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.

.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

ОИБТО

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

по специальности: 38.05.02 «Таможенное дело»

краткое наименование дисциплины (модуля)

Специализация «Таможенные операции и таможенный контроль»

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 программы

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

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
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 в таможенных		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.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».

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	ЛР	ПЗ	КСР	
Тема 1	Понятие и предмет информационной безопасности	8	***2***		**2**		4	УО, Д-Д
Тема 2	Доктрина информационной безопасности РФ. Национальные интересы России в информационной сфере и угрозы информационной безопасности	8	***2***		**2**		4	УО, Д-Д, СЗ
Тема 3	Угрозы информационной безопасности предприятия в условиях современной рыночной экономики	8	***2***		**2**		4	УО, Д-Д, Т
Тема 4	Нормативное правовое обеспечение информационной безопасности	8	***2***		**2**		4	УО, Д-Д, Т

	таможенного органа							
Тема 5	Риски и эффективность обеспечения информационной безопасности	8	***2***		**2**		4	УО, Д-Д, СЗ, Т
Тема 6	Коммерческая, банковская, налоговая и профессиональная тайна в системе обеспечения информационной безопасности таможенных органов	8	***2***		**2**		4	УО, Д-Д
Тема 7	Организация обеспечения информационной безопасности таможенных органов. Ответственность за совершение нарушение правовых норм в области информационной безопасности	8	***2***		**2**		4	УО, Д-Д
Тема 8	Информационно-техническая безопасность и информационно-психологическая безопасность таможенных органов	8	***2***		**2**		4	УО, Д-Д
Тема 9	Методы, способы и средства защиты информации в современных автоматизированных информационных системах; методы, способы и приемы информационно–психологической защиты должностных лиц таможенных органов, методы, способы и приемы информационно – психологической защиты должностных лиц таможенных органов	8	***2***		**2**		4	УО, Д-Д,
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 успеваемос**
		Всего	**Контактная работа обучающихся с преподавателем по видам учебных занятий**	**СР**	

			Л	**ЛР**	**ПЗ**	**КСР**		**ти*, промежуточной аттестации**
Тема 1	Понятие и предмет информационной безопасности	6	***0***		**0**		6	УО, Д-Д
Тема 2	Доктрина информационной безопасности РФ. Национальные интересы России в информационной сфере и угрозы информационной безопасности	8	***1***		**1**		6	УО, Д-Д, СЗ
Тема 3	Угрозы информационной безопасности предприятия в условиях современной рыночной экономики	8	***1***		**1**		6	УО, Д-Д, Т
Тема 4	Нормативное правовое обеспечение информационной безопасности таможенного органа	6	***0***		**0**		6	УО, Д-Д, Т
Тема 5	Риски и эффективность обеспечения информационной безопасности	9	***0***		**1**		8	УО, Д-Д, СЗ, Т
Тема 6	Коммерческая, банковская, налоговая и профессиональная тайна в системе обеспечения информационной безопасности таможенных органов	7	***0***		**1**		6	УО, Д-Д
Тема 7	Организация обеспечения информационной безопасности таможенных органов. Ответственность за совершение нарушение правовых норм в области информационной безопасности	8	***1***		**1**		6	УО, Д-Д
Тема 8	Информационно-техническая безопасность и информационно-психологическая безопасность таможенных органов	10	***1***		1		8	УО, Д-Д
Тема 9	Методы, способы и средства защиты информации в современных автоматизированных информационных	6	***0***		0		6	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	ЛР	ПЗ	КСР		
	системах; методы, способы и приемы информационно–психологической защиты должностных лиц таможенных органов, методы, способы и приемы информационно – психологической защиты должностных лиц таможенных органов							
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. Понятие и предмет информационной безопасности.

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. Доктрина информационной безопасности РФ. Национальные интересы России в информационной сфере и угрозы информационной безопасности.

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. Угрозы информационной безопасности предприятия в условиях современной рыночной экономики

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. Нормативное правовое обеспечение 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.

Тема 5. Риски и эффективность обеспечения информационной безопасности

Этапы алгоритма анализа и оценки информационных рисков. Основные направления управления информационными рисками. Оценка эффективности мероприятий по обеспечению информационной безопасности. Система показателей и критериев оценки эффективности. Анализ возможностей использования различных методов математического моделирования при исследовании проблем обеспечения информационной безопасности.

Тема 6. Коммерческая, банковская, налоговая и профессиональная тайна в системе обеспечения информационной безопасности таможенных органов

Понятие коммерческой тайны и критерии охраноспособности прав на нее. Понятие банковской тайны и критерии охраноспособности прав на нее. Понятие профессиональной тайны и критерии охраноспособности прав на нее. Нормативно-правовые документы регламентирующие отношение к информации, содержащей коммерческую, банковскую, налоговую тайну в таможенных органах. Порядок получения таможенными органами информации, содержащей коммерческую, банковскую, налоговую тайну, необходимую для совершения таможенных операций и проведения таможенного контроля.

Тема 7. Организация обеспечения информационной безопасности таможенных органов. Ответственность за совершение нарушение правовых норм в области информационной безопасности

Роль и место системы обеспечения информационной безопасности в деятельности таможенных органов. Анализ результатов и затрат различных видов ресурсов на обеспечение информационной безопасности. Основные этапы процесса обеспечения информационной безопасности таможенных органов и их содержание. Понятие и виды юридической ответственности за нарушение правовых норм в области информационной безопасности. Уголовно-правовая ответственность за нарушение правовых норм в области информационной безопасности. Административная ответственность за нарушение правовых норм в сфере информационной безопасности. Особенности юридической ответственности за нарушение правовых норм в области информационной безопасности в гражданско-правовых и трудовых отношениях.

Тема 8. Информационно-техническая безопасность и информационно-психологическая безопасность таможенных органов

Демаскирующие признаки информационных объектов. Органы, принципы, методы, способы и средства добывания информации. Технические каналы утечки информации. Способы и средства предотвращения утечки информации. Угрозы и объекты обеспечения информационно-технической безопасности, принципы ее обеспечения. Технология

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

Тема 9. Методы, способы и средства защиты информации в современных автоматизированных информационных системах; методы, способы и приемы информационно–психологической защиты должностных лиц таможенных органов, методы, способы и приемы информационно –психологической защиты должностных лиц таможенных органов

Анализ способов нарушений информационной безопасности в современных автоматизированных информационных системах и их таксономия. Способы и средства. Средства программно-математического и программно-технического воздействия. Виды «вирусов» и защита от них. Использование защищенных компьютерных систем. Системы обнаружения и предотвращения атак. Методы и средства защиты данных, применяемые в сетях. Методы криптографии. Электронная подпись. Теоретические основы межличностной коммуникации, скрытного информационно-психологического управления. Методы и приемы информационно-психологического воздействия на должностных лиц: продуктивного общения, приемы ведения дискуссии, методы и приемы «мягкого» и «жесткого» информационно-психологического воздействия. Психологический анализ учебных видеофрагментов, демонстрирующих различные приемы информационно-психологического воздействия.

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:

Тестирование (Т): осуществляется с использованием опросника, содержащего варианты ответов;

Ситуационные задачи (СЗ): задачи решаются в письменном виде. По условиям ситуационной задачи требуется построить блок-схему, отражающую последовательность действий должностных лиц таможенных органов при реализации той или иной технологии таможенного контроля

Устный опрос (УО).

Доклад – Д-Д. Дополнительно поощряется иллюстрация тезисов доклада с использованием презентации.

Зачет (З): Устный опрос по билетам и решение ситуационной задачи.

4.1.1. 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. Понятие и предмет информационной безопасности	УО, Д-Д
Тема 2. Доктрина информационной безопасности РФ. Национальные интересы России в информационной сфере и угрозы информационной безопасности	УО, Д-Д, СЗ
Тема 3. Угрозы информационной безопасности предприятия в условиях современной рыночной экономики	УО, Д-Д, Т
Тема 4. Нормативное правовое обеспечение информационной безопасности таможенного органа	УО, Д-Д, Т
Тема 5. Риски и эффективность обеспечения информационной безопасности	УО, Д-Д, СЗ, Т

Тема 6. Коммерческая, банковская, налоговая и профессиональная тайна в системе обеспечения информационной безопасности таможенных органов	УО, Д-Д
Тема 7. Организация обеспечения информационной безопасности таможенных органов. Ответственность за совершение нарушение правовых норм в области информационной безопасности	УО, Д-Д
Тема 8. Информационно-техническая безопасность и информационно-психологическая безопасность таможенных органов	УО, Д-Д
Тема 9. Методы, способы и средства защиты информации в современных автоматизированных информационных системах; методы, способы и приемы информационно–психологической защиты должностных лиц таможенных органов, методы, способы и приемы информационно – психологической защиты должностных лиц таможенных органов	УО, Д-Д,

4.1.2. 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.

4.2. Материалы текущего контроля успеваемости обучающихся

Полный перечень типовых оценочных материалов находится на Кафедре таможенного администрирования.

Типовые оценочные материалы по теме 1 «Понятие и предмет информационной безопасности»:

Вопросы для проведения устного опроса:

1. Дайте определение понятию информация.
2. Каковы особенности информационного этапа развития современной цивилизации?
3. В чем суть информационной безопасности с позиций современного менеджмента?
4. Раскройте историю возникновения и основные положения «стратегии непрямых действий в бизнесе».
5. Дайте определение и раскройте содержание понятий «информационная безопасность» и «информационный ресурс».
6. Раскройте цели и задачи информационной безопасности.
7. Перечислите и раскройте содержание основных принципов обеспечения информационной безопасности.
8. Перечислите и раскройте составные части и направления обеспечения информационной безопасности.

Темы докладов:

1. Правовые основы информационного общества в России.
2. Программа «Информационное общество 2011-2024».
3. Конституционные гарантии реализации права на доступ к информации.

Типовые оценочные материалы по теме 2 «Доктрина информационной безопасности РФ. Национальные интересы России в информационной сфере и угрозы информационной безопасности»:

Вопросы для проведения устного опроса:

1. Раскройте наиболее важные положения Доктрины информационной безопасности в Российской Федерации.
2. Дайте краткую характеристику основных международных нормативных правовых документов в области информационной безопасности.

3. Перечислите и охарактеризуйте наиболее часто используемые отечественные и зарубежные стандарты информационной безопасности.
4. Раскройте содержание основных разрабатываемых в организации документов по вопросам информационной безопасности.

Темы докладов:
1. Доктрина информационной безопасности РФ об основных угрозах в информационной сфере и их источниках.
2. Классификация основных угроз информационной безопасности.
3. Разработка и принятие Концепции национальной безопасности и Доктрины информационной безопасности России.
4. Понятие источника угрозы национальной безопасности, информационной безопасности и их разновидности.
5. Информационные войны, понятие, основы теории информационных войн.
6. Информационный терроризм.
7. Информационное оружие.

Ситуационные задачи:
Определите с помощью каких информационных систем и ресурсов можно получить информацию о порядке предоставления государственных услуг таможенными органами, налоговыми органами, органами по сертификации
Определите и открытых данных различных государственных органов (таможенных, налоговых) с помощью информационных ресурсов.
Определите и покажите с помощью информационных ресурсов перечни сведений, используемых при заполнении деклараций на товары, транзитных деклараций.

Типовые оценочные материалы по теме 3 «Угрозы информационной безопасности предприятия в условиях современной рыночной экономики»:

Вопросы для устного опроса:
1. Основные угрозы информационной безопасности для таможенных органов и участников ВЭД.
2. Сопоставление характеристик состояния вопросов обеспечения информационной безопасности в экономической области в Российской Федерации и в наиболее развитых странах.
3. Основные методы прогнозирования и нейтрализации угроз информационной безопасности предприятия.

Темы докладов:
1. Интересы организации (предприятия, фирмы) в информационной сфере
2. (конкретная организация – по выбору студента).
3. Угрозы жизненно-важным интересам организации в информационной
4. сфере (конкретная организация – по выбору студента).
5. Система обеспечения информационной безопасности России.
6. Система информационной безопасности региона, ведомства, таможенного органа.

Примеры тестовых вопросов:
1. Искусственные угрозы безопасности информации вызваны:
    a. деятельностью человека;
    b. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

c. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
d. корыстными устремлениями злоумышленников;
e. ошибками при действиях персонала.

2. Естественные угрозы безопасности информации вызваны:
   a. деятельностью человека;
   b. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
   c. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
   d. корыстными устремлениями злоумышленников;
   e. ошибками при действиях персонала.
3. Защита информации это:
   a. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
   b. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
   c. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
   d. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
   e. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё

Типовые оценочные материалы по теме 4 «***Нормативное правовое обеспечение информационной безопасности таможенного органа***»:

Вопросы для устного опроса:

1. Какие подразделения таможенных органов контролируют соблюдение информационной безопасности?
2. Какие подразделения таможенных органов обязаны соблюдать требования по соблюдению информационной безопасности?
3. В отношении информации какого типа обеспечивается информационная безопасность.
4. Перечислите информационные ресурсы таможенных органов.

Темы докладов:

1. Открытые данные ФТС России.
2. Реализация ФТС России программы «Открытое ведомство».
3. Межведомственное электронное взаимодействие.
4. Личный кабинет участника ВЭД.

Примеры тестовых вопросов:

1. Какой категории лиц доступна информация Личного кабинета участника ВЭД.
   a. Любым лицам.
   b. Любому участнику ВЭД
   c. Участнику ВЭД, зарегистрированному в Личном кабинете
2. Какой категории лиц доступна информация, размещенная в разделе открытых данных ФТС России
   a. Любым лицам.
   b. Любому участнику ВЭД
   c. Участнику ВЭД, зарегистрированному в Личном кабинете

Типовые оценочные материалы по теме 5 «*Риски и эффективность обеспечения информационной безопасности*»:

Вопросы для устного опроса:

1. Перечислите основные этапы анализа и оценки информационных рисков, раскройте их содержание.

2. Раскройте методы снижения рисков в антикризисном менеджменте.

3. Дайте определение понятию "эффективность мероприятий по обеспечению информационной безопасности". Как оно соотносится с понятием риска?

Темы докладов:

1. Анализа информационных рисков и управление ими.
2. Информационный аудита на предприятии и в таможенных органах, сопоставление.
3. Характеристика нормативной правовой базы информационного аудита для российских и зарубежных компаний, государственных органов.
4. Основные виды информационного аудита.
5.

Примеры тестовых вопросов:

1. К методам нейтрализации возможных последствий выявленных рисков относятся:
   a. избегание, противодействие, передача, принятие;
   b. сокрытие, перекладывание на партнеров;
   c. страхование, аутсорсинг, резервирование;
   d. ни один из перечисленных вариантов
2. По какому критерию расставляются приоритеты информационных рисков?
   a. по вероятности реализации угроз;
   b. по величине возможного ущерба;
   c. по стоимости рисков;
   d. по времени реализации угроз;
   e. по срокам преодоления возможных последствий;
   f. по близости к профильной деятельности предприятия.

Ситуационные задачи:

1. Определите эффективность методов выявления информационных рисков на различных этапах совершения таможенных операций.
2. Определите эффективность методов выявления информационных рисков при обеспечении передачи, хранении и обработке информации получаемой ФТС России от участников ВЭД.
3. Определите эффективность методов выявления информационных рисков при обеспечении передачи, хранении и обработке информации на рабочих станциях
4. Определите эффективность методов выявления информационных рисков при обеспечении передачи, хранении и обработке информации таможенных органов.

Типовые оценочные материалы по теме 6 «*. Коммерческая, банковская, налоговая и профессиональная тайна в системе обеспечения информационной безопасности таможенных органов*»:

Вопросы для устного опроса:

1. Дайте определение коммерческой тайне. Назовите источники поступления в таможенные органы сведений, содержащих коммерческую тайну.
2. Дайте определение банковской тайне. Назовите источники поступления в таможенные органы сведений, содержащих банковскую тайну.

3. Дайте определение налоговой тайне. Назовите источники поступления в таможенные органы сведений, содержащих налоговую тайну.
4. Приведите примеры служебной информации таможенных органов.
5. В каких целях может использоваться информация полученная таможенными органами.

Темы докладов:

1. Коммерческая тайна. Понятие и правовое регулирование.
2. Банковская тайна. Понятие и правовое регулирование.
3. Профессиональная тайна. Понятие и правовое регулирование.
4. Служебная тайна. Понятие и правовое регулирование.
5. Основные нормативные правовые и руководящие документы, касающиеся вопросов соблюдения коммерческой тайны и их содержание.

Типовые оценочные материалы по теме 7 «Организация обеспечения информационной безопасности таможенных органов. Ответственность за совершение нарушение правовых норм в области информационной безопасности»:

Вопросы для устного опроса:

1. Перечислите средства обеспечения информационной безопасности, используемые таможенными органами.
2. Как организована ведомственная телефонная связь?
3. Как организовано управление ведомственной интегрированной сети телекоммуникаций?
4. Каковы задачи и состав центра управления ведомственной интегрированной сети телекоммуникаций?
5. Каковы перспективы использования в таможенных органах возможностей сети Internet?
6. Каковы перспективы дальнейшего развития межведомственной интегрированной автоматизированной информационной системы?
7. Перечислите Соглашения ФТС России и министерствами и ведомствами об организации информационного обмена
8. Требования нормативно-правовых документов для начала осуществления межведомственного информационного обмена.

Темы докладов:

1. Тяжесть уголовных преступлений за нарушение правовых норм в области информационной безопасности: сроки, примеры.
2. Виды административной ответственности за нарушения в сфере информационной безопасности, примеры.
3. Особенности юридической ответственности за нарушение правовых норм в области информационной безопасности в гражданско-правовых и трудовых отношениях.
4. Ответственность за нарушение порядка обращения с информацией, составляющей государственную тайну.

Типовые оценочные материалы по теме 8 «*Информационно-техническая безопасность и информационно-психологическая безопасность таможенных органов*»:

Вопросы для устного опроса:

1. Перечислите и дайте краткую характеристику основных способов и средств информационно-технической защиты таможенных органов.
2. Проведите сравнительный анализ средств программно-математического и программно-технического воздействия.
3. Перечислите основные виды вирусов.

Темы докладов:

1. Роль и место информационно-технической безопасности в работе таможенного органа.
2. Основные угрозы и объекты обеспечения информационно-технической безопасности таможенного органа.

Примеры тестовых вопросов:

1. Искусственные угрозы безопасности информации вызваны:
   a. деятельностью человека;
   b. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
   c. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
   d. корыстными устремлениями злоумышленников;
   e. ошибками при действиях персонала.
2. Естественные угрозы безопасности информации вызваны:
   a. деятельностью человека;
   b. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
   c. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
   d. корыстными устремлениями злоумышленников;
   e. ошибками при действиях персонала.
3. Защита информации это:
   a. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
   b. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
   c. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
   d. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
   e. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё

Типовые оценочные материалы по теме 9 «*Методы, способы и средства защиты информации в современных автоматизированных информационных системах; методы, способы и приемы информационно–психологической защиты должностных лиц таможенных органов, методы, способы и приемы информационно –психологической защиты должностных лиц таможенных органов*»:

Вопросы для устного опроса:

1. Раскройте основные методы криптографической защиты.
2. Перечислите основные методы и приемы информационно-психологического воздействия и раскройте их содержание.
3. Перечислите и дайте краткую характеристику основных способов и средств обеспечения информационно-психологической безопасности таможенных органов.
4. Раскройте содержание алгоритма информационно-психологической защиты личности.
5. Перечислите и дайте краткую характеристику техническим каналам уточки информации.

Темы докладов:

1. Характеристики основных способов и средств информационно-психологического воздействия на должностных лиц таможенных органов.
2. Основные способы и приемы информационно-психологической защиты выбранного должностного лица таможенного органа.
3. Сопоставительный анализ способов и приемов информационно-психологической защиты должностных лиц таможенных органов в различных условиях обстановки.
4. Раскройте основные принципы информационно-технической защиты. Определите с помощью каких программных задач реализована антивирусная защита на рабочих станциях.
5. С помощью каких программных задач осуществляется защита передачи данных, заверенных электронной подписью, реализуется ли данная защита при передаче данных с мобильных устройств.
6. Каким образом и с помощью каких программных задач реализована защита от несанкционированного доступа. Предложения по организации защиты данных

Результаты текущего контроля обучающихся используются в рамках балльной рейтинговой системы:

Недели	Виды учебных занятий (лекции/семинары)	Посещение учебных занятий	Письменные работы			Устные выступления		Компенсирующие задания (сверх расчетных 100 баллов)	Промежуточная аттестация (зачет)	Итого (максимально-расчетное количество баллов)
			Контрольные	Решение задач	Тестирование	Доклад (с презентацией / без презентации	Устный опрос			
Кол-во баллов за 1 вид мероприятия		0,5		3	2	1	2	3	25	36,5
1	л	0,5								0
2	л	0,5								0
3	с	0,5		3		1	2	6		12
4	с	0,5			2	1	2			5
5	л	0,5								0
6	л	0,5			2					2
7	с	0,5		3	2	1	2	6		14
8	с	0,5			2	1	2			5
9	с	0,5			2	1	2			5
	Текущий контроль 1*	**4,5**	**0**	**6**	**10**	**5**	**10**	**12**		**47,5**
10	с	0,5				1	2			3,5
11	с	0,5				1	2			3,5
12	л	0,5								0,5
13	л	0,5								0,5
14	л	0,5								0,5
15	л	0,5								0,5
16	с	0,5				1	2			3,5

17	с	0,5		3	2	1	2	6		14,5
	Текущий ** контроль 2	**4**	**0**	**3**	**2**	**4**	**8**	**6**	**25**	**52**
Всего за семестр (баллов)		**8,5**	**0**	**9**	**12**	**9**	**18**	**18**	**25**	**99,5**

4.3. Оценочные средства для промежуточной аттестации.

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

Вопросы для подготовки к зачету.
Вопросы практической направленности:

1. Задачи, решаемые таможенными органами в информационной сфере.
2. Угрозы интересам таможенных органов в информационной сфере.
3. Подразделения, обеспечивающие информационную безопасность таможенных органов.
4. Стандарты, применяемые для обеспечения межведомственного информационного взаимодействия.
5. Виды «нарушителей» режима защиты информации, модели их действий.
6. Основные нормативные правовые и руководящие документы, касающиеся вопросов соблюдения государственной тайны и их содержание.
7. Основные нормативные правовые и руководящие документы, касающиеся вопросов соблюдения коммерческой тайны и их содержание.
8. Содержание процессов лицензирования и сертификации.
9. Система информационной безопасности ФТС России: подразделения обеспечения информационной безопасности предприятия: состав, структура и функции.
10. Организация мероприятий по обеспечению информационной безопасности таможенных органов.
11. Создание и обеспечение защищенного электронного документооборота в

таможенных органах

12. Органы, методы, способы и средства добывания информации по техническим каналам.
13. Способы и средства защиты информации от утечки по техническим каналам в автоматизированных информационных системах.
14. Средства программно-математического и программно-технического воздействия и защита от них.
15. Понятие и содержание криптографии, основные методы, применяемые участниками ВЭД и таможенными органами.
16. Электронная подпись (понятие, содержание процесса использования электронной подписи, проблемы), использование электронной подписи участниками ВЭД и таможенными органами.
17. Методы и приемы информационно-психологического воздействия на должностных лиц.
18. Алгоритмы информационно-психологической защиты.
19. Использование интернет-технологий и обеспечение информационной безопасности.
20. Основные технологии построения защищенных информационных систем.
21. Формы контроля состояния технической защиты информации.
22. Государственные стандарты, регламентирующие терминологию в области защиты информации.
23. Средства защиты информации от утечки по техническим каналам.
24. Информационно-аналитические средства, используемые при разработке и принятии решения по информационной безопасности таможенных органов.

Вопросы теоретической направленности:

25. Понятие и предмет информационной безопасности
26. Соотношение понятий безопасность и информационная безопасность.
27. Уровни обеспечения безопасности: личностный, гражданское общество, государственный.
28. Общая структура правового института информационной безопасности. Объекты информационной безопасности: личность, общество, государство, - особенности каждого из объектов.
29. Основные теории понимания национальных интересов России в информационной сфере.
30. Классификация национальных интересов по срокам их реализации, соотношение интереса и информации.
31. Разработка и принятие Концепции национальной безопасности и Доктрины информационной безопасности России.
32. Понятие источника угрозы национальной безопасности, информационной безопасности и их разновидности.
33. Информационные войны, понятие, основы теории информационных войн.
34. Информационный терроризм.
35. Информационное оружие.
36. Принципы обеспечения информационной безопасности.
37. Основные задачи, функции и стандарты обеспечения информационной безопасности.
38. Конституционное закрепление и охрана информационных прав граждан.
39. Право на неприкосновенность частной жизни, личной и семейной тайны.
40. Персональные данные. Понятие, правовое регулирование.
41. Понятие и виды вредной информации.

42. Правовые средства противодействия деятельности общественных организаций, распространяющих вредную информацию, религиозных сект, политических партий, фондов.
43. Коммерческая тайна. Понятие и правовое регулирование.
44. Банковская тайна. Понятие и правовое регулирование.
45. Профессиональная тайна. Понятие и правовое регулирование.
46. Служебная тайна. Понятие и правовое регулирование.
47. Проблемы правового обеспечения информационной безопасности государства, противодействия информационным войнам и терроризму.
48. Понятие государственной тайны.
49. Доступ и допуск к государственной тайне, категории допуска.
50. Порядок засекречивания и рассекречивания информации, отнесенной к государственной тайне. Предварительное засекречивание.
51. Ответственность за нарушение порядка обращения с информацией, составляющей государственную тайну.
52. Основные виды деятельности по защите информации, подлежащие лицензированию.
53. Система государственного лицензирования деятельности в области защиты информации.
54. Органы государственной власти, полномочные в сфере лицензирования деятельности по защите информации и их правовой статус.
55. Общий порядок лицензирования в области защиты информации.
56. Система сертификации средств защиты информации.
57. Государственные стандарты в области защиты информации.
58. Общий порядок проведения сертификации средств защиты информации.
59. Аттестация объектов информатизации (информационных систем) по требованиям информационной безопасности.

Пример ситуационной задачи:
Сотрудник N-таможенного органа В. по случайности в обеденный перерыв, решив отобедать в кафе неподалеку, вынес с территории таможенного органа в портфеле папку с документами с грифом «Секретно». После обеда по рассеянности сотрудник В. оставил папку с документами на стуле, которая была найдена официантом К., сообщившим о находке в отделение полиции.
Предположите, какова будет ответственность работника В.? Предположите ситуацию, когда В. тоже может быть привлечен к ответственности?

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.

4.4.Методические материалы

Критерии оценки ответа на экзаменационные 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.

51-100 балов - зачет

0-50 балов - незачет

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.

5. Методические указания для обучающихся 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 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.

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

6.1. Основная литература.

1. Афонин, Петр Николаевич. Информационные таможенные технологии [Электронный ресурс] : учебник / П. Н. Афонин. - СПб.: Троицкий мост, 2014. - 350 с. http://idp.nwipa.ru:2228/reading.php?productid=344316
2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2018. — 325 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Режим доступа : www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847.
3. Информационная безопасность: Учебное пособие/Партыка Т. Л., Попов И. И., 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016. - 432 с.: 60х90 1/16. - (Профессиональное образование) (Переплёт) ISBN 978-5-91134-627-0, 200 экз. http://znanium.com/catalog/product/516806.
4. Малышенко Ю.В., Федоров В.В. Информационные таможенные технологии, Учебник. 2-ое издание, переработанное и доп., в 2ч., Ч1.-432 с, Российская таможенная академия, 2011 – 432с.
5. Малышенко Ю.В., Федоров В.В. Информационные таможенные технологии, Учебник. 2-ое издание, переработанное и доп., в 2ч., Ч2.-444 с, Российская таможенная академия, 2012 – 444с.

6.2.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 ограниченногодоступа 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-ogranichennogo-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-ogranichennym-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-ogranichennogo-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-kriticheskih-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

6.3. Учебно-методическое обеспечение самостоятельной работы.

Положение об организации самостоятельной работы студентов ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»;

Тестовые задания – на Кафедре таможенного администрирования;

Вопросы для самостоятельной работы студентов – на Кафедре таможенного администрирования.

1.4. 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».

6.5. Интернет-ресурсы.

Для освоения дисциплины следует пользоваться доступом через сайт научной библиотеки http://nwapa.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 «Znanium.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 «**Рубрикон»**;
- 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/

6.6. Иные источники.

В ходе образовательного процесса не используются.

7. 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