

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»
КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
В РОССИЙСКОЙ ФЕДЕРАЦИИ**

Специальность 38.05.02 Таможенное дело

Направленность (профиль): «Таможенное дело»

Формы обучения: очная; заочная

Квалификация выпускника: специалист таможенного дела

Срок получения образования: очная форма обучения 5 лет, заочная форма обучения 5 лет 6 месяцев

Объем дисциплины:

в зачетных единицах: 7 з.е.

в академических часах: 252 ак.ч.

Рабочая программа по дисциплине «Информационная безопасность в Российской Федерации» по специальности 38.05.02 Таможенное дело направленность (профиль) «Таможенное дело», составлена Качаловым В.Ю. в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по специальности 38.05.02 Таможенное дело, утвержденного приказом Министерства образования и науки Российской Федерации от «25» ноября 2020 г. №1453, Профессионального стандарта 08.039 «Специалист по внешнеэкономической деятельности», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 17 июня 2019 г. № 409н.

Рабочая программа:

обсуждена и рекомендована к утверждению решением Научно-методического совета «7» апреля 2021 г., протокол № 3.

утверждена Ученым советом Российского университета кооперации «26» августа 2021 г. № 1

СОДЕРЖАНИЕ

1. Цели и задачи освоения дисциплины.....	4
2. Место дисциплины в структуре образовательной программы	4
3. Перечень планируемых результатов обучения по дисциплине	5
4. Объем дисциплины и виды учебной работы.....	6
5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий.....	7
5.1. Содержание дисциплины	7
5.2. Разделы, темы дисциплины и виды занятий	11
6. Лабораторные занятия	13
7. Практические занятия.....	13
8. Тематика курсовых работ (проектов).....	18
9. Самостоятельная работа студента	18
10. Перечень нормативных правовых актов, основной и дополнительной учебной литературы, необходимых для освоения дисциплины	21
11. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения, профессиональных баз данных и информационных справочных систем	23
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	24

1. Цели и задачи освоения дисциплины

Целью освоения дисциплины «Информационная безопасность в Российской Федерации» ознакомление студентов с основными понятиями и определениями информационной безопасности; источниками, рисками и формами атак на информацию; угрозами, которым подвергается информация; вредоносными программами; защитой от компьютерных вирусов и других вредоносных программ; методами и средствами защиты информации; политикой безопасности компании в области информационной безопасности; стандартами информационной безопасности; криптографическими методами и алгоритмами шифрования информации; алгоритмами аутентификации пользователей; защитой информации в сетях; требованиям к системам защиты информации

Задачи:

- формирование знаний о содержании информационной безопасности в системе специальных дисциплин, его принципах и назначениях;
- подготовка и представление понятий и категорий современных технологий информационной безопасности и автоматизированных технологий обработки информационной безопасности;
- приобрести знания по основам проектирования и практического применения современных информационных технологий с использованием современных технических и программных средств.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность в Российской Федерации» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы специалитета по специальности 38.05.02 Таможенное дело направленность (профиль) «Таможенное дело».

Дисциплина обеспечивает формирование следующих компетенций:

Код и наименование компетенции	Дисциплины, модули, практики, обеспечивающие формирование компетенции	Периоды формирования компетенции в процессе освоения ОПОП					Место в формировании компетенции
		1 курс (сем.)	2 курс (сем.)	3 курс (сем.)	4 курс (сем.)	5 курс (сем.)	
ПК-2	Основы применения технических средств таможенного контроля				7 сем		Изучаемая
ПК-2	Производственная практика, практика по получению профессиональных умений и опыта профессиональной				8 сем		Последующая

Код и наименование компетенции	Дисциплины, модули, практики, обеспечивающие формирование компетенции	Периоды формирования компетенции в процессе освоения ОПОП					Место в формировании компетенции
		1 курс (сем.)	2 курс (сем.)	3 курс (сем.)	4 курс (сем.)	5 курс (сем.)	
	деятельности						
ПК-2	Производственная практика, практика по получению профессиональных умений и опыта организационно-управленческой деятельности				8 сем		Последующая
ПК-2	Производственная практика, преддипломная практика					10 сем	Последующая

3. Перечень планируемых результатов обучения по дисциплине

Изучение дисциплины направлено на формирование у обучающихся следующих компетенций:

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
ПК-2 Способность применять технические средства таможенного контроля и эксплуатации оборудования и приборов	ПК-2.1 Способен применять методы и средства получения, хранения, обработки информации, использовать навыки использования компьютерной техники, программно-информационных систем, компьютерных сетей	Знать методы и средства получения, хранения, обработки информации Уметь определять необходимые для использования методы и средства получения, хранения, обработки информации, использовать навыки использования компьютерной техники, программно-информационных систем, компьютерных сетей Владеть навыками получения, хранения, обработки информации, использования компьютерной техники, программно-информационных систем, компьютерных сетей
	ПК-2.2 Способен работать с программными средствами по исчислению и учету таможенных платежей, работать с электронными базами данных	Знать систему работы с программными средствами по исчислению и учету таможенных платежей, электронных баз данных Уметь работать с программными средствами по исчислению и учету таможенных платежей, работать с электронными базами данных Владеть навыками работы с программными средствами по исчислению и учету таможенных платежей, работы с электронными базами данных
	ПК-2.3 Способен	Знать методы сбора и анализа данных

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
	применять методы сбора и анализа данных таможенной статистики внешней торговли и специальной таможенной статистики	таможенной статистики внешней торговли и специальной таможенной статистики Уметь применять методы сбора и анализа данных таможенной статистики внешней торговли и специальной таможенной статистики Владеть навыками применения методов сбора и анализа данных таможенной статистики внешней торговли и специальной таможенной статистики

4. Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы в академических часах с выделением объема контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся

очная форма обучения

Вид учебной деятельности	ак. часов	
	Всего	По семестрам 7 семестр
1. Контактная работа обучающихся с преподавателем:	86,5	86,5
Аудиторные занятия, часов всего, в том числе:	86	86
• занятия лекционного типа	34	34
• занятия семинарского типа:	52	52
практические занятия	52	52
лабораторные занятия		
в том числе занятия в интерактивных формах	4	4
в том числе занятия в форме практической подготовки	20	20
Контактные часы на аттестацию в период экзаменационных сессий	0,5	0,5
в том числе курсовая работа (проект)		
2. Самостоятельная работа студентов, всего	129,5	129,5
- курсовая работа (проект)		
- выполнение домашних заданий	129,5	129,5
- контрольное тестирование		
3. Промежуточная аттестация: <i>Экзамен</i>	36	36
ИТОГО:		
Общая трудоемкость	ак. часов	252
	зач. ед.	7

заочная форма обучения

Вид учебной деятельности	ак. часов	
	Всего	По курсам 4 курс
1. Контактная работа обучающихся с преподавателем:	18,5	18,5
Аудиторные занятия, часов всего, в том числе:	18	18
• занятия лекционного типа	8	8
• занятия семинарского типа:	10	10
практические занятия	10	10
лабораторные занятия		
в том числе занятия в интерактивных формах	2	2
в том числе занятия в форме практической подготовки	2	2
Контактные часы на аттестацию в период экзаменационных сессий	0,5	0,5
в том числе курсовая работа (проект)		
2. Самостоятельная работа студентов, всего	224,5	224,5
- курсовая работа (проект)		
- выполнение домашних заданий	224,5	224,5
- контрольное тестирование		
3. Промежуточная аттестация: <i>Экзамен</i>	9	9
ИТОГО:		
	ак. часов	252
Общая трудоемкость	зач. ед.	7

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Основные понятия и положения информационной безопасности

Информация, сообщения, информационные процессы как объекты информационной безопасности. Цели и задачи защиты информации. Классификационная схема понятий в области защиты информации. Концептуальные основы защиты информации. Основные положения государственной политики обеспечения информационной безопасности РФ

Тема 2. Угрозы безопасности информации в информационных системах

Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Методы оценки уязвимости информации. Виды утечки информации. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Структура теории компьютерной безопасности. Основные уровни защиты информации. Защита машинных носителей информации (МНИ). Защита средств взаимодействия с МНИ. Защита представления информации. Защита содержания информации. Основные виды атак на информационные АС. Классификация основных атак и вредоносных программ.

Тема 3. Методы и средства защиты информации

Классификация методов и средств защиты информации. Правовые методы обеспечения информационной безопасности. Организационно-технические методы обеспечения информационной безопасности. Экономические методы обеспечения информационной безопасности.

Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей. Основные критерии защищенности информационных автоматизированных систем (АС). Классы защищенности АС. Критерии и классы защищенности средств вычислительной техники (СВТ), и АС.

Стандарты по оценке защищенности АС. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Основные требования к системам защиты в TCSEC. Классы защиты TCSEC. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.

Тема 4. Криптографические методы защиты информации

Классификация методов криптографического преобразования информации: шифрование, стеганофракия, кодирование, сжатие. Требования к методам шифрования и их классификация. Криптостойкость шифра как основной показатель его эффективности.

Методы шифрования с симметричным ключом: методы замены, методы перестановки, аналитические методы, аддитивные методы, комбинированные методы. Системы шифрования с открытым ключом. Стандарты шифрования. Перспективы использования криптозащиты информации.

Тема 5. Аппаратные и программные средства защиты компьютерной информации

Основные понятия программно-технического уровня информационной безопасности. Архитектурная безопасность. Современные способы и средства негласного получения информации по различным каналам. Пассивные и активные способы обеспечения информационной безопасности. Современные средства выявления каналов утечки информации

Тема 6. Безопасность компьютерных сетей

Основные аспекты безопасности компьютерных сетей (КС). Атакуемые сетевые компоненты на разных уровнях модели OSI, уязвимости сетевых служб (DNS, Telnet), средств передачи информации. Классификация сетевых атак. Межсетевые экраны. Типы и функции межсетевых экранов: пакетных фильтров, прокси-систем, устройств контроля текущего состояния.

Организация виртуальных корпоративных сетей. Протокол IPSec. Защита данных в WWW.

Классификация компьютерных вирусов. Меры по их профилактике. Методология защиты автоматизированных информационных систем. Антивирусные программы.

Тема 7. Роль информационных технологий в таможенном деле. Информационные системы и технологии

1. Информационные таможенные технологии: история развития; роль и место в управлении таможенными процессами.
2. Характеристика информационных процессов и информационных потоков в системе таможенных органов.
3. Стандарты пользовательского интерфейса для информационных таможенных технологий. Операционные системы. Файловые системы.
4. Системы классификации и кодирования.

Тема 8. Информационно-техническая политика ФТС России

1. Концепция информационно-технической политики ФТС России. Системы электронного декларирования, документального контроля, оценки таможенных рисков.
2. Критерии оценки результатов внедрения информационных таможенных технологий.

Тема 9. Сетевые технологии и информационная безопасность в таможенной деятельности

1. Понятие информационного пространства. Тенденции развития телекоммуникационных технологий.
2. Структура компьютерных сетей. Классификация сетей: по типу соединения, по способу передачи, по масштабам.
3. Архитектура открытых сетей. Структура и состав семиуровневого представления сетей. Информационные технологии локальных и глобальных сетей. Internet и Intranet.
4. Электронная почта. Проектирование и использование Web-интерфейса в системах электронного декларирования. Космическая информационно- вычислительная сеть ФТС.

Тема 10. Обеспечение информационной безопасности таможенных органов

1. Политика ФТС России в области обеспечения информационной безопасности таможенных органов. Понятие и структура информационной безопасности.
2. Характер и формы угроз. Модель нарушителя информационной безопасности ЕАИС. Формы обеспечения информационной безопасности ЕАИС.
3. Организационно-правовые основы информационной безопасности.

Тема 11. Единая автоматизированная информационная система ФТС России

1. Предпосылки создания I и II очереди ЕАИС. Архитектура системы, территориальное распределение.
2. Принципы построения ЕАИС. Требования к ЕАИС. Функционирование и эксплуатация. Режимы обработки данных в ЕАИС.
3. Виды обеспечений ЕАИС: техническое, технологическое, информационное, программное, лингвистическое. Технологии электронного документооборота в ЕАИС.
4. Основные направления модернизации функциональных таможенных технологий

Тема 12. Базы информационных данных ЕАИС ФТС России

1. Основные понятия процесса накопления данных. Системы управления базой данных. Особенности баз данных, используемых в ФТС России.
2. Распределенные технологии обработки и хранения данных. Использование в ФТС России систем, ориентированных на анализ данных.
3. Хранилища данных в ЕАИС. Методы анализ данных в хранилищах данных. Особенности OLAP-технологий при формировании таможенной статистики. CASE-системы.
4. Автоматизация формирования информационной среды предметной области. Информационно-поисковые системы.

Тема 13. Правовые основы применения электронных документов деятельности

1. Международные и отечественные нормы права, определяющие возможность применения информационных технологий в торговле и таможенном деле.
2. Правовые основы электронной подписи, электронного декларирования и предварительного информирования

Тема 14. Автоматизированные информационные системы таможенного декларирования и контроля

1. Функциональные АРМы и их взаимодействие. Особенности и недостатки существующих АРМов сотрудников таможенных органов.
2. Комплексные автоматизированные средства таможенных органов. Единая система нормативно-справочной информации (НСИ). Аналитический обзор существующих подходов к обработке таможенной статистики.
3. Комплексные системы автоматизации таможенной деятельности "Аист-РТ21" и "Аист-М". Структура и задачи информационно-справочных систем "Гарант" и "Консультант".
4. Практическая методика получения нормативно-справочной информации с использованием распределенных и телекоммуникационных систем.

5.2. Разделы, темы дисциплины и виды занятий

очная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в ак. часах)				Аудиторных занятий в интерактивной форме
		занятия лекционного типа	занятия семинарского типа /из них в форме практической подготовки	самостоятельная работа	Всего	
1.	Тема 1. Основные понятия и положения информационной безопасности.	2	4	8	14	
2.	Тема 2. Угрозы безопасности информации в информационных системах.	2	2	8	12	
3.	Тема 3. Методы и средства защиты информации.	2	2	8	12	
4.	Тема 4. Криптографические методы защиты информации.	4	4	8	16	
5.	Тема 5. Аппаратные и программные средства защиты компьютерной информации.	4	4/2	8	16	
6.	Тема 6. Безопасность компьютерных сетей.	4	4/2	10	18	
7.	Тема 7. Роль информационных технологий в таможенном деле. Информационные системы и технологии.	2	4/2	10	16	
8	Тема 8. Информационно-техническая политика ФТС России	2	4/2	10	16	
9	Тема 9. Сетевые технологии и информационная безопасность в таможенной деятельности	2	4/2	10	16	
10	Тема 10. Обеспечение информационной безопасности таможенных органов	2	4/2	10	16	
11	Тема 11. Единая автоматизированная информационная система ФТС	2	4/2	10	16	
12	Тема 12. Базы информационных данных ЕАИС ФТС России	2	4/2	10	16	2
13	Тема 13. Правовые основы применения электронных документов деятельности	2	4/2	10	16	
14	Тема 14. Автоматизированные информационные системы таможенного декларирования и контроля	2	4/2	9,5	15,5	2
	Подготовка к экзамену				36	

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в ак. часах)				Аудиторных занятий в интерактивной форме
		занятия лекционного типа	занятия семинарского типа /из них в форме практической подготовки	самостоятельная работа	Всего	
	Контактная работа в период промежуточной аттестации				0,5	
	Итого	34	52/20	129,5	252	4

заочная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в ак. часах)				Аудиторных занятий в интерактивной форме
		занятия лекционного типа	занятия семинарского типа /из них в форме практической подготовки	самостоятельная работа	Всего	
1.	Тема 1. Основные понятия и положения информационной безопасности.	2	1	16	19	
2.	Тема 2. Угрозы безопасности информации в информационных системах.	2	1	16	19	1
3.	Тема 3. Методы и средства защиты информации.		1	16	17	
4.	Тема 4. Криптографические методы защиты информации.			16	16	
5.	Тема 5. Аппаратные и программные средства защиты компьютерной информации.		1	16	17	
6.	Тема 6. Безопасность компьютерных сетей.			16	16	
7.	Тема 7. Роль информационных технологий в таможенном деле. Информационные системы и технологии.	2	2	16	20	1
8	Тема 8. Информационно-техническая политика ФТС России			16	16	
9	Тема 9. Сетевые технологии и информационная безопасность в таможенной деятельности			16	16	
10	Тема 10. Обеспечение информационной безопасности таможенных органов	2	2/1	16	20	
11	Тема 11. Единая			16	16	

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в ак. часах)				Аудиторных занятий в интерактивной форме
		занятия лекционного типа	занятия семинарского типа /из них в форме практической подготовки	самостоятельная работа	Всего	
	автоматизированная информационная система ФТС					
12	Тема 12. Базы информационных данных ЕАИС ФТС России			16	16	
13	Тема 13. Правовые основы применения электронных документов деятельности		2/1	16	18	
14	Тема 14. Автоматизированные информационные системы таможенного декларирования и контроля			16,5	16,5	
	Подготовка к экзамену				9	
	Контактная работа в период промежуточной аттестации				0,5	
	Итого	8	10/2	224,5	252	2

6. Лабораторные занятия

Лабораторные занятия не предусмотрены.

7. Практические занятия

очная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)	В т.ч. в форме практической подготовки
1.	Тема 1. Основные понятия и положения информационной безопасности.	Информация, сообщения, информационные процессы как объекты информационной безопасности. Цели и задачи защиты информации. Классификационная схема понятий в области защиты информации. Концептуальные основы защиты информации. Основные положения государственной политики обеспечения информационной безопасности РФ	4	
2.	Тема 2. Угрозы безопасности информации в информационных системах.	Основные виды атак на информационные АС. Классификация основных атак и вредоносных программ.	2	
3.	Тема 3. Методы и средства защиты информации.	Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Основные	2	

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)	В т.ч. в форме практической подготовки
		требования к системам защиты в TCSEC. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.		
4.	Тема 4. Криптографические методы защиты информации.	Требования к методам шифрования и их классификация. Криптостойкость шифра как основной показатель его эффективности. Методы шифрования с симметричным ключом: методы замены, методы перестановки, аналитические методы, аддитивные методы, комбинированные методы. Системы шифрования с открытым ключом. Стандарты шифрования. Перспективы использования криптозащиты информации.	4	
5.	Тема 5. Аппаратные и программные средства защиты компьютерной информации.	Основные понятия программно-технического уровня информационной безопасности. Архитектурная безопасность. Современные способы и средства негласного получения информации по различным каналам. Пассивные и активные способы обеспечения информационной безопасности. Современные средства выявления каналов утечки информации	4	2
6.	Тема 6. Безопасность компьютерных сетей.	Основные аспекты безопасности компьютерных сетей (КС). Атакуемые сетевые компоненты на разных уровнях модели OSI, уязвимости сетевых служб (DNS, Telnet), средств передачи информации. Классификация сетевых атак. Межсетевые экраны. Типы и функции межсетевых экранов: пакетных фильтров, прокси-систем, устройств контроля текущего состояния.	4	2
7.	Тема 7. Роль информационных технологий в таможенном деле. Информационные системы и технологии.	Информационные таможенные технологии: история развития; роль и место в управлении таможенными процессами. Характеристика информационных процессов и информационных потоков в системе таможенных органов. Стандарты пользовательского интерфейса для информационных таможенных технологий. Операционные системы. Файловые системы. Системы классификации и кодирования.	4	2
8	Тема 8. Информационно-техническая политика ФТС России	Концепция информационно-технической политики ФТС России. Системы электронного декларирования, документального контроля, оценки	4	2

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)	В т.ч. в форме практической подготовки
		таможенных рисков. Критерии оценки результатов внедрения информационных таможенных технологий.		
9	Тема 9. Сетевые технологии и информационная безопасность в таможенной деятельности	Понятие информационного пространства. Тенденции развития телекоммуникационных технологий. Структура компьютерных сетей. Классификация сетей: по типу соединения, по способу передачи, по масштабам. Архитектура открытых сетей. Структура и состав семиуровневого представления сетей. Информационные технологии локальных и глобальных сетей. Internet и Intranet. Электронная почта. Проектирование и использование Web-интерфейса в системах электронного декларирования. Космическая информационно-вычислительная сеть ФТС.	4	2
10	Тема 10. Обеспечение информационной безопасности таможенных органов	1) Политика ФТС России в области обеспечения информационной безопасности таможенных органов. Понятие и структура информационной безопасности. Характер и формы угроз. Модель нарушителя информационной безопасности ЕАИС. Формы обеспечения информационной безопасности ЕАИС. Организационно-правовые основы информационной безопасности.	4	2
11	Тема 11. Единая автоматизированная информационная система ФТС	Предпосылки создания I и II очереди ЕАИС. Архитектура системы, территориальное распределение. Принципы построения ЕАИС. Требования к ЕАИС. Функционирование и эксплуатация. Режимы обработки данных в ЕАИС. Виды обеспечений ЕАИС: техническое, технологическое, информационное, программное, лингвистическое. Технологии электронного документооборота в ЕАИС. Основные направления модернизации функциональных таможенных технологий	4	2
12	Тема 12. Базы информационных данных ЕАИС ФТС России	Основные понятия процесса накопления данных. Системы управления базой данных. Особенности баз данных, используемых в ФТС России. Распределенные технологии обработки и хранения данных. Использование в ФТС	4	2

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)	В т.ч. в форме практической подготовки
		<p>России систем, ориентированных на анализ данных.</p> <p>Хранилища данных в ЕАИС. Методы анализ данных в хранилищах данных. Особенности OLAP-технологий при формировании таможенной статистики. CASE-системы.</p> <p>Автоматизация формирования информационной среды предметной области. Информационно-поисковые системы.</p>		
13	Тема 13. Правовые основы применения электронных документов деятельности	<p>Международные и отечественные нормы права, определяющие возможность применения информационных технологий в торговле и таможенном деле.</p> <p>Правовые основы электронной подписи, электронного декларирования и предварительного информирования</p>	4	2
14	Тема 14. Автоматизированные информационные системы таможенного декларирования и контроля	<p>Функциональные АРМы и их взаимодействие. Особенности и недостатки существующих АРМов сотрудников таможенных органов.</p> <p>Комплексные автоматизированные средства таможенных органов. Единая система нормативно-справочной информации (НСИ). Аналитический обзор существующих подходов к обработке таможенной статистики.</p> <p>3. Комплексные системы автоматизации таможенной деятельности "Аист-РТ21" и "Аист-М". Структура и задачи информационно-справочных систем "Гарант" и "Консультант".</p> <p>4. Практическая методика получения нормативно-справочной информации с использованием распределенных и телекоммуникационных систем.</p>	4	2
	Итого		52	20

заочная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)	В т.ч. в форме практической подготовки
1	Тема 1. Основные понятия и положения информационной безопасности.	Информация, сообщения, информационные процессы как объекты информационной безопасности. Цели и задачи защиты информации. Классификационная схема понятий в области защиты информации. Концептуальные основы защиты информации. Основные положения государственной политики обеспечения информационной безопасности РФ	1	
2	Тема 2. Угрозы безопасности информации в информационных системах.	Основные виды атак на информационные АС. Классификация основных атак и вредоносных программ.	1	
3	Тема 3. Методы и средства защиты информации.	Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Основные требования к системам защиты в TCSEC. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.	1	
4	Тема 5. Аппаратные и программные средства защиты компьютерной информации.	Основные понятия программно-технического уровня информационной безопасности. Архитектурная безопасность. Современные способы и средства негласного получения информации по различным каналам. Пассивные и активные способы обеспечения информационной безопасности. Современные средства выявления каналов утечки информации	1	
5	Тема 7. Роль информационных технологий в таможенном деле. Информационные системы и технологии.	Информационные таможенные технологии: история развития; роль и место в управлении таможенными процессами. Характеристика информационных процессов и информационных потоков в системе таможенных органов. Стандарты пользовательского интерфейса для информационных таможенных технологий. Операционные системы. Файловые системы. Системы классификации и кодирования.	2	
6	Тема 10. Обеспечение информационной безопасности таможенных органов	1) Политика ФТС России в области обеспечения информационной безопасности таможенных органов. Понятие и структура информационной безопасности. Характер и формы угроз. Модель нарушителя информационной безопасности ЕАИС. Формы	2	1

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)	В т.ч. в форме практической подготовки
		обеспечения информационной безопасности ЕАИС. Организационно-правовые основы информационной безопасности.		
7	Тема 13. Правовые основы применения электронных документов деятельности	Международные и отечественные нормы права, определяющие возможность применения информационных технологий в торговле и таможенном деле. Правовые основы электронной подписи, электронного декларирования и предварительного информирования	2	1
	Итого		10	2

8. Тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Информационная безопасность в Российской Федерации» направлена на:

– освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы;

– изучение образовательных ресурсов (электронные учебники, электронные библиотеки, электронные видеокурсы и др.);

– работу с компьютерными обучающими программами;

– выполнение домашних заданий по практическим занятиям;

– самостоятельный поиск информации в Интернете и других источниках;

– подготовку к экзамену.

Тема 1. Основные понятия и положения информационной безопасности.

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Основные понятия и положения информационной безопасности.

В процессе усвоения темы необходимо усвоение студентами основных понятий и положений информационной безопасности.

Оценочные средства: Устный опрос, практическая работа.

Тема 2. Угрозы безопасности информации в информационных системах.

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Угрозы безопасности информации в информационных системах.

В процессе усвоения темы необходимо усвоение студентами основных угроз безопасности информации в информационных системах.

Оценочные средства: решение задач.

Тема 3. Методы и средства защиты информации.

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Методы и средства защиты информации.

В процессе усвоения темы необходимо усвоение студентами основных методов и средств защиты информации.

Оценочные средства: практическая работа.

Тема 4. Криптографические методы защиты информации.

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Криптографические методы защиты информации.

В процессе усвоения темы необходимо усвоение студентами основных криптографических методов защиты информации.

Оценочные средства: устный опрос, тест.

Тема 5. Аппаратные и программные средства защиты компьютерной информации.

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Криптографические методы защиты информации.

В процессе усвоения темы необходимо усвоение студентами аппаратных и программных средств защиты компьютерной информации.

Оценочные средства: решение задач

Тема 6. Безопасность компьютерных сетей.

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Безопасность компьютерных сетей.

В процессе усвоения темы необходимо усвоение студентами основных положений безопасности компьютерных сетей.

Оценочные средства: устный опрос.

Тема 7. Роль информационных технологий в таможенном деле. Информационные системы и технологии.

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Роль информационных технологий в таможенном деле. Информационные системы и технологии.

В процессе усвоения темы необходимо усвоение студентами информационных систем и технологий, применяемых в таможенных органах Российской Федерации.

Оценочные средства: устный опрос, практические задания.

Тема 8. Информационно-техническая политика ФТС России

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Информационно-техническая политика ФТС России.

В процессе усвоения темы необходимо усвоение студентами основных положений информационно-технической политики ФТС России.

Оценочные средства: доклад, групповое обсуждение.

Тема 9. Сетевые технологии и информационная безопасность в таможенной деятельности

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Сетевые технологии и информационная безопасность в таможенной деятельности.

В процессе усвоения темы необходимо усвоение студентами технологии и информационной безопасности в таможенной деятельности.

Оценочные средства: устный опрос, практические задания.

Тема 10. Обеспечение информационной безопасности таможенных органов

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Обеспечение информационной безопасности таможенных органов.

В процессе усвоения темы необходимо усвоение студентами основных способов и методов обеспечения информационной безопасности таможенных органов.

Оценочные средства: кейс-задачи.

Тема 11. Единая автоматизированная информационная система ФТС.

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Единая автоматизированная информационная система ФТС.

В процессе усвоения темы необходимо усвоение студентами основных компонентов, принципов действия Единой автоматизированной информационной системы ФТС.

Оценочные средства: доклад.

Тема 12. Базы информационных данных ЕАИС ФТС России

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Базы информационных данных ЕАИС ФТС России.

В процессе усвоения темы необходимо усвоение студентами компонентов, принципов действия ЕАИС ФТС России.

Оценочные средства: задачи.

Тема 13. Правовые основы применения электронных документов деятельности

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Правовые основы применения электронных документов деятельности.

В процессе усвоения темы необходимо усвоение студентами правовых основ применения электронных документов деятельности.

Оценочные средства: доклад.

Тема 14. Автоматизированные информационные системы таможенного декларирования и контроля

Изучение рекомендуемой литературы и источников, подготовка опорного конспекта по теме Автоматизированные информационные системы таможенного декларирования и контроля.

В процессе усвоения темы необходимо усвоение студентами основных положений автоматизированной информационной системы таможенного декларирования и контроля.

Оценочные средства: доклад.

10. Перечень нормативных правовых актов, основной и дополнительной учебной литературы, необходимых для освоения дисциплины

а) нормативные документы:

1. Федеральный закон от 21 июля 1997 г. № 114-ФЗ «О службе в таможенных органах Российской Федерации» [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». — URL: <http://www.consultant.ru>

3. Федеральный закон от 27 мая 2003 г. № 58-ФЗ «О системе государственной службы Российской Федерации» [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». — URL: <http://www.consultant.ru>.

4. Федеральный закон от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». — URL: <http://www.consultant.ru>

5. Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». — URL: <http://www.consultant.ru>

6. Распоряжение Правительства РФ от 28 декабря 2012 г. № 2575-р «О Стратегии развития таможенной службы Российской Федерации до 2020 года» [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». — URL: <http://www.consultant.ru>.

7. Приказ ФТС России от 18 октября 2005 г. № 970 «Об утверждении Положения об организационно-штатной работе в таможенных органах Российской Федерации и в учреждениях, находящихся в ведении ФТС России» [Электронный ресурс] // Информационно-правовой портал «BestPravo». — URL: <http://www.bestpravo.ru>.

б) основная литература:

1. Староверова, К. О. Информационная безопасность в Российской Федерации: учебник и практикум для вузов. - Москва: Издательство Юрайт, 2019. — 240 с. — (Специалист). — ISBN 978-5-534-00283-6. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <https://bibliotonline.ru/bcode/437194>

2. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва: ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1013711> – Режим доступа: по подписке.

в) дополнительная литература:

1. Управление информационной безопасностью : учебник / Николаев Н.С. — Москва : КноРус, 2021. — 188 с. — ISBN 978-5-406-07325-4. — URL: <https://book.ru/book/939841> — Текст : электронный.

2. Базовые понятия информационной безопасности : учебное пособие / Крылов Г.О., Ларионова С.Л., Никитина В.Л. — Москва : Русайнс, 2020. — 257 с. — ISBN 978-5-4365-1557-1. — URL: <https://book.ru/book/932492> — Текст : электронный.

3. Информационная безопасность : учебник / Мельников В.П., под ред., Куприянов А.И., Васильева Т.Ю. — Москва : КноРус, 2020. — 371 с. — ISBN 978-5-406-07695-8. — URL: <https://book.ru/book/932908> — Текст : электронный.

4. Основы информационной безопасности : учебное пособие / Литвиненко В.И., Козлов Е.С. — Москва : КноРус, 2020. — 199 с. — ISBN 978-5-406-00904-8. — URL: <https://book.ru/book/934627> — Текст : электронный.

5. Информационная безопасность : практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2019. - 84 с. - ISBN 978-5-91612-276-3. - Текст :

электронный. - URL: <https://znanium.com/catalog/product/1094244> – Режим доступа: по подписке.

11. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения, профессиональных баз данных и информационных справочных систем

1. Ресурсы информационно-телекоммуникационной сети «Интернет», включая профессиональные базы данных
 - <http://www.customs.ru/> - Официальный сайт Федеральной таможенной службы
 - 2. <http://www.alta.ru/> - Программное обеспечение участника ВЭД
 - 3. <http://www.vch.ru/> - Информационно-консультационная система «Виртуальная таможня»
 - 4. <http://www.customs.fem.ru/> - Информационная система Таможня Консультант
 - 5. <http://www.logist-ics.ru/> - Информационно-консалтинговая служба
 - 6. <http://www.tsouz.ru/> - Сайт Комиссии таможенного союза
 - 7. www.wcoomd.org. – Сайт Всемирной таможенной организации
 - 8. www.worldcustomsjournal.org – Международный таможенный электронный журнал

- <https://www.book.ru/> - ЭБС Book.ru
- <http://www.iprbookshop.ru> - ЭБС IPRbooks
- <https://ibooks.ru/> -ЭБС Айбукс.ru/ibooks.ru
- <https://rucont.ru/> - ЭБС «Национальный цифровой ресурс «Руконт»
- <http://znanium.com/> - ЭБС Znanium.com
- <https://dlib.eastview.com/>- База данных East View

2. Информационно-справочные системы

СПС КонсультантПлюс. Компьютерная справочная правовая система, широко используется учеными, студентами и преподавателями (подписка на ПО)

3. Лицензионно программное обеспечение

1. Desktop School ALNG LicSAPk MVL.
 - a. Office ProPlus All LngLic/SA Pack MVL Partners in Learning (лицензиянапакет Office Professional Plus)
 - b. Windows 8
2. Консультант + версия проф.- справочная правовая система
3. Система тестирования INDIGO.
4. 1С: Предприятие 8

4. Свободно распространяемое программное обеспечение
1. AdobeAcrobat – свободно-распространяемое ПО
 2. Интернет-браузерыGoogleChrome, Firefox – свободно-распространяемое ПО

Каждый обучающийся в течение всего обучения обеспечивается индивидуальным неограниченным доступом электронно-библиотечной системе и электронной информационно-образовательной среде.

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

Образовательный процесс обеспечивается специальными помещениями, которые представляют собой аудитории для проведения занятий лекционного типа, занятий семинарского типа, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы студентов и помещения для хранения и профилактического обслуживания учебного оборудования.

Специальные помещения соответствуют действующим противопожарным правилам и нормам, укомплектованы специализированной мебелью.

Аудитории лекционного типа, оснащенные проекционным оборудованием и техническими средствами обучения, обеспечивающими представление учебной информации большой аудитории, демонстрационным оборудованием.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, обеспечивающей доступ к сети Интернет и электронной информационно-образовательной среде университета.