

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Андрей Драгомирович Хлутков
Должность: директор
Дата подписания: 27.10.2025 19:39:42
Уникальный программный ключ:
880f7c07c583b07b775f6604a63028b17cc91d1

1

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

**СЕВЕРО-ЗАПАДНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ
Факультет безопасности и таможи**

УТВЕРЖДЕНО
Директор
Северо-Западного института
управления - филиала РАНХиГС
Хлутков А.Д.

ПРОГРАММА СПЕЦИАЛИТЕТА

Информационно-аналитическая деятельность в таможенном деле

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,
реализуемой без применения электронного (онлайн) курса**

Б1.В.10 «Основы информационной безопасности в таможенных органах»

38.05.02 «Таможенное дело»

очная/заочная
(форма(формы) обучения)

Год набора – 2025

Санкт-Петербург-2024

Автор–составитель:

Старший Преподаватель
Кафедры таможенного администрирования

М.Н. Орел

Заведующий кафедрой

таможенного администрирования, канд. экон. наук, доц.

А.Г. Гетман

РПД (*Основы информационной безопасности в таможенных органах*) одобрена на заседании кафедры таможенного администрирования. Протокол от 28.04.2025 № 8

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. Материалы текущего контроля успеваемости обучающихся
5. Оценочные материалы промежуточной аттестации по дисциплине
6. Методические материалы для освоения дисциплины
7. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»
 - 7.1. Основная литература
 - 7.2. Дополнительная литература
 - 7.3. Нормативные правовые документы и иная правовая информация
 - 7.4. Интернет-ресурсы
 - 7.5. Иные источники
8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

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

Дисциплина Б1.В.10 «Основы информационной безопасности в таможенных органах» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКо ОС-3.	Способен применять современные информационно-аналитические системы в практической деятельности таможенных органов и участников ВЭД	ПКо ОС-3.2	Способен демонстрировать умения работать с информационными программными средствами, применяемыми в подразделениях таможенных органов и участников ВЭД, критически оценивать возможности информационных программных средств для решения профессиональных задач. Применяет современные информационные технологии и программные средства при решении задач профессиональной деятельности таможенных органов и участников ВЭД

В результате освоения дисциплины у студентов должны быть сформированы:

Профессиональные действия	Код этапа освоения компетенции	Результаты обучения
---------------------------	--------------------------------	---------------------

Способность использовать специальные программные средства при осуществлении таможенных операций, связанных с заполнением таможенной декларации. Способность применять методы математической статистики в ходе аналитической деятельности	ПКо ОС-3.2	на уровне знаний: -особенности информационных процессов в таможенной сфере и основы повышения эффективности их работы; -информационные процессы и ресурсы информации с целью выявления новых вызовов и угроз, пресечения противоправных деяний в таможенной сфере. на уровне умений: -правильно выявить угрозы информационного взаимодействия в работе таможенных органов; -самостоятельно определять требования по безопасности информации программных средств информационных систем и информационных технологий в таможенных органах; правильно получать юридически значимую таможенную информацию на уровне навыков: -самостоятельно применять организационные и технические основы информационного взаимодействия таможенных органов с иными субъектами информационных правоотношений; -оценки влияния сквозных цифровых технологий на информационную безопасность таможенных органов; навыками определения актуальных проблем правового и организационного обеспечения информационной безопасности системе таможенных органов Рос на уровне знаний: -основные положения, сущность и содержание основных понятий и категорий в области обеспечения информационной защиты гражданских прав участников внешнеэкономической деятельности и лиц, осуществляющих деятельность в сфере таможенного дела; основы применения высоких цифровых технологии для предотвращения несанкционированного доступа к информации. на уровне умений: -выявлять основные вызовы и угрозы правового обеспечения информационной безопасности в системе таможенных органов; использовать основные положения законодательных и правоприменительных актов, регламентирующих обеспечение информационной безопасности; на уровне навыков: - навыками информационно-технического контроля за процессуальными актами и документами, подтверждающих соблюдение запретов и ограничений; навыками применения
--	-------------------	--

		соответствующих положений современной Концепции информационной безопасности таможенных органов Российской Федерации
--	--	---

2. Объем и место дисциплины (модуля) в структуре ОП ВО

Объем дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы или 108 академических часа.

Для очной формы:

Вид работы	Трудоемкость в акад. Часах/астр Часах
Общая трудоемкость	108/81
Контактная работа с преподавателем	42/31,5
Лекции	18/13,5
Практические занятия	22/16,5
Лабораторные занятия	0
Самостоятельная работа	66/49,5
Консультация	2/1,5
Контроль	
Формы текущего контроля	ПЗ, УО, Т, Доклад
Форма промежуточной аттестации	Зачет с оценкой

Для заочной формы:

Вид работы	Трудоемкость в акад. Часах/астр Часах
Общая трудоемкость	108/81
Контактная работа с преподавателем	10/7,5
Лекции	4/3
Практические занятия	4/3
Лабораторные занятия	
Самостоятельная работа	94/70,5
Консультация	2/1,5
Контроль	4/3
Формы текущего контроля	ПЗ, УО, Т, Доклад
Форма промежуточной аттестации	Зачет с оценкой

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.10 «Основы информационной безопасности в таможенных органах» включена в состав дисциплин части формируемой участниками образовательных отношений учебно-образовательного плана подготовки специалистов по специальности 38.05.02 «Таможенное дело».

Дисциплина изучается на 5 курсе (10 семестр) очной формы и 6 курсе (12 семестр) заочной формы обучения.

Содержание курса основывается на изученных дисциплинах «Информатика», «Информационные таможенные технологии», «Анализ бизнес-процессов в таможенном деле».

Форма промежуточной аттестации в соответствии с учебным планом: Зачет с оценкой. Дисциплина реализуется с применением дистанционных образовательных технологий.

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

3. Содержание и структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ДОТ	ЛР/ДОТ	ПЗ/ДОТ	КСР		
Тема 1	Информационная безопасность в современной системе таможенных органов	24	4/4		4/0		16	ПЗ
Тема 2	Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов	26	4/4		6/0		16	УО
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.	28	6/6		6/0		16	Доклад
Тема 4	Особенности классификаций и	28	4/4		6/0		18	Т

	расследования дел о преступлениях в сфере информационной безопасности. таможенного органа.							
Промежуточная аттестация:	2							Зачет
Всего:	108	18/18		22/0		66		

Условные обозначения: ПЗ – практические занятия; УО – устный опрос; Т – тестирование; Д – доклад *- не входит в общий объем дисциплины.

Заочная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа с обучающимися преподавателем по видам учебных занятий				СР	
			Л/ДОТ	ЛР/ДОТ	ПЗ/ДОТ	КСР		
Тема 1	Информационная безопасность в современной системе таможенных органов	22	0		0		22	ПЗ
Тема 2	Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов.	28	2/0		2/0		24	УО
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	24	0		0/0		24	Доклад

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости*, промежуточной
		Всего	Контактная работа обучающихся преподавателем по видам учебных занятий				СР	
			Л/ДОТ	ЛР/ДОТ	ПЗ/ДОТ	КСР		
	информации в таможенных органах.							
Тема 4	Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности.	28	2/0		2/0		24	Т
Промежуточная аттестация:		2						Зачет с оценкой
Всего:		108	4/0		4/0		94	4

Условные обозначения: ПЗ – практические занятия; УО – устный опрос; Т – тестирование; Д – доклад, *- не входит в общий объем дисциплины.

Содержание дисциплины

Тема 1. Информационная безопасность в современной системе таможенных органов.

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.

Направления государственной политики РФ в сфере информатизации и информационной безопасности личности, общества, государства, таможенных органов 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.

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.

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. Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины «Основы информационной безопасности в таможенных органах» используются следующие методы текущего контроля успеваемости обучающихся:

Тема	Формы (методы) текущего контроля успеваемости
Тема 1. Информационная безопасность в современной системе таможенных органов.	ПЗ
Тема 2. Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов.	УО
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.	Доклад
Тема 4. Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности. таможенного органа.	Т

4.2. Материалы текущего контроля успеваемости обучающихся

Полный перечень типовых оценочных материалов находится в ФОСе по дисциплине.

Типовые оценочные материалы по теме 1 «Информационная безопасность в современной системе таможенных органов»:

Практические занятия:

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? Ответ: ввести политику обязательного использования сильных паролей, провести обучение сотрудников по безопасным практикам паролей, регулярно проводить аудит паролей в системе, и внедрить механизм двухфакторной аутентификации для повышения уровня защиты.

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? Ответ: срочно устранить сбой в системе безопасности, отобрать несанкционированный доступ у сотрудников, провести анализ причин сбоя, внести необходимые изменения в систему безопасности, и обучить сотрудников правилам доступа к данным.

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? Ответ: немедленно уведомить ответственного за безопасность в компании, провести аудит утраченных данных, изменить доступы к чувствительной информации, а также провести обучение сотрудников по правилам обращения с конфиденциальной информацией.

Важная государственная информация о научных разработках в сфере высоких технологий подверглась утечке через кибератаку. Какие меры, согласно доктрине информационной безопасности РФ, следует принять для предотвращения подобных инцидентов и защиты национальных интересов? Ответ: реализовать комплекс мер: усиление от кибератак, аудит систем информационной безопасности, внедрение средств мониторинга, а также сотрудничество с силовыми структурами и специализированными органами.

В международных социальных сетях активно распространяется дезинформация, подрывающая общественную стабильность в стране. Какие меры государства могут предпринять в соответствии с доктриной информационной безопасности для противодействия угрозам информационной безопасности? Ответ: Специальные меры по мониторингу и реагированию на дезинформацию, сотрудничество с социальными сетями, образование граждан в области критического мышления.

Типовые оценочные материалы по теме 2 «Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов»:

Вопросы для проведения устного опроса:

1. Объекты информационной безопасности: личность, общество, государство, - особенности каждого из объектов;
2. Информация и информационные системы как объекты правового регулирования в сфере обеспечения информационной безопасности;
3. Право и законодательство в сфере обеспечения информационной безопасности;
4. Подразделения, обеспечивающие информационную безопасность в таможенных органах;
5. Направления государственной политики РФ в сфере информатизации и информационной безопасности личности, общества, государства, таможенные органы России;
6. Концепция национальной безопасности и Доктрина информационной безопасности России.
7. Международная нормативная правовая база по вопросам информационной безопасности;

8. Структура нормативного правового обеспечения Российской Федерации в области информационной безопасности;

9. Характеристика основных угроз в информационной сфере для личности, общества и государства, таможенных органах России;

10. Классификация угроз информационной безопасности на различных уровнях управления таможенных органов;

11. Направления государственной политики РФ в сфере информатизации и информационной безопасности личности, общества, государства, таможенных органов России;

12. Структура внутреннего нормативного правового обеспечения информационной безопасности в ЕАЭС, таможенных органах ЕАЭС и России;

13. Понятие государственной тайны. Критерии отнесения информации к государственной тайне;

14. Роль и место системы обеспечения информационной безопасности в деятельности таможенных органов.

Типовые оценочные материалы по теме 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»:

Темы для подготовки докладов:

1. Понятие и свойства информации;
2. Информационная безопасность таможенных органов Российской Федерации и Евразийского экономического союза;
3. Архитектура информационных таможенных систем;
4. Направления развития информационных таможенных технологий;
5. Информационные ресурсы таможенных органов;
6. Характеристика форм обеспечения информационной безопасности ЕАИС ФТС России;
7. Единая автоматизированная информационная система ФТС России как совокупность мер, обеспечивающих автоматизацию деятельности таможенных органов.
8. Анализа информационных рисков и управление ими;
9. Коммерческая тайна. Понятие и правовое регулирование;
10. Банковская тайна. Понятие и правовое регулирование.
11. Профессиональная тайна. Понятие и правовое регулирование;
12. Служебная тайна. Понятие и правовое регулирование;
13. Роль и место информационно-технической безопасности в работе таможенного органа;
14. Характеристики основных способов и средств информационно-психологического воздействия на должностных лиц таможенных органов.
15. Структура нормативного правового обеспечения РФ в области информационной безопасности;
16. Международная нормативная база по вопросам информационной безопасности;
17. Структура внутреннего нормативного правового обеспечения информационной безопасности в ЕАЭС.

Типовые оценочные материалы по теме 4 «Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности таможенного органа»:

Примеры тестовых вопросов:

1. Обладатель информации имеет право:

- 1) Защищать от незаконного использования информации, способами в рамках закона;
- 2) Использовать информацию по своему усмотрению;
- 3) Использовать конфиденциальную инф другого обладателя без его ведома;
- 4) Разрешать или ограничивать доступ к информации.

2. Что НЕ включает в себя обработка персональных данных? Ошибками при действиях персонала;

- 1) Сбор информации;
- 2) Систематизацию;
- 3) Извлечение;
- 4) Верификацию.

3. Ключи электронной подписи — это:

- 1) Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;
- 2) Уникальная последовательность символов, предназначенная для создания электронной подписи;
- 3) 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;
- 4) Программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

4. Неквалифицированной электронной подписью является электронная подпись, которая:

- 1) Получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- 2) Позволяет определить лицо, подписавшее электронный документ;
- 3) Позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- 4) Создается с использованием средств электронной подписи;
- 5) Все ответы верны.

5. В каком нормативном акте определено понятие обеспечения национальной безопасности?

- 1) Указ Президента РФ от 02.07.2021 N 400;
- 2) Указ Президента РФ от 16.07.2014 N 657;
- 3) Таможенный Кодекс ЕАЭС;
- 4) Федеральный закон от 03.08.2018 N 289-ФЗ.

6. Перечислите виды информационных систем по способу представления информации:

- 1) Фактографические;
- 2) Документальные;
- 3) Геоинформационные;
- 4) Все перечисленные.

7. Лицензия — это;

- 1) Деятельность лицензирующих органов по предоставлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, оценке соблюдения соискателем лицензии, лицензиатом лицензионных требований, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования;

2) Специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается записью в реестре лицензий;

3) Руководитель лицензирующего органа, иное должностное лицо лицензирующего органа, уполномоченное на принятие решения, осуществление иного действия в сфере лицензирования.

8. По степени функциональности информационные системы бывают:

- 1) Геоинформационные, финансовые, кадровые;
- 2) Производственные, документальные, финансовые, кадровые;
- 3) Фактографические, документальные, геоинформационные;
- 4) Производственные, маркетинговые, финансовые, кадровые.

9. Что относится к правовой защите информации?

- 1) Лицензии;
- 2) Патенты;
- 3) Нет верного варианта;
- 4) Верны оба варианта.

10. Виды электронных подписей?

- 1) Простая, квалифицированная и неквалифицированная;
- 2) Простая и квалифицированная;
- 3) Квалифицированная и неквалифицированная;
- 4) Нет верного ответа.

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1 Зачет с оценкой может проводиться с применением следующих методов:

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

5.2. Оценочные материалы промежуточной аттестации

Компонент компетенции	Промежуточный/ключевой индикатор оценивания	Критерий оценивания
ПКо ОС-3.2 Способен демонстрировать умения работать с информационными программными средствами, применяемыми в подразделениях таможенных органов и участников ВЭД, критически оценивать возможности информационных программных средств для решения профессиональных задач. Применяет современные информационные технологии и программные средства при решении задач профессиональной деятельности таможенных органов и участников ВЭД	Демонстрирует умения работать с информационными программными средствами, применяемыми в подразделениях таможенных органов и участников ВЭД, критически оценивать возможности информационных программных средств для решения профессиональных задач. Применяет современные информационные технологии и программные средства при решении задач профессиональной деятельности таможенных органов и участников ВЭД.	Обучающийся обнаружил все-стороннее, систематическое и глубокое знание учебно-программного материала, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии – 40 баллов

Типовые оценочные материалы промежуточной аттестации
Вопросы для подготовки к зачету с оценкой.

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 стран-участниц 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.

5.3. Показатели и критерии оценивания текущих и промежуточных форм контроля

5.3.1 Оценка по БРС за 10 семестр (очная форма)

Расчет ТКУ (ТКУ – текущий контроль успеваемости)

Сумма всех коэффициентов по текущему контролю успеваемости - 0,6.

максимальное кол-во баллов за семестр по устному опросу (УО) = $100 \times 0,1 = 10$

максимальное кол-во баллов за семестр по практическому заданию (ПЗ) = $100 \times 0,1 = 10$

максимальное кол-во баллов за семестр за доклад = $100 \times 0,2 = 20$

максимальное кол-во баллов за семестр за тестирование = $100 \times 0,2 = 20$

максимальная сумма баллов за семестр по ТКУ = $100 \times 0,6 = 60$

Расчет ПА (ПА – промежуточная аттестация) Зачёт с оценкой

Коэффициент по промежуточной аттестации - 0,4

Максимальное кол-во баллов за семестр по ПА = $100 \times 0,4 = 40$

Оценочные средства (наименование контрольной точки)	Коэффициент веса контрольной точки	Максимальное кол-во баллов за семестр	Показатели оценки	Критерии оценки
Устный опрос	0,1	10	Корректность и полнота ответов	Все ответы полные, развернутые, обоснованные 10 баллов
Практические задачи	0,1	10	Студенты получают формулировку проблемной ситуации профессиональной деятельности, для которой нужно найти решения с позиции участников ситуации. Оцениваются применение методов решения проблемных ситуаций, способность анализировать элементы ситуации, навыки, необходимые для профессиональной деятельности.	Полнота раскрытия темы задания и владение терминологией, правильные ответы на дополнительные вопросы 10 баллов
Доклад	0,2	20	Полнота доклада, оформление презентации и соответствие регламенту	Доклад, раскрывающий тему и оформленный в соответствии с требованиями СЗИУ РАНХИГС. 20 баллов
Тестирование	0,2	20	Тестирование проходит с использованием LMS Moodle или в письменной форме. Обучающий-	85-100 % правильно выполненных заданий 20 баллов

			ся получает определённое количество тестовых заданий. На выполнение выделяется фиксированное время в зависимости от количества заданий. Оценка выставляется в зависимости от процента правильно выполненных заданий.	
Всего	0,6	60	Зачет нацелен на комплексную проверку освоения дисциплины, проводится в устной форме по билетам, в которых содержатся вопросы по всем темам курса. Обучающемуся даётся время на подготовку. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.	Обучающийся обнаружил всестороннее, систематическое и глубокое знание учебно-программного материала.
Зачет с оценкой	0,4	40		
Дополнительное (компенсирующее) задание				максимальное кол-во баллов за семестр за дополнительное задание – 30 баллов

Итоговая балльная оценка по дисциплине по семестру= Результат ТКУ + Результат ПА

Система оценивания по заочной форме обучения за 12 семестр

- «Отлично» – теоретическое содержание курса освоено полностью, без пробелов необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено максимальным числом баллов.

- «Хорошо» – теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками.

- «Удовлетворительно»– теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий выполнены с ошибками.

- «неудовлетворительно»– теоретическое содержание курса освоено частично, пробелы носят существенный характер, необходимые практические навыки работы с освоенным материалом в основном не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, некоторые из выполненных заданий выполнены с ошибками.

5.4. Шкала оценивания

Оценка результатов производится на основе балльно-рейтинговой системы (БРС). Использование БРС осуществляется в соответствии с Приказом РАНХиГС №02-2531 от 12.12.2024 г "Об утверждении Положения о единой балльно-рейтинговой системе оценивания успеваемости студентов Академии и ее использовании при поведении текущей и промежуточной аттестации"

Схема расчетов доводится до сведения студентов на первом занятии по данной дисциплине, является составной частью рабочей программы дисциплины и содержит информацию по изучению дисциплины, указанную в Положении о балльно-рейтинговой системе оценки знаний обучающихся в РАНХиГС.

В соответствии с балльно-рейтинговой системой максимально-расчетное количество баллов за семестр составляет 100, из них в рамках дисциплины отводится:

60 баллов – на текущий контроль успеваемости;

40 баллов – на промежуточную аттестацию;

Формула расчета итоговой балльной оценки по дисциплине

Итоговая балльная оценка по дисциплине = Результат ТКУ + Результат ПА

В случае если студент в течение семестра не набирает минимальное число баллов, необходимое для сдачи промежуточной аттестации, то он может заработать дополнительные баллы, отработав соответствующие разделы дисциплины, получив от преподавателя компенсирующие задания.

В случае получения на промежуточной аттестации неудовлетворительной оценки студенту предоставляется право повторной аттестации в срок, установленный для ликвидации академической задолженности по итогам соответствующей сессии. Студент, набравший в течение семестра сумму баллов, достаточную для получения оценки "зачтено" и "удовлетворительно" (55 баллов) может получить оценку без прохождения промежуточной аттестации. В таком случае студент обязан выразить свое согласие на получение оценки без прохождения промежуточной аттестации. Студент вправе отозвать свое согласие на получение оценки без прохождения промежуточной аттестации не более одного раза и не позднее, чем за один день до начала промежуточной аттестации. Если студент хочет получить более высокую оценку, он должен пройти промежуточную аттестацию. Студент имеет право выразить свое согласие на получение оценки без прохождения промежуточной аттестации и отозвать соответствующее согласие только в период после получения баллов за все контрольные точки в рамках текущего контроля успеваемости и не позднее 1 (одного) рабочего дня до даты начала промежуточной аттестации по дисциплине.

Система перевода итоговой балльной оценки в традиционную и бинарную

таблица

Итоговая балльная оценка по БРС РАНХиГС	Традиционная система	Бинарная система
95-100	Отлично	зачтено
85-94		
75-84	Хорошо	
65-74		
55-64	Удовлетворительно	
0-54	Неудовлетворительно	не зачтено

6. Методические материалы по освоению дисциплины

При подготовке к лекционным занятиям студенту следует ознакомиться с учебно-тематическим планом изучаемой учебной дисциплины, а также с Календарным планом прохождения соответствующего курса - с тем, чтобы иметь возможность вспомнить уже пройденный материал данного курса и на этой основе подготовиться к восприятию новой информации, следуя логике изложения курса преподавателем-лектором.

В процессе лекционного занятия студент ведет свой конспект лекций, делая записи, касающиеся основных тезисов лектора. Это могут быть исходные проблемы и вопросы, ключевые понятия и их определения, важнейшие положения и выводы, существенные оценки и т. д.

В заключительной части лекции студент может задать вопросы преподавателю по содержанию лекции, уточняя и уясняя для себя теоретические моменты, которые остались ему непонятными.

Стоит отметить, что необходимо также систематическая самостоятельная работа студента. Самостоятельная работа студента, прежде всего, подразумевает изучение им учебной и научной литературы, рекомендуемой рабочей программой дисциплины и программой курса.

Занятия по дисциплине проводятся в следующей форме:

Ознакомление с материалом опорного конспекта, размещенного в соответствующем разделе дисциплины на базе образовательной платформы LMS MOODLE по каждой из тем, предусмотренной настоящей РПД. Важным моментом в предварительном ознакомлении с опорным конспектом является предупреждение пассивности студентов и обеспечение активного восприятия и осмысления ими новых знаний. Определяющее значение в решении этой задачи имеют два дидактических условия:

1) во-первых, само изложение материала педагогом должно быть содержательным в научном отношении, живым и интересным по форме;

2) во-вторых, в процессе изложения материала опорного конспекта необходимо применять особые педагогические приемы, возбуждающие мыслительную активность студентов и способствующие поддержанию их внимания

Один из этих приемов – *создание проблемной ситуации*. Самым простым в данном случае является достаточно четкое определение темы нового материала и выделение тех

основных вопросов, в которых надлежит разобраться студентам.

Термин **«практическое занятие»** используется в педагогике как родовое понятие, включающее такие виды, как лабораторную работу, семинар в его разновидностях. Аудиторные практические занятия играют исключительно важную роль в выработке у студентов навыков применения полученных знаний для решения практических задач в процессе совместной деятельности с преподавателями.

Если опорный конспект закладывает основы научных знаний в обобщенной форме, практические занятия призваны углубить, расширить и детализировать эти знания, содействовать выработке навыков профессиональной деятельности. Практические занятия развивают научное мышление и речь студентов, позволяют проверить их знания, в связи с чем, упражнения, семинары, лабораторные работы выступают важным средством достаточно оперативной обратной связи.

Для успешной подготовки к практическим занятиям студенту требуется предварительная самостоятельная работа по теме планируемого занятия. Не может быть и речи об эффективности занятий, если студенты предварительно не поработают над опорным конспектом, учебником, учебным пособием, чтобы основательно овладеть теорией вопроса.

Практические занятия служат своеобразной формой осуществления связи теории с практикой. Структура практических занятий в основном одинакова – вступление преподавателя, вопросы студентов по материалу, который требует дополнительных разъяснений, собственно практическая часть, заключительное слово преподавателя. Разнообразие возникает в основной, собственно практической части, доклады, дискуссии, тренировочные упражнения, решение задач, наблюдения, и т. д.

Семинарские занятия как форма обучения имеют давнюю историю, восходящую к античности. Само слово «семинар» происходит от латинского «*seminarium*» – рассадник и связано с функциями «посева» знаний, передаваемых от учителя к ученикам и «прорастающих» в сознании учеников, способных к самостоятельным суждениям, к воспроизведению и углублению полученных знаний.

Семинар является одним из основных видов практических занятий. Он представляет собой средство развития у студентов культуры научного мышления. Семинар предназначен для углубленного изучения дисциплины, овладения методологией научного познания. Главная цель семинарских занятий – обеспечить студентам возможность овладеть навыками и умениями использования теоретического знания применительно к особенностям изучаемой отрасли. На семинарах решаются следующие педагогические задачи:

- развитие творческого профессионального мышления;
- познавательная мотивация;
- профессиональное использование знаний в учебных условиях.

Кроме того, в ходе семинарского занятия преподаватель решает и такие частные задачи, как:

- повторение и закрепление знаний;
- контроль;
- педагогическое общение.

Для подготовки к семинарским занятиям студенты имеют доступ к электронным правовым базам «Кодекс», «Гарант», «Консультант» в интернет-классе научной библиотеки СЗИУ, а также к электронной полнотекстовой базе журнальных статей «Интегрум» с сайта научной библиотеки СЗИУ РАНХиГС.

Интерактивные методы на лекциях

Интерактивное обучение обеспечивает взаимопонимание, взаимодействие, взаимообогащение. Интерактивные методики ни в коем случае не заменяют лекционный материал, но способствуют его лучшему усвоению и, что особенно важно, формируют мнения, отношения, навыки поведения.

«Мозговая атака», «мозговой штурм» – это метод, при котором принимается любой ответ обучающегося на заданный вопрос. Важно не давать оценку высказываемым точкам зрения сразу, а принимать все и записывать мнение каждого на доске или листе бумаги. Участники должны знать, что от них не требуется обоснований или объяснений ответов. «Мозговой штурм» – это простой способ генерирования идей для разрешения проблемы. Во время мозгового штурма участники свободно обмениваются идеями по мере их возникновения, таким образом, что каждый может развивать чужие идеи.

Мини-лекция является одной из эффективных форм преподнесения теоретического материала. Перед объявлением какой-либо информации преподаватель спрашивает, что знают об этом студенты. После предоставления какого-либо утверждения преподаватель предлагает обсудить отношение студентов к этому вопросу.

Презентации с использованием различных вспомогательных средств с обсуждением.

К интерактивным методам относятся презентации с использованием различных вспомогательных средств: доски, книг, видео, слайдов, компьютеров и т.п. Интерактивность обеспечивается процессом последующего обсуждения.

Обратная связь - Актуализация полученных на лекции знаний путем выяснения реакции участников на обсуждаемые темы.

Лекция с заранее объявленными ошибками позволяет развить у обучаемых умение оперативно анализировать профессиональные ситуации, выступать в роли экспертов, оппонентов, рецензентов, выделять неверную и неточную информацию.

Интерактивные методы на практических занятиях (семинарах)

Разминка способствует развитию коммуникативных навыков (общению). Она должна быть уместна по содержанию, форме деятельности и продолжительности. Вопросы для разминки не должны быть ориентированы на прямой ответ, а предполагают логическую цепочку из полученных знаний, т.е. конструирование нового знания.

Дискуссия – одна из важнейших форм коммуникации, плодотворный метод решения спорных вопросов и вместе с тем своеобразный способ познания. Дискуссия предусматривает обсуждение какого-либо вопроса или группы связанных вопросов компетентными лицами с намерением достичь взаимоприемлемого решения. Дискуссия является разновидностью спора, близка к полемике, и представляет собой серию утверждений, по очереди высказываемых участниками.

Деловая или ролевая игра. Имитируются реальные условия, отрабатываются конкретные специфические операции, моделируется соответствующий рабочий процесс.

При изучении дисциплины студент должен не только ознакомиться с содержанием нормативных актов, приведенных в списке рекомендуемой литературы, но и научиться применять полученные знания на практике, к конкретным ситуациям. Для этого рекомендуется составлять самостоятельно схемы, рисунки, таблицы, другой иллюстративный материал, подобрать практические примеры.

Студентам очной формы обучения при подготовке к практическому занятию следует внимательно ознакомиться с содержанием конспекта лекции, выучить основные понятия, которые были рассмотрены в ходе лекции. Необходимо изучить положения международных конвенций, законодательных и нормативно-правовых актов, перечень которых приведен в каждой теме. Для облегчения понимания и усвоения положений законодательства предназначен перечень вопросов для подготовки к занятиям. Затем следует рассмотреть учебный материал, содержащийся в списке основной литературы, рекомендуемой к изучению, дополнив конспект лекции той информацией, которая, по мнению студента, позволяет углубить и уточнить его знания по тому или иному вопросу.

Проработав обязательный учебный материал, студенту рекомендуется обратиться к дополнительным источникам информации (официальный сайт ФТС России www.customs.ru, сайты Интернет, например, www.vch.ru, www.garant.ru, www.tks.ru, www.tamognia.ru, фонды библиотеки СЗИУ РАНХиГС, в том числе электронной

библиотеки, вновь изданные учебные пособия, публикации в специализированных изданиях, справочные правовые системы «КонсультантПлюс», «Гарант») в целях сбора и анализа дополнительной информации по теме практического занятия, которая позволит студенту активно участвовать в обсуждении выносимых на практическое занятие вопросов, например данные таможенной и других видов статистики, характеризующие основные тенденции перемещения физическими лицами товаров, транспортных средств, валюты через таможенную границу и другие.

Тематика докладов носит рекомендательный характер и может быть уточнена по согласованию с преподавателем, ведущим практические занятия, с учетом содержания публикаций в средствах массовой информации и на Интернет - сайтах. Доклады должны опираться на нормы права ЕАЭС, законодательства Российской Федерации о таможенном регулировании, носить проблемный характер, отражать содержание не менее 3-4 источников, с момента выпуска (публикации) которых прошло не более 2 лет. При подготовке докладов студент должен совершенствовать навыки проведения научного исследования, критически оценивать собранную информацию, уметь выделять главное, второстепенное и делать краткие выводы из изложенного материала.

Излагая материал доклада, студент должен уметь поставить проблемные вопросы, подлежащие обсуждению, быть готовым предложить свои ответы на них, уметь приводить аргументы в подтверждение своих предположений, активно участвовать в обсуждении проблем, поставленных другими студентами.

Подготовленный презентационный материал должен быть хорошо структурирован, помогать докладчику и слушателям выделять главное, акцентировать внимание на важных, значимых моментах, а также дополнять доклад с помощью различных средств визуализации. Не допускается выносить на слайды текст доклада целиком, превращая слайды в титры. Не допускается в тексте доклада дублировать текст, выведенный на слайд.

При подготовке к практическому занятию студенту, независимо от подготовки доклада, следует обязательно подготовить устные ответы по всем вопросам, выносимым на практическое занятие.

Активное участие в обсуждении рассматриваемых вопросов является основанием для оценки качества самостоятельной работы как докладчика, так и других студентов, участвующих в обсуждении проблемы.

Студентам заочной формы обучения при выполнении задания следует внимательно ознакомиться с содержанием основной литературы, рекомендуемой к изучению; составить опорный конспект; выделить основные понятия темы. Проработав обязательный учебный материал, студенту рекомендуется обратиться к содержанию законодательных и нормативно-правовых актов, дополнительным источникам информации, Интернет-сайтам в целях сбора и анализа дополнительной информации по теме, которая позволит студенту углубить полученные знания.

После изучения теории следует приступить к выполнению задания для самостоятельной работы. Обзор публикаций должен содержать информацию из 5–6 источников, анализ содержания этих публикаций в привязке к нормам права ЕАЭС и законодательства Российской Федерации о таможенном деле, полностью раскрывать тему.

Студент должен продемонстрировать знание норм права, навыки проведения научного исследования, умения критически оценивать собранную информацию, выделять главное, второстепенное и делать краткие выводы. Источники информации должны быть указаны в списке использованной литературы (автор, название материала, место и год издания, страницы, название сайта в Интернете).

Аттестационное испытание (экзамен, зачёт, в т.ч. дифференцированный) проводится преподавателем или экзаменационной комиссией для оценивания степени и уровня достижения результатов обучения. При прохождении аттестационного испытания студенты должны иметь при себе зачётные книжки, которые они перед началом аттестационного испытания предъявляют преподавателю или экзаменационной комиссии.

При проведении аттестационного испытания не допускается наличие у студентов посторонних объектов и технических устройств, способных затруднить (сделать невозможной) объективную оценку результатов аттестационного испытания, в т.ч. в части самостоятельного выполнения задания (подготовки к ответу на вопрос) студентом.

Продолжительность проведения аттестационного испытания, включая время подготовки студента к ответу на аттестационном испытании, проводимом в устной форме, составляет от 15 до 30 минут. При сдаче аттестационного испытания в устной форме по билетам студент, испытывающий затруднения при подготовке к ответу по выбранному билету, имеет право выбора второго билета с соответствующим продлением времени на подготовку к ответу. При этом оценка снижается на один балл при традиционной системе оценивания. Выбор третьего билета не допускается. Количество обучающихся, одновременно находящихся в аудитории при проведении аттестационного испытания определяется преподавателем

При проведении промежуточного контроля в билете или во вложении (дополнении) к билету может присутствовать на усмотрение преподавателя задание (задача, тест или другие формы контроля, допустимые при проведении аттестации), как один из элементов оценки при ответе.

Аттестационное испытание проводится преподавателем или экзаменационной комиссией для оценивания степени и уровня достижения результатов обучения. При прохождении аттестационного испытания студенты должны иметь при себе зачётные книжки, которые они перед началом аттестационного испытания предъявляют преподавателю или экзаменационной комиссии. При проведении аттестационного испытания не допускается наличие у студентов посторонних объектов и технических устройств, способных затруднить (сделать невозможной) объективную оценку результатов аттестационного испытания, в т.ч. в части самостоятельного выполнения задания (подготовки к ответу на вопрос) студентом.

Продолжительность проведения аттестационного испытания, включая время подготовки студента к ответу на аттестационном испытании, проводимом в устной форме, составляет от 15 до 30 минут. При сдаче аттестационного испытания в устной форме по билетам студент, испытывающий затруднения при подготовке к ответу по выбранному билету, имеет право выбора второго билета с соответствующим продлением времени на подготовку к ответу. При этом оценка снижается на один балл при традиционной системе оценивания. Выбор третьего билета не допускается. Количество обучающихся, одновременно находящихся в аудитории при проведении аттестационного испытания определяется преподавателем

7. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет», включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

7.1 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.

7.2.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. Олимпиаев. — 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.
4. Власенков, Г. Ю. Информационная безопасность таможенных технологий. Том 2 : монография / Г. Ю. Власенков, В. А. Карданов. — Москва : Юстиция, 2020. — 68 с. — URL: <https://book.ru/book/936066> — Текст: электронный. - Режим доступа: для авторизир. пользователей. — Режим доступа: для авториз. пользователей.
5. Ищейнов, В. Я. Информационная безопасность и защита информации: словарь терминов и понятий : словарь / В. Я. Ищейнов. — Москва : Русайнс, 2024. — 226 с. — URL: <https://book.ru/book/951881> .— Текст: электронный. - Режим доступа: для авторизир. пользователей. — Режим доступа: для авториз. пользователей.
6. Максимов Ю. А. Обеспечение информационной безопасности интеллектуального пункта пропуска при применении технологий искусственного интеллекта / Ю. А. Максимов, Ю. И. Сомов // Вестник Российской таможенной академии. - 2023. - № 3.
7. Прокушев, Я. Е. Программно-аппаратные средства защиты информации: лабораторный практикум : учебное пособие / Я. Е. Прокушев. — Санкт-Петербург : Интермедия, 2024. — 262 с. — ISBN 978-5-4383-0277-3. — Текст : электронный// Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/444998> (дата обращения: 12.04.2025). — Режим доступа: для авториз. пользователей.
8. Т.А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/560516>. — Режим доступа: для авториз. пользователей.
9. Сидоренко, Г. Г. Обеспечение безопасности в сфере таможенной деятельности: учебник / Г. Г. Сидоренко, В. И. Прасолов; Федеральное государственное образовательное бюджетное учреждения высшего образования "Финансовый университет при Правительстве Российской Федерации" (Финансовый университет). - Москва: Прометей,

2022: Текст: электронный. - URL: <https://www.iprbookshop.ru/125669.html>. — Режим доступа: для авториз. пользователей.

7.3 Нормативные правовые документы и иная правовая информация.

1. Конституция РФ.
2. Гражданский кодекс Российской Федерации, Федеральный закон Российской Федерации от 30.11.1994 № 51-ФЗ.
3. Договор о ЕАЭС.
4. Таможенный кодекс ЕАЭС.
5. Уголовный кодекс Российской Федерации.
6. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».
7. Федеральный закон Российской Федерации от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».
8. Федеральный закон от 03.08.2018 № 289-ФЗ «О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации».
9. Постановление Правительства РФ от 24.10.2013 № 940 «О принятии Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах».
10. Постановление Правительства РФ от 16.09.2013 № 809 «О Федеральной таможенной службе» (вместе с «Положением о Федеральной таможенной службе»).
11. Распоряжение Правительства РФ от 06.10.2021 № 2816-р «Прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года».
12. Распоряжение Правительства Российской Федерации от 23 мая 2020 г. N 1388-р «Стратегия развития таможенной службы Российской Федерации до 2030 года».
13. Приказ ГТК Российской Федерации от 26.09.2003 № 1069 «Об утверждении Концепции системы управления рисками в таможенной службе РФ».
14. Приказ ФТС России от 29.04.2021 N 358 "Об установлении Порядка подключения информационной системы информационного оператора к информационной системе таможенных органов".
15. Приказ ФТС России от 30.10.2020 № 949 "Об утверждении типовых положений об информационно-технических подразделениях региональных таможенных управлений".
16. Приказ ФТС России от 28.06.2021 № 535 "Об утверждении Положения по организации процессов жизненного цикла информационно-программных средств в таможенных органах".
17. 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».
18. 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».
19. Приказ ФТС России от 04.08.2015 № 1552 "О внесении изменений в приказ ФТС России от 6 июня 2012 г. N 1118".
20. Приказ ФТС России от 19.07.2021 № 616 "Об утверждении перечня типовых структурных подразделений таможенных органов Российской Федерации".
21. 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 подтвер-

ждения 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".

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

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

24. 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».

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

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

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

28. 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».

29. 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».

30. 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».

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

32. 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».

33. 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".

34. 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".

35. Решение Коллегии ЕЭК от 12.11.2013 № 254 (ред. от 06.03.2014) «О структурах и форматах электронных копий таможенных документов».
36. 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».
37. Письмо ФТС России от 22.06.2009 № 09-105/28328 «О направлении требований по техническому оснащению таможенных органов».
38. Письмо ФТС России от 28.03.2012 № 01-11/14513 «О применении технологии удаленного выпуска товаров».
39. Письмо ФТС России от 03.02.2016 № 14-112/04552 «О личном кабинете участника ВЭД».
40. 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».
41. 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".
42. 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».
43. Приказ ФТС России от 16.04.2012 № 699 «О реализации Соглашения о сотрудничестве Федеральной таможенной службы и Федеральной налоговой службы».
44. Приказ ФТС России от 24.04.2013 № 819 «О реализации Соглашения об информационном взаимодействии ФТС и Федеральной миграционной службы».
45. Приказ ФТС России от 10.02.2015 № 215 «Соглашение о порядке взаимодействия ФТС и Федеральной службы судебных приставов».
46. 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».

7.4 Интернет-ресурсы.

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

Русскоязычные ресурсы

1. Электронные учебники электронно-библиотечной системы (ЭБС) «Айбукс» https://sziu-lib.ranepa.ru/index.php?page_id=76&infres=1.
2. Электронные учебники электронно-библиотечной системы (ЭБС) «Лань» https://sziu-lib.ranepa.ru/index.php?page_id=76&infres=1.
3. Электронные учебники электронно-библиотечной системы (ЭБС) «Юрайт» https://sziu-lib.ranepa.ru/index.php?page_id=76&infres=1.
4. Электронные учебники Цифрового образовательного ресурса «IPR SMART» https://sziu-lib.ranepa.ru/index.php?page_id=76&infres=1.
5. Электронные учебники электронно-библиотечной системы (ЭБС) «ZNANIUM.COM» https://sziu-lib.ranepa.ru/index.php?page_id=76&infres=1.
6. Электронные учебники электронно-библиотечной системы (ЭБС) «BOOK.RU»

https://sziu-lib.ranepa.ru/index.php?page_id=76&infres=1.

7. Научно-практические статьи по экономике и менеджменту Издательского дома «Библиотека Гребенникова» https://sziu-lib.ranepa.ru/index.php?page_id=76.

8. Статьи из журналов и статистических изданий Ист Вью https://sziu-lib.ranepa.ru/index.php?page_id=76.

Англоязычные ресурсы

1. EBSCO Publishing – доступ к мультидисциплинарным полнотекстовым базам данных различных мировых издательств по бизнесу, экономике, финансам, бухгалтерскому учету, гуманитарным и естественным областям знаний, рефератам и полным текстам публикаций из научных и научно – популярных журналов.

2. Emerald – крупнейшее мировое издательство, специализирующееся на электронных журналах и базах данных по экономике и менеджменту. Имеет статус основного источника профессиональной информации для преподавателей, исследователей и специалистов в области менеджмента

7.5 Иные источники.

1. <http://www.government.ru> – интернет-портал Правительства Российской Федерации.

2. <http://www.gks.ru> – сайт Федеральной статистической государственной службы РФ.

3. <http://www.consultant.ru> – справочная правовая система Консультант Плюс.

4. <http://www.customs.ru> – сайт Федеральной таможенной службы РФ.

5. <http://www.customs.ru/index.php?option> – Итоговые отчеты ФТС России.

6. <http://www.economy.ru> – сайт Минэкономразвития РФ.

7. <http://www.cbr.ru> – официальный сайт Центрального Банка Российской Федерации.

8. <http://www.worldcustomsjournal.org> – международный таможенный электронный журнал.

9. <http://www.garant.ru> – справочная правовая система Гарант.

10. <http://www.www.edu.ru> – Федеральный портал «Российское образование».

11. <http://www.wcoomd.org/en/topics/facilitation/resources> – Компедиум ВТамО по управлению таможенными рисками

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

Под информационной технологией понимается процесс, использующий совокупность средств и методов сбора, обработки и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления (информационного продукта).

В последние годы термин «информационные технологии» часто выступает синонимом термина «компьютерные технологии», так как все информационные технологии в настоящее время так или иначе связаны с применением компьютера. Однако, термин «информационные технологии» намного шире и включает в себя «компьютерные технологии» в качестве составляющей. При этом, информационные технологии, основанные на использовании современных компьютерных и сетевых средств, образуют термин «Современные информационные технологии».

Виды информационных технологий:

«Ручная» информационная технология, инструментарий которой составляют: перо, чернильница, книга. Коммуникация осуществляется ручным способом (написание конспектов и т.д.). Основная цель технологии – представление информации в нужной форме.

«Механическая» технология, оснащенная более совершенными средствами передачи и доставки информации, инструментарий которой составляют: телефон, диктофон. Основная цель технологии – представление информации в нужной форме более удобными средствами.

«Электрическая» технология, инструментарий которой составляют: ксероксы,

портативные диктофоны. Основная цель информационной технологии начинает перемещаться с формы представления информации на формирование ее содержания.

«Электронная» технология, основным инструментарием которой становятся ЭВМ и создаваемые на их базе автоматизированные системы управления (АСУ) и информационно-поисковые системы, оснащенные широким спектром базовых и специализированных программных комплексов. Центр тяжести технологии еще более смещается на формирование содержательной стороны информации для управленческой среды различных сфер общественной жизни, особенно на организацию аналитической работы.

«Компьютерная» («новая») технология, основным инструментарием которой является персональный компьютер с широким спектром стандартных программных продуктов разного назначения (Excel, Word, Power Point). На этом этапе происходит процесс персонализации АСУ, который проявляется в создании систем поддержки принятия решений определенными специалистами. Подобные системы имеют встроенные элементы анализа и искусственного интеллекта для разных уровней управления, реализуются на персональном компьютере и используют телекоммуникации. В связи с переходом на микропроцессорную базу существенным изменениям подвергаются и технические средства бытового, культурного и прочего назначений.

«Сетевая технология» (иногда ее считают частью компьютерных технологий) только устанавливается. Начинают широко использоваться в различных областях глобальные и локальные компьютерные сети. Ей предсказывают в ближайшем будущем бурный рост, обусловленный популярностью ее основателя – глобальной компьютерной сети Internet.

**Описание материально-технической базы,
необходимой для осуществления образовательного процесса
по дисциплине**

№ п/п	Наименование
1.	Специализированная мебель и оргсредства: аудитории и компьютерные классы, оборудованные посадочными местами (в том числе для проведения занятий лабораторного типа).
2.	Технические средства обучения: Многофункциональный мультимедийный комплекс в лекционной аудитории; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов.
3.	Персональные компьютеры с доступом к электронному каталогу, полнотекстовым базам, подписным ресурсам и базам данных научной библиотеки СЗИУ РАНХиГС.
4.	Технические средства обучения: Персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV.
5.	компьютерные классы -в которых установлены программные средства ВЭД-Декларант, ВЭД-Инфо, 5 программными средствами Альта-Максимум и доступом в Интернет
6.	Тематическая аудитория «Таможенное дело в России» - оснащена средствами мультимедиа, доской, демонстрационными материалами, отражающими процессы осуществления таможенного контроля и таможенных операций.