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-Западного института
управления - филиала РАНХиГС
Хлутков А.Д.

ПРОГРАММА СПЕЦИАЛИТЕТА
Таможенные операции и таможенный контроль

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 – 2023

Автор–составитель:

Старший преподаватель кафедры таможенного администрирования Ю.Б. Тубанова

Преподаватель кафедры таможенного администрирования М.Н. Орел

Заведующий кафедрой
таможенного администрирования д-р мед. наук, проф. В.Ю. Чепрасов

РПД одобрена на заседании кафедры таможенного администрирования. Протокол от *25.05.2023* № *10.* С изменениями: Протокол от 29.08.2024 № 1.

СОДЕРЖАНИЕ

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 компонента компетенции	Наименование компонента 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:

ОТФ/ТФ (при наличии профстандарта)/ трудовые или профессиональные действия	Код компонента 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 таможенных органов и участников внешнеэкономической деятельности.	ПКо ОС-3.2	на уровне знаний: -особенности информационных процессов в таможенной сфере и основы повышения эффективности их работы; -информационные процессы и ресурсы информацию с целью выявления новых вызовов и угроз, пресечения противоправных деяний в таможенной сфере. 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: -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. 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: -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 России. Навыки информационно-технического контроля за процессуальными актами и документами, подтверждающих соблюдение запретов и ограничений; навыками применения соответствующих положений 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:

Вид работы	Трудоемкость в акад. Часах/астр Часах
Общая трудоемкость	**72/54**
Контактная работа с преподавателем	**36/27**
Лекции	**18/13,5**
Практические занятия	**18/13,5**
Лабораторные занятия	**0**
Самостоятельная работа	**36/27**
Консультация	
Контроль	
Формы текущего контроля	Т – тестирование, СЗ – ситуационные задачи, УО – устный опрос, Д – доклад,
Форма промежуточной аттестации	Зачет

Для заочной формы:

Вид работы	Трудоемкость в акад. Часах/астр Часах
Общая трудоемкость	**72/54**
Контактная работа с преподавателем	**10/7,5**
Лекции	**4/3**
Практические занятия	**6/4,5**
Лабораторные занятия	**0**
Самостоятельная работа	**58/43,5**
Консультация	
Контроль	**4/3**
Формы текущего контроля	Т – тестирование, СЗ – ситуационные задачи, УО – устный опрос, Д – доклад,
Форма промежуточной аттестации	Зачет

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.10 «Основы информационной безопасности в таможенных органах» включена в состав дисциплин вариативного профессионального цикла учебного плана подготовки специалистов по специальности 38.05.02 «Таможенное дело».

Дисциплина изучается в 9 семестре по очной форме и на 6 курсе в весеннем семестре по заочной форме 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

Дисциплина реализуется с применением дистанционных образовательных технологий

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	8	***4***		**4**		9	УО, Д
Тема 2	Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов	8	***4***		**4**		9	УО, 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	***4***		**4**		9	УО, Д, Т
Тема 4	Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности. таможенного органа.	8	***6***		**6**		9	УО, Д, Т
Промежуточная аттестация:								**Зачет**
Всего:		**72**	18		18		36	

Условные обозначения: Т – тестирование, СЗ – ситуационные задачи, УО – устный опрос, Д-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 обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ ДОТ	ЛР/ ДОТ	ПЗ/ ДОТ	КСР		
Тема 1	Информационная безопасность в современной системе таможенных органов	6	***0***		**0**		14	УО, Д-Д

№ 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 2	Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов.	8	***2***		**2**		14	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***		**2**		15	УО, Д-Д, Т
Тема 4	Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности.	6	***2***		**2**		15	УО, Д-Д, Т
Промежуточная аттестация:								**Зачет**
Всего:		**72**	**4**		**6**		**58**	4

Условные обозначения: Т – тестирование, СЗ – ситуационные задачи, УО – устный опрос, Д-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, таможенные 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.	УО, Д
Тема 2. Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов.	УО, 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.	УО, Д, Т
Тема 4. Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности. таможенного органа.	УО, Д, Т

.2. Материалы текущего контроля успеваемости обучающихся

Полный перечень типовых оценочных материалов находится в фонде оценочных средств по дисциплине.

Типовые оценочные материалы по теме 1 «Информационная безопасность в современной системе 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 органов России;
6. Концепция национальной безопасности и Доктрина информационной безопасности России.

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. Информационные системы для анализа таможенных данных;
5. Информационные таможенные системы.

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. Международная нормативная правовая база по вопросам информационной безопасности;
2. Структура нормативного правового обеспечения Российской Федерации в области информационной безопасности;
3. Характеристика основных угроз в информационной сфере для личности, общества и государства, таможенных органах России;
4. Классификация угроз информационной безопасности на различных уровнях управления таможенных органов;
5. Направления государственной политики РФ в сфере информатизации и информационной безопасности личности, общества, государства, таможенные органов России;
6. Структура внутреннего нормативного правового обеспечения информационной безопасности в ЕАЭС, таможенных органах ЕАЭС и России;
7. Понятие государственной тайны. Критерии отнесения информации к государственной тайне.

Темы для подготовки докладов:

1. Направления развития информационных таможенных технологи;
2. Информационные ресурсы таможенных органов;
3. Характеристика форм обеспечения информационной безопасности ЕАИС ФТС России;
4. Единая автоматизированная информационная система ФТС России как совокупность мер, обеспечивающих автоматизацию деятельности таможенных органов.

5. ЕАИС таможенных органов: проблемы и перспективы развития.

Ситуационные задачи:

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

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? 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.

3. В офисе компании один из сотрудников случайно утратил USB-флешку, 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.

4. 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 киберзащиты, аудит систем информационной безопасности, внедрение средств мониторинга, а также сотрудничество с силовыми структурами и специализированными органами.

5. 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 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»:

Вопросы для проведения устного опроса:

1. Роль и место системы обеспечения информационной безопасности в деятельности таможенных органов.;
2. Основные этапы процесса обеспечения информационной безопасности таможенных органов и их содержание;
3. Оценка эффективности мероприятий по обеспечению информационной безопасности;
4. Понятие коммерческой тайны и банковской тайны. Критерии охраноспособности прав на нее;
5. Нормативно-правовые документы, регламентирующие отношение к информации, содержащей коммерческую, банковскую, налоговую тайну в таможенных органах;

6. Угрозы и объекты обеспечения информационно-технической безопасности, принципы ее обеспечения;

7. Способы и средства предотвращения утечки информации;

8. Технология процесса обеспечения информационно-технической безопасности таможенных органов. Контроль состояния технической защиты информации.

Темы для подготовки докладов:

1. Анализа информационных рисков и управление ими;
2. Коммерческая тайна. Понятие и правовое регулирование;
3. Банковская тайна. Понятие и правовое регулирование.
4. Профессиональная тайна. Понятие и правовое регулирование;
5. Служебная тайна. Понятие и правовое регулирование;
6. Роль и место информационно-технической безопасности в работе таможенного органа;
7. Характеристики основных способов и средств информационно-психологического воздействия на должностных лиц таможенных органов.

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;

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

Вопросы для проведения устного опроса:

1. Понятие и виды юридической ответственности за нарушение правовых норм в области информационной безопасности;
2. Уголовно-правовая ответственность за нарушение правовых норм в области информационной безопасности;
3. Административная ответственность за нарушение правовых норм в сфере информационной безопасности;
4. Особенности юридической ответственности за нарушение правовых норм в области информационной безопасности в гражданско-правовых и трудовых отношениях;
5. Способы нарушений информационной безопасности в современных автоматизированных информационных системах;
6. Виды «вирусов» и защита от них;
7. Методы криптографии. Электронная подпись;
8. Методы и приемы информационно-психологического воздействия на должностных лиц.

Темы для подготовки докладов:

1. Структура нормативного правового обеспечения РФ в области информационной безопасности;
2. Международная нормативная база по вопросам информационной безопасности;
3. Структура внутреннего нормативного правового обеспечения информационной безопасности в ЕАЭС, ТО ЕАЭС и России:
4. Разрабатываемые в таможенных органах РФ документы по вопросам информационной безопасности;
5. Понятие государственной тайны. Критерии отнесения информации к государственной тайне.

Примеры тестовых вопросов:

1. Перечислите виды информационных систем по способу представления информации:

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

2. 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.

3. По степени функциональности информационные системы бывают:
1) Геоинформационные, финансовые, кадровые;
2) Производственные, документальные, финансовые, кадровые;
3) Фактографические, документальные, геоинформационные;
4) Производственные, маркетинговые, финансовые, кадровые.
4. Что относится к правовой защите информации?
1) Лицензии;
2) Патенты;
3) Нет верного варианта;
4) Верны оба варианта.
5. 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 проводятся с применением следующих методов:

Устный опрос по билетам. В каждом билете не менее 2- х вопросов. Один вопрос теоретической направленности, второй – практической направленности.

В ходе сдачи зачета студент решает задачу, по условиям которой предлагается с помощью имеющихся информационных систем найти требуемые сведения в области таможенного дела.

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 всестороннее, 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.

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

Оценочные средства	Показатели оценки	Критерии оценки
Устный опрос	Корректность и полнота ответов	Полный, развернутый, обоснованный ответ – 2 балла. Правильный, но неполный ответ – 1 балл. Неверный ответ – 0 баллов.
Практические (ситуационные) задачи	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, ответы на дополнительные вопросы – до 5 баллов
Доклад	Полнота доклада, оформление презентации и соответствие регламенту	Доклад, раскрывающий тему и оформленный в соответствии с требованиями СЗИУ РАНХИГС – 2 балла. Доклад, раскрывающий тему, но не оформленный в соответствии с установленными требованиями, либо не соответствующий регламенту – 1 балл. Доклад, не раскрывающий тему – 0 баллов
Тестирование	Тестирование проходит с использованием LMS Moodl или в письменной форме. Обучающийся получает определённое количество тестовых заданий. На выполнение выделяется фиксированное время в зависимости от количества заданий. Оценка выставляется в зависимости от процента правильно выполненных заданий	За 15 правильных вопросов 5 баллов
Зачет	Нацелен на комплексную проверку освоения дисциплины. проводится в	Обучающийся обнаружил всестороннее, систематическое

	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.	и глубокое знание учебно-программного материала, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии – 40 баллов

5.4. Шкала перевода оценки из многобалльной системы в систему зачета

Критерии оценки ответа на вопросы:

«Зачтено» ставится в том случае, если студент продемонстрирует знание основных понятий, относящихся к изучаемой дисциплине, правильно ответить, по крайней мере, на один дополнительный вопрос, в состоянии выполнить практическое действия. Ответ должен быть логичным и последовательным, либо студент способен уточнить содержание ответа

«Не зачтено» ставится в том случае, если студент не демонстрирует знание основных понятий, относящихся к изучаемой дисциплине, не отвечает ни на один дополнительный вопрос, и изложение ответа на вопрос не последовательное и не логичное. При этом, студент не в состоянии выполнить практическое действия.

Примечание к оценке ситуационной задачи: в ходе практического обеспечения информационной безопасности при оценке качества решения ситуационной задачи студентом следует исходить из того, насколько он убедительно сможет обосновать свой вариант решения с использованием регламентированной профессиональной терминологии.

Шкала оценивания.

Оценка результатов производится на основе балльно-рейтинговой системы (БРС). Использование БРС осуществляется в соответствии с приказом от 06 сентября 2019 г. №306 «О применении балльно-рейтинговой системы оценки знаний обучающихся».

Схема расчетов сформирована в соответствии с учебным планом направления, согласована с руководителем научно-образовательного направления, утверждена деканом факультета.

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:

40 баллов - на промежуточную аттестацию

40 баллов - на работу на практических занятиях

20 баллов - на посещаемость занятий

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.

51-100 балов - зачет
0-50 балов - незачет

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.

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 проводиться 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.

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»,

7.1 Основная литература.

1. . Башмаков, И. А. Информационное обеспечение перевозочного процесса: учебник / И. А. Башмаков, А. В. Олимпиев. — Москва: КноРус, 2024. — 196 с. — URL: https://book.ru/book/950242 — Текст: электронный. — Режим доступа: для авториз. пользователей.

2. Внуков, А.А. Защита информации: учебное пособие для вузов/ А.А. Внуков. — 3-е изд., перераб. и доп.— Москва: Издательство Юрайт, 2024. — (Высшее образование). — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL:https://urait.ru/bcode/537247. . — Режим доступа: для авториз. пользователей.

3. Зенков, А.В. Информационная безопасность и защита информации: учебное пособие для вузов / А.В. Зенков. — 2-е изд., перераб. и доп.— Москва: Издательство Юрайт, 2024. — (Высшее образование).— Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:https://urait.ru/bcode/544290— Режим доступа: для авториз. пользователей.

4. 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.

5. Полякова Т. А., Стрельцов А. А. Организационное и правовое обеспечение информационной безопасности: учебник. - Москва: Юрайт, 2024. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL:https://urait.ru/bcode/537247. . — Режим доступа: для авториз. пользователей.

6. 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 авторизир. пользователей. . — Режим доступа: для авториз. пользователей.

7. . Аксенов И. А. Цифровые технологии в таможенной и околотаможенной деятельности: учеб. пособие. - ISBN 978-5-9984-1698-9. изд. - Владимир: ВлГУ, 2022.

7.2.Дополнительная литература.

1. 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.

2. 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.

3. 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 (дата обращения: 25.04.2024). — Текст: электронный. - Режим доступа: для авторизир. пользователей. — Режим доступа: для авториз. пользователей.

4. 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.

7.3 **Нормативные правовые документы.**

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 подтверждения о регистрации документов, Порядка выдачи (отказа в выдаче) разрешения на проведение операций, указанных в пункте 2 статьи 102 Таможенного кодекса Евразийского экономического союза, определении Условий и Порядка выдачи (отмены) разрешения на временное хранение товаров в иных местах, Способа предоставления отчетности владельцами складов временного хранения и лицами, получившими разрешение на временное хранение в местах временного хранения товаров, форм отчетов, порядка их заполнения, а также порядка и сроков представления отчетности".
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 экономики 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.goverment.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 использование современных компьютерных и сетевых средств, образуют термин «Современные информационные технологии».

Виды информационных технологий:

«Ручная» информационная технология, инструментарий которой составляют: перо, чернильница, книга. Коммуникации 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.	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