

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Андрей Драгомирович Хлутков
Должность: директор
Дата подписания: 10.09.2026 23:19:48
Уникальный программный ключ:
880f7c07c583b07b775f6604a630281b13ca9d2

**Федеральное государственное бюджетное образовательное
учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
Северо-Западный институт управления - филиал РАНХиГС
«ФАКУЛЬТЕТ БЕЗОПАСНОСТИ И ТАМОЖНИ**

КАФЕДРА ТАМОЖЕННОГО АДМИНИСТРИРОВАНИЯ»

УТВЕРЖДЕНО

Директор

Северо-Западный института
управления - филиала РАНХиГС

Хлутков А.Д.

ПРОГРАММА СПЕЦИАЛИТЕТА

«информационно-аналитическая деятельность в таможенном деле»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Б1.В.11 «Основы информационной безопасности в таможенных
органах»**

ОИБТО

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

38.05.02 «Таможенное дело»

Квалификация: специалист таможенного дела

Формы обучения: очная, заочная

Год набора - 2022

Автор–составитель:

Старший преподаватель кафедры таможенного администрирования

Ю.Б. Тубанова

Врио Заведующего кафедрой

таможенного администрирования

д с/х.н.

Р.Х.Кочкаров

РПД одобрена на заседании кафедры таможенного администрирования. Протокол от (30.08.2022) № 1

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

1.1. Дисциплина Б1.В.11 «Основы информационной безопасности в таможенных органах» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКс3	Владение навыками управления и анализа больших объемов данных с применением передовых инструментов и методов автоматической обработки структурированной и неструктурированной информации в целях обеспечения безопасности цепей поставок товаров и транспортных средств.	ПКс3.2	Исследует порядок использования больших объемов данных с применением передовых инструментов и методов автоматической обработки структурированной и неструктурированной информации в целях обеспечения безопасности цепей поставок товаров и транспортных средств

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Профессиональные действия	Код этапа освоения компетенции	Результаты обучения
Осуществление информационной безопасности при осуществлении таможенных операций с товарами и транспортными средствами и при таможенном контроле Осуществление применения принципов и методов анализа угроз и опасностей, разработки и принятия управленческих решений в области информационной	ПКс-3.2	на уровне знаний: основы информационной безопасности в целях информационного сопровождения профессиональной деятельности таможенных органов
		на уровне умений: выявлять основные факторы, влияющие на процессы обеспечения информационной безопасности таможенного органа; - осуществлять анализ состояния информационной безопасности таможенного органа; - принимать рациональные управленческие решения по обеспечению информационной безопасности таможенного органа в различных условиях обстановки)
		на уровне навыков: практического применения принципов и методов анализа угроз и опасностей, разработки и принятия управленческих решений в области информационной безопасности; организации работы подразделения

безопасности таможенных	В	информационной безопасности таможенных органов на основе современной концепции информационной безопасности
-------------------------	---	--

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

Объем дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы или 72 академических часа.

Для очной формы обучения трудоемкость контактной работы с преподавателем составляет 36 академических часа (из них 18 часов – лекций, 18 часов – практических занятий), самостоятельной работы – 36 академических часа.

Для заочной формы обучения трудоемкость контактной работы с преподавателем составляет 10 академических часов (из них 4 часа – лекции, 6 часов – практические занятия), самостоятельной работы – 58 академических часов, контроль 4 часа.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.11 «Основы информационной безопасности в таможенных органах» включена в состав дисциплин вариативного профессионального цикла учебного плана подготовки специалистов по специальности 38.05.02 «Таможенное дело».

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

Дисциплина реализуется с применением дистанционных образовательных технологий

3. Содержание и структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.					СР	Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий					
			Л	ЛР	ПЗ	КСР		
Тема 1	Информационная безопасность в современной системе таможенных органов	13	2		2		9	Т, ПЗ
Тема 2	Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов	17	4		4		9	Т, УО
Тема 3	Понятие и структура информационной безопасности. Характер и формы угроз. Каналы утечки информации в таможенных органах. Формы обеспечения	21	6		6		9	Т, Д

	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	21	6		6		9	Т, УО
Промежуточная аттестация:								Зачет
Всего:		72	18		18		36	

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

Заочная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.					СР	Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий					
			Л	ЛР	ПЗ	КСР		
Тема 1	Информационная безопасность в современной системе таможенных органов	6	0		1		6	УО, Д-Д
Тема 2	Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов	8	2		2		6	УО, Д-Д, СЗ
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.	8	0		1		6	УО, Д-Д, Т
Тема 4	Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности. таможенного органа	6	2		2		6	УО, Д-Д, Т
Промежуточная аттестация:								Зачет
Всего:		72	4		6		58	4

Условные обозначения: Т – тестирование, ПЗ – практические задачи, УО – устный опрос, 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 и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации:

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

в том числе, задания к контрольным точкам):

Т – тестирование, УО – устный опрос, ПЗ – практическое задание,

Д – доклад.

4.2. Материалы текущего контроля успеваемости обучающихся

Полный перечень типовых оценочных материалов находится в ФОСе по дисциплине.

Тема 1. Информационная безопасность в современной системе таможенных органов.

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:

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

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.

По степени функциональности информационные системы бывают:

-) геоинформационные, финансовые, кадровые;
-) производственные, документальные, финансовые, кадровые;
-) фактографические, документальные, геоинформационные;
-) производственные, маркетинговые, финансовые, кадровые.

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.

Ключи электронной подписи — это:

-) уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;
-) уникальная последовательность символов, предназначенная для создания электронной подписи;
-) 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;
-) 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.

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.

По степени функциональности информационные системы бывают:

-) геоинформационные, финансовые, кадровые;
-) производственные, документальные, финансовые, кадровые;
-) фактографические, документальные, геоинформационные;

-) производственные, маркетинговые, финансовые, кадровые.

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.

Защита информации – это...

-) комплекс мероприятий, направленных на обеспечение информационной безопасности;
-) процесс разработки структуры базы данных в соответствии с требованиями пользователей;
-) 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?

-) международно-правовые нормы;
-) национально-правовые нормы;
-) 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.

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:

) 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;

) 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;

) 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;

) 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?

-) документ, подтверждающий право на занятие определённой деятельностью;
-) разрешение на въезд в страну;
-) сертификат на покупку товаров;
-) 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?

-) лицензии;
-) патенты;
-) разрешения;
-) 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.

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.

Обладатель информации имеет право:

) защищать от незаконного использования информации, способами в рамках закона;

) использовать информацию по своему усмотрению;

) использовать конфиденциальную инф другого обладателя без его ведома;

) 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?

) только сбор персональных данных;

) сбор и хранение персональных данных;

) сбор, хранение, распространение и использование персональных данных без согласия субъекта;

) 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?

-) открытый ключ;
-) закрытый ключ;
-) общий ключ;
-) 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?

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

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

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

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

5. Оценочные материалы промежуточной аттестации по дисциплине

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:	х	0,6	60

Формула расчета результата контрольной точки:

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

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
Количество правильных ответов	0	Количество правильных ответов менее 55%
	25	Количество правильных ответов от 55% до 64%
	50	Количество правильных ответов от 65% до 74%
	75	Количество правильных ответов от 75% до 84%
	100	Количество правильных ответов от 85% до 100%
Итого максимально:	100	

2. Критерии оценивания практических заданий (ПЗ):

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

3. Критерии оценивания устного опроса (УО):

Критерии оценки	Диапазон баллов	Описание критерия
Качество правильных ответов	0-54	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.
	55-64	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои

		примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
	65-84	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
	85-100	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.
Итого максимально:		100

4. Критерии оценивания доклада (Д):

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

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.

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

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.

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	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать	По степени функциональности информационные системы бывают:) геоинформационные, финансовые, кадровые;) производственные, документальные, финансовые,

нескольких вариантов предложенных	предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	кадровые;) фактографические, документальные, геоинформационные;) производственные, маркетинговые, финансовые, кадровые.	
		Защита информации – это...) комплекс мероприятий, направленных на обеспечение информационной безопасности;) процесс разработки структуры базы данных в соответствии с требованиями пользователей;) небольшая программа для выполнения определенной задачи.	
		) Какова основная цель обеспечения информационной безопасности таможенных органов?) Защита конфиденциальной информации.) Обеспечение бесперебойной работы таможенных систем.) Защита от кибератак и мошенничества.) 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. Владелец информации имеет право: а) защищать от незаконного использования информации, способами в рамках закона; б) использовать информацию по своему усмотрению; в) использовать конфиденциальную инф другого владельца без его ведома; г) разрешать или ограничивать доступ к информации.
Задание закрытого типа на установление последовательности	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	1. Расставьте в порядке убывания по степени серьезности потенциальные информационные угрозы безопасности:) Несанкционированный доступ к конфиденциальной информации;) Вредоносное программное обеспечение;) Случайное удаление важных данных сотрудником;) Физическое повреждение серверов и другого оборудования. 2. Расположите в хронологическом порядке основные этапы формирования доктрины информационной безопасности России, начиная с самого раннего: а) Принятие Доктрины информационной безопасности Российской Федерации в её нынешнем виде; б) Разработка и утверждение основ политики обеспечения информационной безопасности в РФ в) Создание нормативно-правовой базы для защиты информационной инфраструктуры страны; г) Формирование концепции

		информационной безопасности на основе анализа внешних и внутренних угроз
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	1. Одно из наиболее общих понятий науки, обозначающее некоторые сведения, совокупность каких-либо данных, знаний и т. п.?) Разъяснение;) Информация;) Справка;) Информирование.
		2. Классификация информации по категории доступа подразделяется на: 1) Публичную, массовую и конфиденциальную; 2) Общедоступную и конфиденциальную; 3) Массовую и доступ к которой ограничен ФЗ; 4) Общедоступную и доступ к которой ограничен ФЗ
Задание открытого типа с развернутым ответом	1. Внимательно прочитать текст задания и понять суть вопроса. 2. Продумать логику и полноту ответа. 3. Записать ответ, используя четкие компактные формулировки. 4. В случае расчетной задачи записать решение и ответ	1. Персональные данные — это:
		2. что такое электронная подпись?

Критерии и шкала оценивания на основе БРС.

Критерии и балльная шкала определяются преподавателем

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок	40
Дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством	30-39

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

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.

6. Методические материалы по освоению дисциплины

Дисциплина «Основы информационной безопасности», изучается студентами на пятом курсе в 9 семестре. 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.

Кроме того, необходимо детальное изучение нормативно-правовых источников.

Значительную роль в изучении данной дисциплины выполняют семинарские занятия, которые призваны, прежде всего, закреплять теоретические знания, полученные в ходе прослушивания и запоминания лекционного материала, изучения источников, ознакомления с учебной и научной литературой. Тем самым семинары способствуют получению студентами наиболее качественных знаний, а также позволяют осуществлять со стороны преподавателя текущий контроль над успеваемостью студентов.

Семинарские занятия преподаватель может проводить в различных формах: обсуждение вопросов темы, заслушивание докладов по отдельным вопросам и их обсуждение, выполнение письменных работ, тестирование и решение практических задач.

Подчеркнем, что студент должен заранее уточнить форму проведения предстоящего практического (семинарского) занятия и ознакомиться с планом его проведения. В процессе подготовки к семинару студент самостоятельно аккумулирует знания путем изучения конспекта лекций и соответствующих разделов учебника, ознакомления с дополнительной литературой и источниками, рекомендованными к этому семинарскому занятию.

Отвечать на тот или иной вопрос студентам рекомендуется формулировать наиболее полно и точно, при этом нужно уметь логически грамотно выражать и обосновывать свою точку зрения, свободно оперировать понятиями и терминами.

Таким образом, посещение студентом лекционных занятий, активная самостоятельная работа, а также заметное участие на семинарских занятиях необходимы для подготовки и успешной сдачи экзамена как формы итогового контроля.

В процессе проведения семинарских занятий проводится тестирование либо в письменной, либо компьютерной форме. Компьютерная программа использует некий исходный, достаточно большой банк тестовых вопросов, формируя случайным образом для каждого студента индивидуальное тестовое задание, не совпадающее с тестовыми заданиями для других студентов; при этом учитывается и тематика вопросов – на основе Учебно-тематического плана по данной дисциплине.

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. 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.

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.

7.2.Дополнительная литература.

1. Алешин, Леонид Ильич. Информационные технологии: учеб. пособие / Л. И. Алешин - Москва : Литера, 2008. - 423 с. : ил. ; 20 см. - (Современная библиотека ; вып. 35). - Библиогр.: с. 412-416 (23 назв.) и в подстроч. примеч. - Др. кн. авт. на 4-й с. Обл..
2. Граничин, Олег Николаевич. Информационные технологии в управлении: учеб. пособие / О. Н. Граничин, В. И. Кияев. - М.: БИНОМ. Лаб. знаний [и др.], 2011. - 335 с.
3. Бундин М. В. Система информации ограниченного доступа и конфиденциальность // Вестник ННГУ. 2015. №1. URL: <https://cyberleninka.ru/article/n/sistema-informatsii-ogranichennogodostupa-i-konfidentsialnost>
4. Верютин Владимир Николаевич Отдельные аспекты защиты государственной тайны в Российской Федерации // Вестник ВИ МВД России. 2009. №2. URL: <https://cyberleninka.ru/article/n/otdelnye-aspekty-zaschity-gosudarstvennoy-tayny-v-rossiyskoy-federatsii>
5. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 261 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. — Режим доступа: www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1
6. Гайдарева Инна Николаевна Правовое обеспечение информационной безопасности в России // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2009. №1. URL: <https://cyberleninka.ru/article/n/pravovoe-obespechenie-informatsionnoy-bezopasnosti-v-rossii>
7. Гильмуллина Динара Абдурауфовна Государственная тайна в правовом государстве // Известия ОГАУ. 2014. №2. URL: <https://cyberleninka.ru/article/n/gosudarstvennaya-tayna-v-pravovom-gosudarstve>
8. Гильмуллина Динара Абдурауфовна, Чикенёва Ирина Валерьевна О защите персональных данных в системе трудовых правоотношений // Известия ОГАУ. 2014. №3. URL: <https://cyberleninka.ru/article/n/o-zaschite-personalnyh-dannyh-v-sisteme-trudovyh-pravootnosheniy>
9. Е.К. Волчинская Место персональных данных в системе информации ограниченного доступа // Право. Журнал Высшей школы экономики. 2014. №4. URL: <https://cyberleninka.ru/article/n/mesto-personalnyh-dannyh-v-sisteme-informatsii-ogranichenного-dostupa>
10. Жирнова Наталья Алексеевна Банковская и налоговая тайна в системе правовых режимов информации с ограниченным доступом // Ленинградский юридический журнал. 2012. №4. URL: <https://cyberleninka.ru/article/n/bankovskaya-i-nalogovaya-tayna-v-sisteme-pravovyh-rezhimov-informatsii-s-ogranichenным-dostupom>
11. Занин Константин Анатольевич Проблемы административно-правовой защиты информации ограниченного доступа // Вестник ВИ МВД России. 2010. №1. URL: <https://cyberleninka.ru/article/n/problemy-administrativno-pravovoy-zaschity-informatsii-ogranichenного-dostupa>
12. Зейналова И. Д., Османов М. Х. Правовое обеспечение информационной безопасности в российском информационном праве // Вестник СПИ. 2014. №1 (9). URL: <https://cyberleninka.ru/article/n/pravovoe-obespechenie-informatsionnoy-bezopasnosti-v-rossiyskom-informatsionnom-prave>
13. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5, 1000 экз. <http://znanium.com/catalog/product/423927>
14. Камалова Гульфия Гафиятовна Вопросы ограничения доступа к информации в системе государственного управления // Вестник Удмуртского университета. Серия «Экономика

- и право». 2015. №6. URL: <https://cyberleninka.ru/article/n/voprosy-ogranicheniya-dostupa-k-informatsii-v-sisteme-gosudarstvennogo-upravleniya>
15. Камалова Гульфия Гафиятовна Вопросы систематизации информации ограниченного доступа // Вестник Удмуртского университета. Серия «Экономика и право». 2016. №2. URL: <https://cyberleninka.ru/article/n/voprosy-sistematizatsii-informatsii-ogranichennogo-dostupa>
 16. Камалова Гульфия Гафиятовна О правовом режиме служебной тайны // Вестник Удмуртского университета. Серия «Экономика и право». 2014. №4. URL: <https://cyberleninka.ru/article/n/o-pravovom-rezhime-sluzhebnoy-tayny>
 17. Коротков Андрей Викентьевич, Зиновьева Елена Сергеевна Безопасность критических информационных инфраструктур в международном гуманитарном праве // Вестник МГИМО. 2011. №4. URL: <https://cyberleninka.ru/article/n/bezopasnost-kriticheskikh-informatsionnyh-infrastruktur-v-mezhdunarodnom-gumanitarnom-prave>
 18. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. — Режим доступа : www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7
 19. Хомяков Эдуард Геннадьевич Информационная безопасность как составляющая прав граждан Российской Федерации // Вестник Удмуртского университета. Серия «Экономика и право». 2011. №3. URL: <https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-sostavlyayuschaya-prav-grazhdan-rossiyskoy-federatsii>

7.3 Нормативные правовые документы.

1. Гражданский кодекс Российской Федерации, Федеральный закон Российской Федерации от 30.11.1994 № 51-ФЗ.
2. Таможенный кодекс ЕАЭС.
3. Уголовный кодекс Российской Федерации, Федеральный закон Российской Федерации от 13.06.1996 № 63-ФЗ.
4. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».
5. Федеральный закон Российской Федерации от 27.07. 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Федеральный закон Российской Федерации от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».
7. Федеральный закон Российской Федерации от 27.11.2010 № 311-ФЗ «О таможенном регулировании в Российской Федерации».
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. Федеральный закон Российской Федерации от 28.12.2010 № 394-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с передачей полномочий по осуществлению отдельных видов государственного контроля таможенным органам Российской Федерации».
10. Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».
11. Постановление Правительства Российской Федерации от 28.12.2011 № «О мерах по обеспечению перехода федеральных органов исполнительной власти и органов государственных внебюджетных фондов на межведомственное информационное взаимодействие в электронном виде» (вместе с «Правилами обеспечения перехода федеральных органов исполнительной власти и органов государственных внебюджетных

фондов на межведомственное информационное взаимодействие в электронном виде при предоставлении государственных услуг»).

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

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

14. Распоряжение Правительства РФ от 17.11.2008 №1662-р «О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года» (вместе с «Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года»).

15. Распоряжение Правительства Российской Федерации от 28.12.2012 г. № 2575-р «Стратегия развития таможенной службы Российской Федерации до 2020 года».

16. Приказ ГТК России от 08.09.2003 № 973 «Об утверждении инструкции о совершении таможенных операций при внутреннем и международном таможенном транзите товаров».

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

18. Приказ ГТК РФ от 13.05.2004 № 564 «Об утверждении Положения об организации проверок информационных систем, информационных технологий и средств их обеспечения, используемых участниками внешнеэкономической деятельности» (Зарегистрировано в Минюсте РФ 01.06.2004 № 5806).

19. Приказ ФТС России от 10.03.2006 № 192 «Об утверждении концепции системы предварительного информирования таможенных органов Российской Федерации».

20. Приказ ФТС России от 24.01.2008 № 52 «О внедрении информационной технологии представления таможенным органам сведений в электронной форме для целей таможенного оформления товаров, в том числе с использованием международной ассоциации сетей «Интернет»».

21. Приказ ФТС России от 22.08.2008 № 1025 «Об организации доступа к центральной базе данных валютного контроля при осуществлении таможенными органами валютного контроля».

22. Приказ ФТС России от 03.10.2008 № 1230 «Об утверждении Инструкции об особенностях совершения должностными лицами таможенных органов отдельных таможенных операций в отношении товаров и транспортных средств, перемещаемых через таможенную границу российской федерации, с использованием предварительной информации».

23. Приказ ФТС России от 25.11.2009 № 2141 «О вводе в эксплуатацию транспортной технологической подсистемы Единой автоматизированной информационной системы таможенных органов».

24. Приказ ФТС России от 03.02.2010 № 183 «Об утверждении Порядка организации процессов жизненного цикла программных средств информационных систем и информационных технологий таможенных органов».

25. Приказ ФТС России от 18.03.2010 № 510 «Об утверждении Порядка осуществления таможенных операций с товарами при прибытии на таможенную территорию Российской Федерации в морских портах и их перемещении из мест прибытия в места временного хранения».

26. Распоряжение ФТС России от 16.04.2010 № 96-р (ред. от 05.07.2011) «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»

27. 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».
28. Приказ ФТС России от 28.12.2010 № 2636 «Об утверждении порядка представления и форм отчетности лицами, осуществляющими деятельность в сфере таможенного дела».
29. Приказ ФТС России от 22.04.2011 № 845 «Об утверждении порядка совершения таможенных операций при таможенном декларировании в электронной форме товаров, находящихся в регионе деятельности таможенного органа, отличного от места их декларирования».
30. Приказ ФТС России от 01.09.2011 № 1789 «Об утверждении технологии контроля за перевозками товаров в соответствии с таможенной процедурой таможенного транзита с использованием автоматизированной системы контроля таможенного транзита с учетом взаимодействия с системой NCTS (АС КТТ-2)».
31. Приказ ФТС России от 25.10.2011 № 2187 «Об утверждении Положения об использовании участниками внешнеэкономической деятельности и лицами, осуществляющими деятельность в сфере таможенного дела, средств электронной подписи при реализации информационного взаимодействия с таможенными органами Российской Федерации» (Зарегистрировано в Минюсте РФ 27.12.2011 № 22786).
32. Приказ ФТС России от 10.02.2012 № 245 «Об утверждении порядка действий должностных лиц таможенных органов при работе с поручительством по обязательствам нескольких лиц при таможенном транзите товаров».
33. Приказ ФТС России от 14.02.2012 № 261 «О внесении изменений в приказ ФТС России от 3 февраля 2010 г. № 183».
34. Приказ ФТС России от 05.07.2012 № 1345 «Об утверждении порядка использования в рамках системы управления рисками предварительной информации о товарах, ввозимых на территорию Российской Федерации автомобильным транспортом, и транспортных средствах международной перевозки, перемещающих такие товары».
35. Приказ ФТС России от 06.06.2012 № 1118 «О вводе в эксплуатацию Системы управления ведомственной интегрированной телекоммуникационной сетью ФТС России».
36. Приказ Федеральной таможенной службы от 26.09.2012 № 1926 «Об утверждении перечня типовых структурных подразделений таможенных органов Российской Федерации».
37. Приказ ФТС России от 29.12.2012 № 2688 «Об утверждении Порядка представления документов и сведений в таможенный орган при помещении товаров на склад временного хранения (иные места временного хранения товаров), помещения (выдачи) товаров на склад временного хранения (со склада) и иные места временного хранения, представления отчетности о товарах, находящихся на временном хранении, а также порядка и условий выдачи разрешения таможенного органа на временное хранение товаров в иных местах» (Зарегистрировано в Минюсте России 25.06.2013 № 28894)
38. Приказ ФТС России от 11.02.2013 № 228 «Об утверждении Порядка уничтожения на территориях особых экономических зон или вывоза с территорий ОЭЗ в целях уничтожения товаров, помещенных под таможенную процедуру свободной таможенной зоны, и (или) упаковки и упаковочных материалов».
39. Приказ ФТС России от 18.06.2013 № 1115 «Об утверждении Порядка и технологий совершения таможенных операций в отношении товаров, включая транспортные средства, ввозимых (ввезённых) на территории портовых особых экономических зон или вывозимых с территорий портовых особых экономических зон».
40. Приказ ФТС России от 13.08.2013 № 1526 «Об утверждении концепции развития Единой автоматизированной информационной системы таможенных органов до 2020 года»

41. Приказ ФТС России от 02.09.2013 № 1643 «О внесении изменений в Порядок организации процессов жизненного цикла программных средств информационных систем и информационных технологий таможенных органов, утвержденный приказом ФТС России от 3 февраля 2010 г. № 183».
42. 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».
43. Приказ ФТС России от 03.02.2014 № 164 «О внесении изменений в Порядок организации процессов жизненного цикла программных средств информационных систем и информационных технологий таможенных органов, утвержденный приказом ФТС России от 3 февраля 2010 г. № 183».
44. Приказ ФТС России от 04.09.2014 № 1700 «Об утверждении Общего положения о региональном таможенном управлении и Общего положения о таможне». (Зарегистрировано в Минюсте России 24.12.2014 № 35376).
45. Распоряжение ФТС России от 18.02.2015 № 62-р «О проведении эксперимента по совершению таможенными органами таможенных операций при таможенном декларировании товаров, помещаемых под таможенную процедуру таможенного транзита, в электронной форме».
46. Приказ ФТС России от 13.03.2015 № 423 «Об утверждении Положения по организации процессов жизненного цикла информационно-программных средств в таможенных органах».
47. 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».
48. 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».
49. 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».
50. Приказ ФТС России от 21.10.2015 № 2133 «Об утверждении основных направлений развития информационно-коммуникационных технологий в таможенных органах Российской Федерации до 2030 года».
51. Распоряжение ФТС России от 14.04.2016 № 106-р «О проведении эксперимента».
52. Решение коллегии евразийской экономической комиссии от 08.12. 2010 № 494 «О порядке предоставления и использования таможенной декларации в виде электронного документа».
53. Решение комиссии таможенного союза от 09.12.2011 № 899 «О введении обязательного предварительного информирования о товарах, ввозимых на таможенную территорию Таможенного союза автомобильным транспортом».
54. Решение коллегии евразийской экономической комиссии от 17.09. 2013 № 196 «О введении обязательного предварительного информирования о товарах, ввозимых на единую таможенную территорию Таможенного союза железнодорожным транспортом».

55. Решение Коллегии Евразийской экономической комиссии (далее – ЕЭК) от 12.11.2013 № 254 (ред. от 06.03.2014) «О структурах и форматах электронных копий таможенных документов».
56. Решение Коллегии ЕЭК от 01.12.2015 № 158 «О введении обязательного предварительного информирования о товарах, ввозимых на таможенную территорию Евразийского экономического союза воздушным транспортом».
57. Письмо ФТС России от 22.06.2009 № 09-105/28328 «О направлении требований по техническому оснащению таможенных органов».
58. Письмо ФТС России от 28.03.2012 № 01-11/14513 «О применении технологии удаленного выпуска товаров».
59. Письмо ФТС России от 03.02.2016 № 14-112/04552 «О личном кабинете участника ВЭД».
60. «Соглашение о представлении и об обмене предварительной информацией о товарах и транспортных средствах, перемещаемых через таможенную границу Таможенного союза» (Заключено в г. Санкт-Петербурге 21.05.2010).
61. 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».
62. Приказ Минтранса России и ФТС России от 26.09.2011 № 254/1950 «Об утверждении Порядка информационного взаимодействия при осуществлении транспортного контроля в пунктах пропуска через государственную границу Российской Федерации».
63. 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».
64. Приказ ФТС России от 16.04.2012 № 699 «О реализации Соглашения о сотрудничестве Федеральной таможенной службы и Федеральной налоговой службы».
65. Приказ ФТС России от 24.04.2013 № 817 «О реализации Соглашения о взаимодействии Федеральной службы по оборонному заказу и Федеральной таможенной службы от 29 сентября 2010 г. № 01-69/41».
66. Приказ ФТС России от 24.04.2013 № 819 «О реализации Соглашения о взаимодействии Федеральной таможенной службы и Федеральной миграционной службы от 11 марта 2008 г. № 01-12/0005».
67. Приказ ФТС России от 10.02.2015 № 215 «О реализации Соглашения о порядке взаимодействия Федеральной таможенной службы и Федеральной службы судебных приставов при исполнении постановлений таможенных органов и иных исполнительных документов от 29 декабря 2014 г. № 0001/36/01-69/17».
68. Приказ ФТС России от 11.02.2015 № 233 «О реализации Соглашения о сотрудничестве Федеральной таможенной службы и Ассоциации производственных и торговых предприятий рыбного рынка».
69. 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».
70. Приказ ФТС России от 18.08.2015 № 1674 «О реализации Соглашения об информационном взаимодействии между Федеральной таможенной службой и Ассоциацией предприятий компьютерных и информационных технологий».
71. Приказ ФТС России от 03.11.2015 № 2229 «О реализации Соглашения об информационном взаимодействии между Федеральной таможенной службой и

Федеральной службой судебных приставов в электронном виде от 9 октября 2015 г. № 01-69/10/33».

7.4 Интернет-ресурсы.

Для освоения дисциплины следует пользоваться доступом через сайт научной библиотеки <http://nwapr.spb.ru/> к следующим подписным электронным ресурсам:

Русскоязычные ресурсы:

- официальный сайт Евразийского экономического союза <http://www.eaeunion.org/>;
- официальный сайт Евразийской экономической Комиссии <http://www.eurasiancommission.org/>;
- портал открытых данных Российской Федерации (<http://data.gov.ru/frontpage?language=ru>);
- официальный сайт Министерства финансов Российской Федерации (<http://minfin.ru/ru/>);
- официальный сайт ФТС России <http://customs.ru/>;
- Портал «Гуманитарное образование» <http://www.humanities.edu.ru/>
- Федеральный портал «Российское образование» <http://www.edu.ru/>
- Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» <http://school-collection.edu.ru/>
- Открытая электронная библиотека <http://www.elibrary.ru/>
- Справочная правовая система «Консультант Плюс».
- ЭБС «Znaniium.com» <http://www.pravo.gov.ru> Официальный интернет-портал правовой информации.
- <http://www.gdf.ru/> - фонд защиты гласности.
- <http://privacy.hro.org/> - сайт о проблемах обеспечения права на неприкосновенность частной жизни.
- <http://echr.ru/> - сайт о деятельности Европейского суда по правам человека.
- <http://www.elrussia.ru/> - материалы реализации ФЦП «Электронная Россия».
- <http://www.ogic.ru/> - федеральный портал государственных услуг населению.
- <http://www.internet-law.ru/> - центр «ИНТЕРНЕТ и право».
- <http://www.russianlaw.net/> - сайт о проблемах правового регулирования ИНТЕРНЕТ.
- электронные учебники электронно-библиотечной системы (ЭБС) «Айбукс»;
- электронные учебники электронно-библиотечной системы (ЭБС) «Лань»;
- статьи из периодических изданий по общественным и гуманитарным наукам «Ист-Вью»
- энциклопедии, словари, справочники «Рубриконт»;
- полные тексты диссертаций и авторефератов Электронная Библиотека Диссертаций РГБ.

Англоязычные ресурсы:

- **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.

- Таможенные службы государств-членов ЕС, кандидатов и других государств:
- Бельгия: <http://www.minfin.fgov.be/fr-admin/0006/index.html>
- Великобритания: <http://www.hmce.gov.uk/>
- Германия <http://www.zoll-d.de/>
- Греция: <http://www.gsis.gov.gr/>
- Дания: <http://www.toldskat.dk/>
- Ирландия: <http://www.revenue.ie/>

- Испания: <http://www.aeat.es/inicio.htm>
 - Италия: <http://www.finanze.it/utente/profili/profilo-06.htm>
 - Люксембург: <http://www.etat.lu/DO/>
 - Нидерланды: <http://www.belastingdienst.nl/>
 - Португалия: <http://www.dgaiec.min-financas.pt/sitedgaiec.nsf>
 - Финляндия: <http://www.tulli.fi/>
 - Франция: <http://www.finances.gouv.fr/DGDDI/>
 - Швеция: <http://www.tullverket.se/>
 - Болгария: <http://www.minfin.government.bg/en/index.html>
 - Венгрия: <http://www.vam.hu/>
 - Латвия: <http://www.vid.gov.lv/>
 - Литва: <http://www.cust.lt/>
 - Мальта: <http://www.business-line.com/depofcus/>
 - Польша: <http://www.guc.gov.pl/>
 - Румыния: <http://www.customs.ro/>
 - Словакия: <http://www.colnasprava.sk/cssr/>
 - Словения: <http://www.sigov.si/mf/angl/apredmf6.html>
 - Турция: <http://www.gumruk.gov.tr/>
 - Чехия: <http://www.cs.mfcr.cz/>
 - Эстония: <http://www.customs.ee/>
 - Андорра: <http://www.duana.ad/>
 - Израиль: <http://www.mof.gov.il/customs/>
 - Исландия: <http://www.tollur.is/>
 - Марокко: <http://www.douane.gov.ma/>
 - Норвегия: <http://www.toll.no/>
 - Хорватия: <http://www.carina.hr/>
 - Швейцария: <http://www.zoll.admin.ch/>
 - Комиссия Европейских сообществ: http://europa.eu.int/comm/taxation_customs/index-en.htm
 - База данных законодательства ЕС и решений Суда ЕС: <http://europa.eu.int/eur-lex>
<http://europa.eu.int/celex>
 - ВТО: <http://www.wto.org>
 - Всемирная таможенная организация: <http://www.wcoomd.org>
 - Европейская экономическая комиссия ООН: <http://www.unece.org>
 - Международная торговая палата: <http://www.iccwbo.org>
 - Интернет-сайт, посвященный вопросам европейского налогообложения и таможенного регулирования
http://ec.europa.eu/taxation_customs/common/about/welcome/index_en.htm
- Кроме вышеперечисленных ресурсов, используются следующие ресурсы сети Интернет:
<http://uristy.ucoz.ru/>; <http://www.garant.ru/>; <http://www.kodeks.ru/>

7.5 Иные источники.

В ходе образовательного процесса не используются.

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

Информационные средства обучения:

- Поисковые системы, используемые для поиска источников информации в сети

Интернет;

- Программные средства «Access», «Excel».

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

№ п/п	Наименование
1.	Специализированные компьютерные классы (2 класса) - оснащены 49-ю рабочими станциями ПК, на которых установлены программные средства ВЭД-Декларант, ВЭД-Инфо, 5 программными средствами Альта-Максимум и 4-мя досками (по 2 в каждом из классов), доступом в Интернет
2.	Специализированная аудитория «Лаборатория товароведения и экспертизы в таможенном деле» - оснащена средствами мультимедиа, 2-мя досками, демонстрационными материалами, отражающими процессы осуществления таможенного контроля и таможенных операций.
3.	Тематическая аудитория «Таможенное дело в России» - оснащена средствами мультимедиа, 2-мя досками, демонстрационными материалами, отражающими процессы осуществления таможенного контроля и таможенных операций.
4.	Специализированная аудитория «Лаборатория товароведения и экспертизы в таможенном деле» - оснащена средствами мультимедиа, 2-мя досками, демонстрационными материалами, отражающими процессы осуществления таможенного контроля и таможенных операций