

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

«Забайкальский государственный университет»  
(ФГБОУ ВО «ЗабГУ»)

Юридический факультет

Кафедра Административного права и таможенного дела

УТВЕРЖДАЮ:

Декан факультета

Юридический факультет

Макаров Андрей  
Владимирович

«\_\_\_» \_\_\_\_\_ 20\_\_\_\_  
г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Б1.В.ДВ.06.02 Информационная безопасность в таможенном деле  
на 108 часа(ов), 3 зачетных(ые) единиц(ы)  
для направления подготовки (специальности) 38.05.02 - Таможенное дело

составлена в соответствии с ФГОС ВО, утвержденным приказом  
Министерства образования и науки Российской Федерации от  
«\_\_\_» \_\_\_\_\_ 20\_\_\_\_ г. №\_\_\_\_\_

Профиль – Таможенный контроль (для набора 2021)

Форма обучения: Очная

# 1. Организационно-методический раздел

## 1.1 Цели и задачи дисциплины (модуля)

Цель изучения дисциплины:

формирование знаний в области обеспечения информационной безопасности в условиях широкого применения информационных таможенных технологий, умений и навыков, необходимых для внутриорганизационного и межведомственного информационного взаимодействия с целью выявления информационных угроз и принятия мер по защите информационных ресурсов в профессиональной деятельности.

Задачи изучения дисциплины:

- изучение основ информационного обеспечения деятельности таможенных органов;
- изучение влияния сквозных цифровых технологий (искусственного интеллекта) на и информационную безопасность в таможенном деле
- освоение новых вызовов и угроз информационной и экономической безопасности в современной системе таможенных органов Российской Федерации;
- формирование практических навыков использования полученных знаний о методах защиты информации при использовании информационно-телекоммуникационных сетей международного информационного обмена в таможенных органах России.

## 1.2. Место дисциплины (модуля) в структуре ОП

Дисциплина «Информационная безопасность в таможенном деле» относится к дисциплинам по выбору (часть, формируемая участниками образовательных отношений) специальности 38.05.02 «Таможенное дело» и является базовой для дальнейшего успешного освоения следующих дисциплин: Система управления рисками при таможенном контроле, «Противодействие коррупции в Российской Федерации». В этом курсе, наравне с дисциплинами этого же цикла формируются общеправовые знания, умения и навыки для профессиональной деятельности. По очной форме обучения дисциплина изучается на 4 курсе в 7 семестре. По заочной форме обучения на 5 курсе в 10 семестре.

## 1.3. Объем дисциплины (модуля) с указанием трудоемкости всех видов учебной работы

Общая трудоемкость дисциплины (модуля) составляет 3 зачетных(ые) единиц(ы), 108 часов.

Виды занятий	Семестр 7	Всего часов
Общая трудоемкость		108
Аудиторные занятия, в т.ч.	51	51
Лекционные (ЛК)	17	17
Практические (семинарские) (ПЗ, СЗ)	34	34

Лабораторные (ЛР)	0	0
Самостоятельная работа студентов (СРС)	57	57
Форма промежуточной аттестации в семестре	Зачет	0
Курсовая работа (курсовой проект) (КР, КП)		

## 2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы		Планируемые результаты обучения по дисциплине
Код и наименование компетенции	Индикаторы достижения компетенции, формируемые в рамках дисциплины	Дескрипторы: знания, умения, навыки и (или) опыт деятельности
ОПК-5	ОПК-5.1. использует для решения коммуникативных задач современные технические средства и информационные технологии;	<p>Знать: основы применения технических средств и информационные технологии для решения коммуникативных задач</p> <p>Уметь: правильно использовать информационно-технические средства и технологии для решения поставленных задач</p> <p>Владеть: навыками самостоятельного применения современных технических средств, сквозных цифровых технологий, информационных технологий для решения коммуникативных задач</p>
ОПК-5	ОПК-5.2. анализирует коммуникативные процессы в организации и разрабатывает предложения по повышению их эффективности;	<p>Знать: особенности информационных процессов в таможенной сфере и основы повышения эффективности их работы</p> <p>Уметь: правильно выявить угрозы информационного взаимодействия в работе таможенных органов</p> <p>Владеть: навыками</p>

		самостоятельного формирования перспективных предложений по повышению эффективности применения информационно-коммуникационных технологий
ОПК-5	ОПК-5.3. обеспечивает взаимодействие органов власти с гражданами, коммерческими организациями, институтами гражданского общества, средствами массовой информации.	<p>Знать: организационные и технические основы информационного взаимодействия органов власти с различными субъектами информационных отношений</p> <p>Уметь: применять нормы информационного законодательства в целях обеспечения взаимодействия субъектов информационных правоотношений</p> <p>Владеть: навыками применения организационных и технических основ информационного взаимодействия органов власти с гражданами, коммерческими организациями, институтами гражданского общества, средствами массовой информации.</p>
ПК-1	ПК-1.1. применяет нормы таможенного законодательства ЕАЭС и законодательства Российской Федерации о таможенном деле в профессиональной деятельности;	<p>Знать: основы информационного законодательства стран-участниц Евразийского экономического союза</p> <p>Уметь: применять нормы информационного законодательства и оценивать последствия правовых норм в профессиональной деятельности</p> <p>Владеть: навыками применения нормативных актов в информационной сфере Евразийского экономического союза и Российской Федерации; обоснования применения правовых норм в конкретных профессиональных ситуациях</p>
ПК-1	ПК-1.2. контролирует соблюдение	Знать: нормы таможенного,

	таможенного, валютного, налогового и иного законодательства, при осуществлении участниками внешнеэкономической деятельности и иными лицами деятельности в сфере таможенного дела;	валютного, налогового законодательства, регулирующие содержание правовых действий и правила их реализации в сфере обеспечения информационной безопасности  Уметь: юридически правильно определять вызовы и угрозы информационной безопасности, обстоятельства ее обеспечения в том числе в деятельности участников внешнеэкономической деятельности и иных лиц в сфере таможенного дела;  Владеть: навыками соблюдения нормативных актов в таможенной, валютной, и налоговой сферах в целях обеспечения информационной безопасности
ПК-1	ПК-1.3. обеспечивает в пределах своей компетенции защиту прав интеллектуальной собственности;	Знать: основы обеспечения информационной защиты прав интеллектуальной собственности  Уметь: применять информационно-технические методы выявления контрафактного и фальсифицированного товара  Владеть: навыками информационно-технического контроля за процессуальными актами и документами, подтверждающих соблюдение запретов и ограничений внешнеторговой деятельности
ПК-1	ПК-1.4. контролирует соблюдение мер таможенно-тарифного регулирования, запретов и ограничений, мер защиты внутреннего рынка в отношении товаров, перемещаемых через таможенную границу Евразийского экономического союза, установленных в соответствии с законодательством Евразийского экономического	Знать: основные положения таможенно-тарифного и нетарифного регулирования  Уметь: применять нормы и методы информационной защиты внутреннего рынка в отношении товаров, перемещаемых через таможенную границу Евразийского экономического союза

	союза и Российской Федерации о государственном регулировании внешнеторговой деятельности;	Владеть: навыками самостоятельного контроля за соблюдением запретов и ограничений, установленных в соответствии с законодательством Евразийского экономического союза и Российской Федерации о государственном регулировании внешнеторговой деятельности
ПК-1	ПК-1.5. обеспечивает защиту гражданских прав участников внешнеэкономической деятельности и лиц, осуществляющих деятельность в сфере таможенного дела.	<p>Знать: 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</p> <p>Уметь: использовать основные положения законодательных и правоприменительных актов, регламентирующих обеспечение информационной безопасности гражданских прав участников внешнеэкономической деятельности, в деятельности таможенных органов</p> <p>Владеть: навыками применения соответствующих положений законодательных и правоприменительных актов, регламентирующих обеспечение информационной безопасности гражданских прав участников внешнеэкономической деятельности, к конкретным практическим ситуациям</p>
ПК-4	ПК-4.1. проводит комплексный анализ угроз экономической безопасности при осуществлении профессиональной деятельности;	<p>Знать: основы, общие положения, принципы обеспечения экономической безопасности в профессиональной деятельности</p> <p>Уметь: выявлять и проводить системный анализ вызовов и угроз экономической безопасности</p>

		<p>Владеть: навыками выявления новых вызовов и угроз обеспечения экономической безопасности; навыками комплексного анализа угроз экономической безопасности при реализации профессиональных задач</p>
ПК-4	<p>ПК-4.2. владеет навыками применения системы управления рисками при осуществлении профессиональной деятельности;</p>	<p>Знать: основы, общие положения, принципы применения системы управления рисками при реализации профессиональных задач</p> <p>Уметь: самостоятельно анализировать профиль риска с использованием современных информационно-коммуникационных технологий в профессиональной деятельности</p> <p>Владеть: навыками комплексного анализа системы управления рисками при осуществлении профессиональной деятельности</p>
ПК-4	<p>ПК-4.3. реализовывает мероприятия по получению юридически значимой информации, проверяет, анализирует, оценивает и использует в интересах выявления рисков и угроз экономической безопасности, предупреждения, пресечения, раскрытия и расследования преступления и иных правонарушений в сфере экономики;</p>	<p>Знать: организационно-правовые основы, мероприятия обеспечения экономической безопасности; юридически значимую информацию с целью выявления вызовов и угроз, пресечения противоправных деяний в экономической сфере</p> <p>Уметь: правильно получать юридически значимую таможенную информацию; самостоятельно оценивать риски и угрозы экономической безопасности в таможенном деле; оценивать факты и обстоятельства преступных посягательств и иных правонарушений в экономике</p> <p>Владеть: навыками анализа и проверки информации с целью определения и правовой оценки существующих угроз и рисков</p>

		обеспечения информационной, экономической безопасности; навыками получения и правильного применения полученной информации с целью раскрытия и расследования преступлений и правонарушений в экономической сфере
ПК-4	ПК-4.4. анализирует состояние и перспективы развития внешнеэкономических связей и их влияние на экономическую безопасность	<p>Знать: основы обеспечения экономической безопасности в системе таможенных органов; общее состояние развития внешнеэкономических связей</p> <p>Уметь: самостоятельно оценивать текущее состояние развития внешнеэкономических связей и их влияние на экономическую безопасность</p> <p>Владеть: навыками оценки и определения перспективных направлений развития внешнеэкономических связей в условиях новых вызовов и угроз обеспечения экономической безопасности</p>

### 3. Содержание дисциплины

#### 3.1. Разделы дисциплины и виды занятий

##### 3.1 Структура дисциплины для очной формы обучения

Модуль	Номер раздела	Наименование раздела	Темы раздела	Всего часов	Аудиторные занятия			СРС
					ЛК	ПЗ (СЗ)	ЛР	
1	1.1	Информация и информационная безопасность в современной системе	Информация, информационные процессы, информационные ресурсы, особенности обеспечения	18	3	6	0	9



		таможенных органов	информационной безопасности системе таможенных органов					
	1.2	Информационное обеспечение деятельности таможенных органов Евразийского экономического союза	Особенности и формы информационного обеспечения деятельности таможенных органов стран-членов Евразийского экономического союза	14	2	4	0	8
2	2.1	Организация системы защиты информации Федеральной таможенной службы Российской Федерации.	Программно-технические и организационно-правовые методы защиты таможенной информации	17	3	6	0	8
	2.2	Концепция информационной безопасности таможенных органов Российской Федерации	Концепция информационной безопасности таможенных органов Российской Федерации	14	2	4	0	8
3	3.1	Обеспечение информационной безопасности Единой автоматизированной информационной системы таможенных органов России.	Информационная безопасность ЕАИС ФТС России	14	2	4	0	8
4	4.1	Обеспечение информационной безопасности при использовании	Вопросы обеспечения информационной безопасности при использовании информационно-телекоммуникационных	14	2	4	0	8

		и информационно-телекоммуникационных сетей международного информационного обмена в таможенных органах России	сетей информационного обмена в таможенных органах России					
	4.2	Искусственный интеллект и информационная безопасность в таможенной сфере	Роль, значение, реальные и мнимые угрозы влияния сквозных цифровых технологий (технологий искусственного интеллекта) на информационную безопасность в таможенной сфере	17	3	6	0	8
Итого				108	17	34	0	57

### 3.2. Содержание разделов дисциплины

#### 3.2.1. Лекционные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Информация, информационные процессы, информационные ресурсы, особенности обеспечения и информационной безопасности системы таможенных органов	Информация в таможенном деле, ее свойства и виды. Информационные процессы и технологии в таможенном деле. Информационные системы в таможенном деле. Исторические аспекты использования информации и информационных технологий в таможенном деле Информационные ресурсы таможенных органов. понятие и структура информационной безопасности. Основы обеспечения информационной безопасности в таможенных органах. Объекты обеспечения информационной безопасности таможенных органов. Состояние обеспечения информационной безопасности	3

			таможенных органов. Информационная безопасность таможенных органов в системе национальной и экономической безопасности Российской Федерации	
	1.2	Особенности и формы информационного обеспечения деятельности таможенных органов стран-членов Евразийского экономического союза	Информационное обеспечение деятельности таможенных органов стран-участниц Евразийского экономического союза. Правовое регулирование основ информационной безопасности Казахстана. Правовое регулирование основ информационной безопасности Белоруссии. Правовое регулирование основ информационной безопасности Киргизии и Армении. Зарубежный опыт правового обеспечения информационной безопасности. Продвижение инициатив евразийского союза в области обеспечения международной информационной безопасности. Формы обеспечения информационной безопасности. Идентификация. Аутентификация. Установление подлинности пользователя единых автоматизированных информационных систем.	2
2	2.1	Программно-технические и организационно-правовые методы защиты таможенной информации	Защита информации: понятие, принципы, система, Актуальные проблемы правового и организационного обеспечения информационной безопасности ФТС России. Основные факторы, влияющие на обеспечение информационной безопасности таможенных органов Российской Федерации. Характер и формы угроз. Потенциальный (вероятный) нарушитель информационной безопасности таможенных органов Российской Федерации. Методы криптографической защиты таможенной информации Симметричное шифрование. Методы асимметричного шифрования. Электронная цифровая подпись:	3

			алгоритмы, открытый и секретный ключи, сертификаты. Открытый и закрытый ключи в электронной цифровой подписи. Программные средства и технологии формирования электронной цифровой подписи, используемые в таможенных органах. Ответственность за преступления и правонарушения в сфере защиты информации в системе таможенных органов.	
	2.2	Концепция информационной безопасности таможенных органов Российской Федерации	Концепция информационной безопасности таможенных органов Российской: реализация, стратегические цели, направления развития. Концепция информационно-технической политики ФТС РФ. Информационная политика ФТС России в области обеспечения информационной безопасности таможенных органов.	2
3	3.1	Информационная безопасность ЕАИС ФТС России	Общая характеристика форм обеспечения информационной безопасности ЕАИС ФТС России. Единая автоматизированная информационная система ФТС России как совокупность мер, обеспечивающих автоматизацию деятельности таможенных органов. Задачи автоматизации процессов управления таможенной службой России. Этапы разработки ЕАИС ФТС России. Характеристика информационных процессов и информационных потоков в системе таможенных органов. Принципы построения ЕАИС. Порядок организации и процессов жизненного цикла программных средств информационных систем и информационных технологий таможенных органов. Формирование заказа на создание программных средств. Территориальное распределение системы управления ЕАИС. Задачи Совета по обеспечению информационной безопасности таможенных органов	2

			Российской Федерации.	
4	4.1	Вопросы обеспечения и информационной безопасности при использовании информационно-телекоммуникационных сетей информационного обмена в таможенных органах России	Типовые требования по безопасности информации программных средств информационных систем и информационных технологий в таможенных органах. Особенности обеспечения информационной безопасности при использовании информационно-телекоммуникационных сетей информационного обмена в таможенных органах России: условия и порядок. Угрозы и методы обеспечения безопасности.	2
	4.2	Роль, значение, реальные и мнимые угрозы влияния сквозных цифровых технологий (технологий искусственного интеллекта) на информационную безопасность в таможенной сфере	Применение искусственного интеллекта в обеспечении безопасности данных. Использование высоких цифровых технологий для предотвращения несанкционированного доступа к информации. Искусственный интеллект: концепции и подходы к пониманию. Оценка влияния на состояние защищенности личности, общества, государства. Стратегия развития таможенной службы до 2030 года. Практика использования искусственного интеллекта в таможенной сфере иностранных государств. Подходы правового регулирования применения искусственного интеллекта в работе таможенных органов отдельных стран Европы и Китая. Перспективные направления внедрения технологий искусственного интеллекта в таможенную службу России.	3

### 3.2.2. Практические занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Информация,	Информация в таможенном деле, ее	6

		информационные процессы, информационные ресурсы, особенности обеспечения и информационной безопасности таможенных органов	свойства и виды. Информационные процессы и технологии в таможенном деле. Информационные системы в таможенном деле. Исторические аспекты использования информации и информационных технологий в таможенном деле Информационные ресурсы таможенных органов. понятие и структура информационной безопасности. Основы обеспечения информационной безопасности в таможенных органах. Объекты обеспечения информационной безопасности таможенных органов. Состояние обеспечения информационной безопасности таможенных органов. Информационная безопасность таможенных органов в системе национальной и экономической безопасности Российской Федерации	
	1.2	Особенности и формы информационного обеспечения деятельности таможенных органов стран-членов Евразийского экономического союза	Информационное обеспечение деятельности таможенных органов стран-участниц Евразийского экономического союза. Правовое регулирование основ информационной безопасности Казахстана. Правовое регулирование основ информационной безопасности Белоруссии. Правовое регулирование основ информационной безопасности Киргизии и Армении. Зарубежный опыт правового обеспечения информационной безопасности. Продвижение инициатив евразийского союза в области обеспечения международной информационной безопасности. Формы обеспечения информационной безопасности. Идентификация. Аутентификация. Установление подлинности пользователя единых автоматизированных информационных систем.	4
2	2.1	Программно-технические и	Защита информации: понятие, принципы, система, Актуальные	6

		<p>организационно-правовые методы защиты таможенной информации</p>	<p>проблемы правового и организационного обеспечения информационной безопасности ФТС России. Основные факторы, влияющие на обеспечение информационной безопасности таможенных органов Российской Федерации. Характер и формы угроз. Потенциальный (вероятный) нарушитель информационной безопасности таможенных органов Российской Федерации. Методы криптографической защиты таможенной информации Симметричное шифрование. Методы асимметричного шифрования. Электронная цифровая подпись: алгоритмы, открытый и секретный ключи, сертификаты. Открытый и закрытый ключи в электронной цифровой подписи. Программные средства и технологии формирования электронной цифровой подписи, используемые в таможенных органах. Ответственность за преступления и правонарушения в сфере защиты информации в системе таможенных органов.</p>	
	2.2	<p>Концепция информационной безопасности таможенных органов Российской Федерации</p>	<p>Концепция информационной безопасности таможенных органов Российской: реализация, стратегические цели, направления развития. Концепция информационно-технической политики ФТС РФ. Информационная политика ФТС России в области обеспечения информационной безопасности таможенных органов.</p>	4
3	3.1	<p>Информационная безопасность ЕАИС ФТС России</p>	<p>Общая характеристика форм обеспечения информационной безопасности ЕАИС ФТС России. Единая автоматизированная информационная система ФТС России как совокупность мер, обеспечивающих автоматизацию деятельности таможенных органов. Задачи автоматизации процессов управления таможенной службой</p>	4

			<p>России. Этапы разработки ЕАИС ФТС России. Характеристика информационных процессов и информационных потоков в системе таможенных органов. Принципы построения ЕАИС. Порядок организации и процессов жизненного цикла программных средств информационных систем и информационных технологий таможенных органов. Формирование заказа на создание программных средств. Территориальное распределение системы управления ЕАИС. Задачи Совета по обеспечению информационной безопасности таможенных органов Российской Федерации.</p>	
4	4.1	<p>Вопросы обеспечения информационной безопасности при использовании информационно-телекоммуникационных сетей информационного обмена в таможенных органах России</p>	<p>Типовые требования по безопасности информации программных средств информационных систем и информационных технологий в таможенных органах. Особенности обеспечения информационной безопасности при использовании информационно-телекоммуникационных сетей информационного обмена в таможенных органах России: условия и порядок. Угрозы и методы обеспечения безопасности.</p>	4
	4.2	<p>Роль, значение, реальные и мнимые угрозы влияния сквозных цифровых технологий (технологий искусственного интеллекта) на информационную</p>	<p>Применение искусственного интеллекта в обеспечении безопасности данных. Использование высоких цифровых технологии для предотвращения несанкционированного доступа к информации. Искусственный интеллект: концепции и подходы к пониманию. Оценка влияния на состояние защищенности личности, общества, государства. Стратегия развития таможенной службы до 2030 года. Практика использования искусственного интеллекта в</p>	6



		<p>безопасность в таможенной сфере. Роль, значение, реальные и мнимые угрозы влияния сквозных цифровых технологий (технологий искусственного интеллекта) на информационную безопасность в таможенной сфере</p>	<p>таможенной сфере иностранных государств. Подходы правового регулирования применения искусственного интеллекта в работе таможенных органов отдельных стран Европы и Китая. Перспективные направления внедрения технологий искусственного интеллекта в таможенную службу России.</p>	
--	--	--	---	--

### 3.2.3. Лабораторные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)

### 3.3. Содержание материалов, выносимых на самостоятельное изучение

Модуль	Номер раздела	Содержание материалов, выносимого на самостоятельное изучение	Виды самостоятельной деятельности	Трудоемкость (в часах)
1	1.1	<p>Информация в таможенном деле, ее свойства и виды. Информационные процессы и технологии в таможенном деле. Информационные системы в таможенном деле. Исторические аспекты использования информации и информационных технологий в таможенном деле</p>	<p>Анализ литературы Подготовка докладов</p>	9

		<p>Информационные ресурсы таможенных органов. понятие и структура информационной безопасности. Основы обеспечения информационной безопасности в таможенных органах. Объекты обеспечения информационной безопасности таможенных органов. Состояние обеспечения информационной безопасности таможенных органов. Информационная безопасность таможенных органов в системе национальной и экономической безопасности Российской Федерации</p>		
	1.2	<p>Информационное обеспечение деятельности таможенных органов стран-участниц Евразийского экономического союза. Правовое регулирование основ информационной безопасности Казахстана. Правовое регулирование основ информационной безопасности Белоруссии. Правовое регулирование основ информационной безопасности Киргизии и Армении. Зарубежный опыт правового обеспечения информационной безопасности. Продвижение инициатив</p>	<p>Анализ литературы Подготовка докладов</p>	8

		евразийского союза в области обеспечения международной информационной безопасности. Формы обеспечения информационной безопасности. Идентификация. Аутентификация. Установление подлинности пользователя единых автоматизированных информационных систем.		
2	2.1	Защита информации: понятие, принципы, система, Актуальные проблемы правового и организационного обеспечения информационной безопасности ФТС России. Основные факторы, влияющие на обеспечение информационной безопасности таможенных органов Российской Федерации. Характер и формы угроз. Потенциальный (вероятный) нарушитель информационной безопасности таможенных органов Российской Федерации. Методы криптографической защиты таможенной информации Симметричное шифрование. Методы асимметричного шифрования. Электронная цифровая подпись: алгоритмы, открытый и секретный	Анализ литературы Подготовка докладов	8

		<p>ключи, сертификаты. Открытый и закрытый ключи в электронной цифровой подписи. Программные средства и технологии формирования электронной цифровой подписи, используемые в таможенных органах. Ответственность за преступления и правонарушения в сфере защиты информации в системе таможенных органов.</p>		
	2.2	<p>Концепция информационной безопасности таможенных органов Российской: реализация, стратегические цели, направления развития. Концепция информацио но-технической политики ФТС РФ. Информационная политика ФТС России в области обеспечения информационной безопасности таможенных органов.</p>	<p>Анализ литературы Подготовка докладов</p>	8
3	3.1	<p>Общая характеристика форм обеспечения информационной безопасности ЕАИС ФТС России. Единая автоматизированная информационная система ФТС России как совокупность мер, обеспечивающих автоматизацию деятельности таможенных органов. Задачи автоматизации процессов управления таможенной службой</p>	<p>Анализ литературы Подготовка докладов</p>	8

		<p>России. Этапы разработки ЕАИС ФТС России. Характеристика информационных процессов и информационных потоков в системе таможенных органов. Принципы построения ЕАИС. Порядок организации и процессов жизненного цикла программных средств информационных систем и информационных технологий таможенных органов. Формирование заказа на создание программных средств. Территориальное распределение системы управления ЕАИС. Задачи Совета по обеспечению информационной безопасности таможенных органов Российской Федерации.</p>		
4	4.1	<p>Типовые требования по безопасности информации программных средств информационных систем и информационных технологий в таможенных органах. Особенности обеспечения информационной безопасности при использовании информационно-телекоммуникационных сетей информационного обмена в таможенных органах России: условия и порядок. Угрозы и методы обеспечения</p>	<p>Анализ литературы Подготовка докладов</p>	8

		безопасности.		
	4.2	<p>Применение искусственного интеллекта в обеспечении безопасности данных. Использование высоких цифровых технологии для предотвращения несанкционированного доступа к информации. Искусственный интеллект: концепции и подходы к пониманию. Оценка влияния на состояние защищенности личности, общества, государства. Стратегия развития таможенной службы до 2030 года. Практика использования искусственного интеллекта в таможенной сфере иностранных государств. Подходы правового регулирования применения искусственного интеллекта в работе таможенных органов отдельных стран Европы и Китая. Перспективные направления внедрения технологий искусственного интеллекта в таможенную службу России.</p>	<p>Анализ литературы Подготовка докладов</p>	8

#### **4. Фонд оценочных средств для проведения текущей и промежуточной аттестации обучающихся по дисциплине**

Фонд оценочных средств текущего контроля и промежуточной аттестации по итогам освоения дисциплины представлен в приложении.

[Фонд оценочных средств](#)

#### **5. Учебно-методическое и информационное обеспечение дисциплины**

## 5.1. Основная литература

### 5.1.1. Печатные издания

1.

### 5.1.2. Издания из ЭБС

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. – Москва : Издательство Юрайт, 2021. – 253 с. – (Высшее образование). – ISBN 978-5-534-13960-0. – Режим доступа: <https://urait.ru/viewer/informacionnaya-bezopasnost-467370>.

2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. – 2-е изд., испр. и доп. – Москва : Издательство Юрайт, 2021. – 243 с. – (Высшее образование). – ISBN 978-5-534-12774-4. – Режим доступа: <https://urait.ru/viewer/informacionnaya-bezopasnost-cheloveka-476294>.

3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. – Москва : Издательство Юрайт, 2021. – 325 с. – (Высшее образование). – ISBN 978-5-534-03600-8. – Режим доступа: <https://urait.ru/viewer/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-469235>.

## 5.2. Дополнительная литература

### 5.2.1. Печатные издания

1.

### 5.2.2. Издания из ЭБС

1. Джабиев, А. П. Основы таможенного дела : учебник для вузов / под общей редакцией А. П. Джабиева. – 2-е изд. – Москва : Издательство Юрайт, 2020. – 489 с. – (Высшее образование). – ISBN 978-5-534-13241-0. – Режим доступа: <https://urait.ru/viewer/osnovy-tamozhennogo-dela-449589>.

2. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. – Москва : Издательство Юрайт, 2021. – 111 с. – (Высшее образование). – ISBN 978-5-534-12769-0. – Режим доступа: <https://urait.ru/viewer/prestupleniya-v-sfere-informacionnoy-bezopasnosti-476798>.

3. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. – Москва : Издательство Юрайт, 2021. – 342 с. – (Высшее образование). – ISBN 978-5-534-05142-1. – Режим доступа: <https://urait.ru/viewer/nadezhnost-i-bezopasnost-programmnogo-obespecheniya-473348>.

## 5.3. Базы данных, информационно-справочные и поисковые системы

Название	Ссылка
ЭБС «Лань»	<a href="http://www.e.lanbook.ru/">http://www.e.lanbook.ru/</a>

ЭБС «Юрайт»	<a href="https://www.biblio-online.ru/">https://www.biblio-online.ru/</a>
ЭБС «Консультант студента»	<a href="https://www.studentlibrary.ru/">https://www.studentlibrary.ru/</a>
«Электронно-библиотечная система»	<a href="https://elibrary.ru/">https://elibrary.ru/</a>
Российская национальная библиотека	<a href="http://www.nlr.ru/">http://www.nlr.ru/</a>
Информационно-просветительский портал «Электронные журналы»	<a href="http://www.eduhmao.ru/info">http://www.eduhmao.ru/info</a>
«Электронная библиотека диссертаций»	<a href="http://www.diss.rsl.ru/">http://www.diss.rsl.ru/</a>

## **6. Перечень программного обеспечения**

Программное обеспечение общего назначения: ОС Microsoft Windows, Microsoft Office, ABBYY FineReader, ESET NOD32 Smart Security Business Edition, Foxit Reader, АИБС "МегаПро".

Программное обеспечение специального назначения:

- 1) Система ГАРАНТ
- 2) СПС "Консультант Плюс"

## **7. Материально-техническое обеспечение дисциплины**

Наименование помещений для проведения учебных занятий и для самостоятельной работы обучающихся	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебные аудитории для проведения занятий лекционного типа	Состав оборудования и технических средств обучения указан в паспорте аудитории, закреплённой расписанием по факультету
Учебные аудитории для проведения практических занятий	
Учебные аудитории для промежуточной аттестации	
Учебные аудитории для проведения групповых и индивидуальных консультаций	Состав оборудования и технических средств обучения указан в паспорте аудитории, закреплённой расписанием по кафедре
Учебные аудитории для текущей аттестации	

## **8. Методические рекомендации по организации изучения дисциплины**

1. Общие методические рекомендации по изучению дисциплины

Для эффективного освоения материала дисциплины необходимым является выполнение следующих требований:

- обязательное посещение всех лекционных и практических занятий, способствующее



системному овладению материалом курса;

- все вопросы соответствующих разделов и тем по дисциплине необходимо фиксировать (на любых носителях информации);
- обязательное выполнение домашних заданий является важнейшим требованием и условием формирования целостного и системного знания по дисциплине;
- обязательность личной активности каждого студента на всех занятиях по дисциплине;
- в случаях неясности каких-либо вопросов, обсуждаемых на занятиях, необходимо задать соответствующие вопросы преподавателю, а не оставлять их непонятыми;
- в случаях пропусков занятий по уважительным причинам студентам предоставляется право подготовки и представления заданий и ответов на вопросы изученного материала, с расчетом на помощь преподавателя в его усвоении;
- в случаях пропусков без уважительной причины студент обязан самостоятельно изучить соответствующий материал;
- необходимым условием является самостоятельность и инициативность студентов при контроле набора баллов по дисциплине для успешного прохождения промежуточной аттестации.

## 2. Формы контроля

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

## 3. Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

## 4. Лекции

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана. На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс. Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

## 5. Семинарские (практические) занятия

Семинарские (практические занятия) представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на практических занятиях оценивается по следующим критериям:

- ответы на вопросы, предлагаемые преподавателем;
- участие в дискуссиях;
- выполнение проектных и иных заданий;
- ассистирование преподавателю в проведении занятий.

Доклады и оппонирование докладов проверяют степень владения теоретическим

материалом, а также корректность и строгость рассуждений.

Оценивание практических заданий входит в накопленную оценку.

#### 6. Самостоятельная работа студента

Для успешного усвоения курса необходимо не только посещать аудиторные занятия, но и вести активную самостоятельную работу.

При самостоятельной проработке курса обучающиеся должны:

- просматривать основные определения и факты;
- повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;
- изучить рекомендованную основную и дополнительную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;
- самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;
- использовать для самопроверки материалы фонда оценочных средств;
- выполнять домашние задания по указанию преподавателя.

Домашнее задание оценивается по следующим критериям:

- Степень и уровень выполнения задания;
- Аккуратность в оформлении работы;
- Использование специальной литературы;
- Сдача домашнего задания в срок.

Оценивание домашних заданий входит в накопленную оценку.

Разработчик/группа разработчиков:

**Типовая программа утверждена**

Согласована с выпускающей кафедрой  
Заведующий кафедрой

\_\_\_\_\_ «\_\_\_» \_\_\_\_\_ 20\_\_ г.