию.
47. Система и органы государственного лицензирования деятельности в области защиты информации.
48. Общий порядок лицензирования в области защиты информации.
49. Государственные стандарты в области защиты информации.

50. Общий порядок проведения сертификации средств защиты информации.

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

ТИП ЗАДАНИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	ТИПОВЫЕ ЗАДАНИЯ	
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	По степени функциональности информационные системы бывают: а) геоинформационные, финансовые, кадровые; б) производственные, документальные, финансовые, кадровые; в) фактографические, документальные, геоинформационные; г) производственные, маркетинговые, финансовые, кадровые.	
		Защита информации – это... а) комплекс мероприятий, направленных на обеспечение информационной безопасности; б) процесс разработки структуры базы данных в соответствии с требованиями пользователей; в) небольшая программа для выполнения определенной задачи.	
		а) Какова основная цель обеспечения информационной безопасности таможенных органов? б) Защита конфиденциальной информации. в) Обеспечение бесперебойной работы таможенных систем. г) Защита от кибератак и мошенничества. д) Все вышеперечисленное.	
Задание закрытого типа на установление соответствия	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).	1. Обладатель информации имеет право:	
		1) Разрешать или ограничивать доступ к информации -	а) Разрешать или ограничивать доступ к информации
		2) Передавать информацию третьим лицам без согласия	б) Передавать информацию третьим лицам без согласия
		3) Скрывать информацию от государственных органов	с) Скрывать информацию от государственных органов
		4) Использовать информацию любым способом без ограничений	д) Использовать информацию любым способом без ограничений-
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	1. Какие категории персональных данных выделяет Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ? а) личные; б) общедоступные; в) физиологические; г) специальные; д) биометрические.	
		2. Обладатель информации имеет право: а) защищать от незаконного использования информации, способами в рамках закона; б) использовать информацию по своему	

		<p>усмотрению;</p> <p>в) использовать конфиденциальную инф другого обладателя без его ведома;</p> <p>г) разрешать или ограничивать доступ к информации.</p>
Задание закрытого типа на установление последовательности	<p>1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.</p> <p>2. Внимательно прочитать предложенные варианты ответа.</p> <p>3. Построить верную последовательность из предложенных элементов.</p> <p>4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).</p>	<p>1. Расставьте в порядке убывания по степени серьезности потенциальные информационные угрозы безопасности:</p> <p>а) Несанкционированный доступ к конфиденциальной информации;</p> <p>б) Вредоносное программное обеспечение;</p> <p>в) Случайное удаление важных данных сотрудником;</p> <p>г) Физическое повреждение серверов и другого оборудования.</p> <p>2. Расположите в хронологическом порядке основные этапы формирования доктрины информационной безопасности России, начиная с самого раннего:</p> <p>а) Принятие Доктрины информационной безопасности Российской Федерации в её нынешнем виде;</p> <p>б) Разработка и утверждение основ политики обеспечения информационной безопасности в РФ</p> <p>в) Создание нормативно-правовой базы для защиты информационной инфраструктуры страны;</p> <p>г) Формирование концепции информационной безопасности на основе анализа внешних и внутренних угроз</p>
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	<p>1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.</p> <p>2. Внимательно прочитать предложенные варианты ответа.</p> <p>3. Выбрать один верный ответ.</p> <p>4. Записать только номер (или букву) выбранного варианта ответа.</p> <p>5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).</p>	<p>1. Одно из наиболее общих понятий науки, обозначающее некоторые сведения, совокупность каких-либо данных, знаний и т. п.?</p> <p>а) Разъяснение;</p> <p>б) Информация;</p> <p>в) Справка;</p> <p>г) Информирование.</p> <p>2. Классификация информации по категории доступа подразделяется на:</p> <p>1) Публичную, массовую и конфиденциальную;</p> <p>2) Общедоступную и конфиденциальную;</p> <p>3) Массовую и доступ к которой ограничен ФЗ;</p> <p>4) Общедоступную и доступ к которой ограничен ФЗ</p>
Задание открытого типа с развернутым ответом	<p>1. Внимательно прочитать текст задания и понять суть вопроса.</p> <p>2. Продумать логику и полноту ответа.</p> <p>3. Записать ответ, используя четкие компактные формулировки.</p> <p>4. В случае расчетной задачи записать решение и ответ</p>	<p>1. Персональные данные — это:</p> <p>2. что такое электронная подпись?</p>

### 6.3. Критерии и шкала оценивания на основе БРС.

*Критерии и балльная шкала определяются преподавателем*

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
---------------------	--------------------

<p><i>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</i></p>	<p>40</p>
<p><i>Дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.</i></p>	<p>30-39</p>
<p><i>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.</i></p>	<p>20-29</p>
<p><i>Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.</i></p>	<p>0-19</p>

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

Для решения практических заданий, тестовых заданий студенту разрешается использование калькулятора; программ для работы с электронными таблицами для обработки, анализа и визуализации данных.

## 7. Методические материалы по освоению дисциплины (модуля)

Подготовка к лекциям.

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

Самостоятельная работа на лекции.

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лекции лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места, определения, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек. Лучше если они будут собственными, чтобы не приходилось просить их у однокурсников и тем самым не отвлекать их во время лекции. 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 письменно). 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.

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.

Структура практического занятия:

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

1. Обсуждение теоретических вопросов, определенных программой дисциплины.

2. Доклад и/ или выступление с презентациями по проблеме практического занятия.

3. Обсуждение выступлений по теме – дискуссия.

4. Выполнение практического задания с последующим разбором полученных результатов или обсуждение практического задания, выполненного дома, если это предусмотрено программой.

5. Подведение итогов занятия.

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

Работа с литературными источниками.

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

широкий спектр мнений по изучаемой проблеме.

## **8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет**

### **8.1. Основная литература**

1. Внуков, А. А. Защита информации: учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561313> — Режим доступа: для авториз. пользователей.

2. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567915> — Режим доступа: для авториз. пользователей.

3. Николаев, Н. С. Управление информационной безопасностью: учебник / Н. С. Николаев. — Москва: КноРус, 2021. — ISBN 978-5-406-07325-4. — URL: <https://book.ru/book/939841> — Текст: электронный. — Режим доступа: для авториз. пользователей.

4. Суворова, Г. М. Информационная безопасность: учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567672>. — Режим доступа: для авториз. пользователей.

5. Чернова, Е. В. Информационная безопасность человека: учебник для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/566457>. — Режим доступа: для авториз. пользователей.

### **8.2. Дополнительная литература**

1. Аксенов, И. А. Цифровые технологии в таможенной и околотаможенной деятельности: учеб. пособие. / И. А. Аксенов ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. — Владимир : Изд-во ВлГУ, 2022. — 363 с. — ISBN 978-5-9984-1698-9. — Режим доступа: для авториз. пользователей.

2. Башмаков, И. А., Информационное обеспечение перевозочного процесса: учебник / И. А. Башмаков, А. В. Олимпиев. — Москва : КноРус, 2025. — 196 с. — ISBN 978-5-406-14646-0. — [URL:](#)

<https://book.ru/book/957571> — Текст: электронный. — Режим доступа: для авториз. пользователей.

3. Власенков, Г. Ю. Информационная безопасность таможенных технологий. Том 1: монография / Г. Ю. Власенков, В. А. Карданов. — Москва : Юстиция, 2020. — 60 с. — URL: <https://book.ru/book/935204> — Текст : электронный. - Режим доступа: для авторизир. пользователей. — Режим доступа: для авториз. пользователей.

### 8.3. Нормативные правовые документы и иная правовая информация

1. Международная конвенция об упрощении и гармонизации таможенных процедур от 18 мая 1973 года (в редакции Протокола о внесении изменений от 26 июня 1999 года).

2. Конституция РФ.

3. Гражданский кодекс Российской Федерации, Федеральный закон Российской Федерации от 30.11.1994 № 51-ФЗ.

4. Договор о ЕАЭС.

5. Таможенный кодекс ЕАЭС.

6. Уголовный кодекс Российской Федерации.

7. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».

8. Федеральный закон Российской Федерации от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

9. Федеральный закон от 03.08.2018 № 289-ФЗ «О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации».

10. Постановление Правительства РФ от 24.10.2013 № 940 «О принятии Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах».

11. Постановление Правительства РФ от 16.09.2013 № 809 «О Федеральной таможенной службе» (вместе с «Положением о Федеральной таможенной службе»).

12. Распоряжение Правительства РФ от 06.10.2021 № 2816-р «Прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года».

13. Распоряжение Правительства Российской Федерации от 23 мая 2020 г. N 1388-р «Стратегия развития таможенной службы Российской Федерации до 2030 года».

14. Приказ ГТК Российской Федерации от 26.09.2003 № 1069 «Об утверждении Концепции системы управления рисками в таможенной службе РФ».

15. Приказ ФТС России от 29.04.2021 N 358 "Об установлении Порядка подключения информационной системы информационного оператора к информационной системе таможенных органов".

16. Приказ ФТС России от 30.10.2020 № 949 "Об утверждении типовых положений об информационно-технических подразделениях региональных таможенных управлений".

17. Приказ ФТС России от 28.06.2021 № 535 "Об утверждении Положения по организации процессов жизненного цикла информационно-программных средств в таможенных органах".

18. Распоряжение ФТС России от 16.04.2010 № 96-р «Об утверждении Положения о рабочей группе по управлению ведомственной программой внедрения информационно-коммуникационных технологий в деятельность ФТС России и координации перехода на предоставление государственных услуг и исполнение государственных функций в электронном виде».

19. Приказ ФТС России от 07.10.2010 № 1866 «Об утверждении положения по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена в таможенных органах Российской Федерации».

20. Приказ ФТС России от 04.08.2015 № 1552 "О внесении изменений в приказ ФТС России от 6 июня 2012 г. N 1118".

21. Приказ ФТС России от 19.07.2021 № 616 "Об утверждении перечня типовых структурных подразделений таможенных органов Российской Федерации".

22. Приказ ФТС России от 18.03.2019 № 444 "Об утверждении Порядка совершения таможенных операций при помещении товаров на склад временного хранения и иные места временного хранения, при хранении и выдаче товаров, Порядка регистрации документов, представленных для помещения товаров на временное хранение и выдачи подтверждения о регистрации документов, Порядка выдачи (отказа в выдаче) разрешения на проведение операций, указанных в пункте 2 статьи 102 Таможенного кодекса Евразийского экономического союза, определении Условий и Порядка выдачи (отмены) разрешения на временное хранение товаров в иных местах, Способа предоставления отчетности владельцами складов временного хранения и лицами, получившими разрешение на временное хранение в местах временного хранения товаров, форм отчетов, порядка их заполнения, а также порядка и сроков представления отчетности".

23. Приказ ФТС России от 17 июня 2010 г. N 1154 "Об утверждении Положения о Единой автоматизированной информационной системе таможенных органов".

24. Приказ ФТС России от 28.06.2021 № 535 "Об утверждении Положения по организации процессов жизненного цикла информационно-программных средств в таможенных органах".

25. Приказ ФТС России от 17.09.2013 №1761 «Об утверждении Порядка использования Единой автоматизированной информационной системы таможенных органов при таможенном декларировании и выпуске (отказе в выпуске) товаров в электронной форме, после выпуска таких товаров, а также при осуществлении в отношении них таможенного контроля».

26. Приказ ФТС России от 20.09.2021 № 798 "Об утверждении Общего положения о таможне".

27. Приказ ФТС России от 20.09.2021 № 797 "Об утверждении Общего положения о региональном таможенном управлении".

28. Приказ ФТС России от 28.06.2021 № 535 "Об утверждении Положения по организации процессов жизненного цикла информационно-программных средств в таможенных органах".

29. Приказ ФТС России от 01.06.2015 № 1035 «Об утверждении Временного порядка совершения таможенных операций в отношении железнодорожных транспортных средств и перемещаемых ими товаров в международном грузовом сообщении при представлении документов и сведений в электронном виде».

30. Приказ ФТС России от 05.08.2015 № 1572 «Об утверждении Порядка использования Единой автоматизированной информационной системы таможенных органов при совершении таможенных операций в отношении железнодорожных транспортных средств и перемещаемых ими товаров в международном грузовом сообщении при представлении документов и сведений в электронном виде».

31. Распоряжение ФТС России от 21.10.2015 № 321-р «Об утверждении Временного порядка действий должностных лиц таможенных органов при проведении эксперимента по использованию сертификатов обеспечения уплаты таможенных пошлин, налогов при помещении товаров под таможенную процедуру таможенного транзита на принципах электронного документооборота».

32. Приказ ФТС России от 21.10.2015 № 2133 «Об утверждении основных направлений развития информационно-коммуникационных технологий в таможенных органах Российской Федерации до 2030 года».

33. Распоряжение ФТС России от 14.04.2016 № 106-р «О проведении эксперимента по оформлению и контролю воздушных судов, осуществляющих международные перевозки, и перемещаемых ими товаров на основании электронных документов и сведений».

34. Решение Коллегии Евразийской экономической комиссии (далее – ЕЭК) от 17.04.2018 № 56 "Об утверждении Порядка представления предварительной информации о товарах, предполагаемых к ввозу на таможенную территорию Евразийского экономического союза автомобильным транспортом".

35. Решение коллегии ЕЭК от 17 апреля 2018 г. N 57 "Об утверждении Порядка представления предварительной информации о товарах,

предполагаемых к ввозу на таможенную территорию Евразийского экономического союза железнодорожным транспортом".

36. Решение Коллегии ЕЭК от 12.11.2013 № 254 (ред. от 06.03.2014) «О структурах и форматах электронных копий таможенных документов».

37. Решение Коллегии ЕЭК от 24.04.2018 № 62 «Об утверждении Порядка представления предварительной информации о товарах, предполагаемых к ввозу на таможенную территорию Евразийского экономического союза воздушным транспортом».

38. Письмо ФТС России от 22.06.2009 № 09-105/28328 «О направлении требований по техническому оснащению таможенных органов».

39. Письмо ФТС России от 28.03.2012 № 01-11/14513 «О применении технологии удаленного выпуска товаров».

40. Письмо ФТС России от 03.02.2016 № 14-112/04552 «О личном кабинете участника ВЭД».

41. Приказ ФТС России от 26.09.2011 № 1937 «Об объявлении Соглашения о порядке взаимодействия Федеральной таможенной службы и Федерального агентства по распоряжению государственным имуществом при организации приема-передачи отдельных категорий имущества».

42. Приказ Министерства транспорта РФ и Федеральной таможенной службы от 2 марта 2022 г. N 68/146 "Об утверждении Порядка информационного взаимодействия между Федеральной службой по надзору в сфере транспорта и Федеральной таможенной службой при осуществлении государственного контроля (надзора) за осуществлением международных автомобильных перевозок в пунктах пропуска через государственную границу Российской Федерации".

43. Приказ ФТС России от 30.09.2011 № 1981 «Об утверждении Регламента организации работ по соглашениям о взаимодействии (информационном взаимодействии) ФТС России с федеральными органами исполнительной власти и иными организациями».

44. Приказ ФТС России от 16.04.2012 № 699 «О реализации Соглашения о сотрудничестве Федеральной таможенной службы и Федеральной налоговой службы».

45. Приказ ФТС России от 24.04.2013 № 819 «О реализации Соглашения об информационном взаимодействии ФТС и Федеральной миграционной службы».

46. Приказ ФТС России от 10.02.2015 № 215 «Соглашение о порядке взаимодействия ФТС и Федеральной службы судебных приставов».

47. Распоряжение ФТС России от 20.05.2015 № 151-р «Об утверждении порядка организации межведомственного взаимодействия ФТС России с федеральными органами исполнительной власти и организациями с использованием технологических карт межведомственного взаимодействия для предоставления государственных

услуг и осуществления государственных функций, в том числе проведения мониторинга межведомственного электронного взаимодействия».

#### 8.4 Интернет-ресурсы

СЗИУ располагает доступом через сайт научной библиотеки <https://sziiu-lib.ranepa.ru/> к следующим подписным электронным ресурсам:

##### ***Русскоязычные ресурсы***

- Электронные учебники электронно-библиотечной системы (ЭБС) «Айбукс»
- Электронные учебники электронно-библиотечной системы (ЭБС) «Юрайт»
- Электронные учебники электронно-библиотечной системы (ЭБС) «Лань»
- Электронные учебники электронно-библиотечной системы (ЭБС) «ZNANIUM.COM»
- Электронные учебники электронно-библиотечной системы (ЭБС) «BOOK.RU»
- Электронные учебники электронно-библиотечной системы (ЭБС) «IPR SMART»
- <http://www.government.ru> – интернет-портал Правительства Российской Федерации.
- <http://www.gks.ru> – сайт Федеральной статистической государственной службы РФ.
- <http://www.consultant.ru> – справочная правовая система Консультант Плюс.
- <http://www.customs.ru> – сайт Федеральной таможенной службы РФ.
- <http://www.customs.ru> – Итоговые отчеты ФТС России.
- <http://www.economy.ru> – сайт Минэкономразвития РФ.
- <http://www.cbr.ru> – официальный сайт Центрального Банка Российской Федерации.
- <http://www.worldcustomsjournal.org> – международный таможенный электронный журнал.
- <http://www.garant.ru> – справочная правовая система Гарант.
- <http://www.www.edu.ru> – Федеральный портал «Российское образование».
- <http://www.wcoomd.org/en/topics/facilitation/resources> – Компедиум ВТамО по управлению таможенными рисками.

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

№ п/п	Наименование
1.	Специализированные залы для проведения лекций, оснащенные персональным компьютером/ноутбуком и мультимедийным проектором
2.	Аудитории и компьютерные классы, оборудованные посадочными местами и персональными компьютерами с выходом в Интернет для проведения практических занятий
3.	«МТС Линк» — российская платформа для онлайн-коммуникаций и совместной работы команд; «Яндекс Телемост» — сервис для видеоконференций от Яндекса; Я-мессенджер
4.	Технические средства обучения: персональные компьютеры; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV; программы для работы с электронными таблицами для обработки, анализа и визуализации данных; соответствующие онлайн-инструменты для построения интеллект-карты и моделей в различных нотациях
5.	Научная библиотека (в т.ч. электронные информационные ресурсы научной библиотеки)
6.	СДО Академии <a href="https://lms.ranepa.ru/">https://lms.ranepa.ru/</a>