Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
Среднерусский институт управления - филиал
ФАКУЛЬТЕТ «Государственное, муниципальное управление и экономика народного хозяйства»
КАФЕДРА «Социология и информационные технологии»

Меркулов Павел Александрович

Подписан: Меркулов Павел Александрович
Основание: я подтверждаю этот документ
Местоположение: Среднерусский институт управления - филиал РАНХиГС
Дата: 2021.02.03 13:33:44+03'00'

УТВЕРЖДЕНА
решением кафедры «Социология и информационные технологии»
Протокол №1 от 27.08.2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.Б.30 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ТАМОЖЕННОМ ДЕЛЕ

Направление подготовки 38.05.02 Таможенное дело
Специализация: «Таможенные операции и таможенный контроль»
Квалификация: специалист таможенного дела
Форма обучения: заочная
Год набора: 2020

Орел, 2019 г.

Автор-составитель:

канд. техн. наук, доцент кафедры
«Социология и информационные технологии» В.В. Николаев

Заведующая кафедрой
«Социология и информационные технологии»
доктор социологических наук, доцент Н.В. Проказина

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 4

2. Объем и место дисциплины в структуре образовательной программы 7

3. Содержание и структура дисциплины 7

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине 9

5. Методические указания для обучающихся по освоению дисциплины 29

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине 30

6.1. Основная литература 30

6.2. Дополнительная литература 31

6.3. Учебно-методическое обеспечение самостоятельной работы 32

6.4. Нормативные правовые документы 32

6.5. Интернет-ресурсы 32

6.6. Иные источники 32

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы 33

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Дисциплина «Информационная безопасность в таможенном деле» обеспечивает овладение следующими компетенциями:

ОПК-3 - способность владеть методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей;

ПК-17 – умение выявлять и анализировать угрозы экономической безопасности страны при осуществлении профессиональной деятельности;

ПК-32 – владение навыками применения в таможенном деле информационных технологий и средств обеспечения их функционирования в целях информационного сопровождения профессиональной деятельности;

ПК-35 – владение навыками использования электронных способов обмена информацией и средств их обеспечения, применяемых таможенными органами.

Этапы освоения компетенций

Таблица 1

Код компетенции	Наименование компетенции	Код этапа освоения компетенций	Наименование этапа компетенции
ОПК - 3	способность владеть методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей	ОПК - 3.2	Способностью обеспечения информационной безопасности в деятельности таможенных органов, прогнозирования финансово-экономических показателей в таможенной деятельности
ПК - 17	умение выявлять и анализировать угрозы экономической безопасности страны при осуществлении профессиональной деятельности	ПК - 17.1	Умение выявлять при осуществлении профессиональной деятельности реальные и потенциальные угрозы экономической безопасности страны с использованием современных информационных технологий
ПК - 32	владение навыками применения в таможенном деле информацион-	ПК - 32.1	Способностью применять современные методы для выявления потенциальных и реальных угроз ин-

Код компетенции	Наименование компетенции	Код этапа освоения компетенций	Наименование этапа компетенции
	ных технологий и средств обеспечения их функционирования в целях информационного сопровождения профессиональной деятельности		формационной безопасности в таможенной деятельности в области использования IT-технологий и управления IT-контентом
ПК - 35	владение навыками использования электронных способов обмена информацией и средств их обеспечения, применяемых таможенными органами	ПК - 35.1	Владение навыками обеспечения информационной безопасности в деятельности таможенных органов с использованием информационных технологий

1.2. В результате освоения дисциплины у студентов должны быть: Результаты освоения компетенций

Таблица 2

ОТФ	Код этапа освоения компетенции	Результаты обучения
разработка системы управления рисками; внедрение системы управления рисками; эксплуатация системы управления рисками; координация работ по технико-информацион	ОПК-3.2	- сформированы знания: современные методы и средства создания, хранения, обработки и передачи информации; в области защиты информации, хранящейся на рабочих станциях и серверах таможенных органов, подключенных к сети Интернет, а также при ее передаче по открытым каналам Интернет - сформированы умения: реализовывать способы защиты информации при работе в информационных системах; - сформированы навыки: использования компьютерной техники, программных средств и компьютерных сетей; освоения практических приемов защиты рабочих станций и серверов в таможенных органах
	ПК - 17.1	- сформированы знания: об основных принципах формирования на основе научных подходов современных систем

ному обеспечению системы управления рисками		обеспечения информационной безопасности, месте и роли деятельности по выявлению, предотвращению и нейтрализации угроз экономической безопасности в данных системах; классификация угроз и составление модели нарушителя; - сформированы умения: анализировать уязвимости информационных систем, применяемых в профессиональной деятельности; - сформированы навыки: выявления на основе научных подходов потенциальных и реальных угроз экономической безопасности страны с использованием современных информационных технологий; защиты данных от внешних и внутренних угроз
	ПК - 32.1	- сформированы знания: методов и приемов противодействия возможным угрозам в области состояния и сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере; применения информационных технологий в профессиональной деятельности; - сформированы умения: использовать организационные, программные и технические методы защиты информации; - сформированы навыки: применения информационных технологий и средств обеспечения их функционирования
	ПК - 35.1	- сформированы знания: в области защиты информации, хранящейся на рабочих станциях и серверах таможенных органов, подключенных к сети Интернет, а также при ее передаче по открытым каналам Интернет; электронных средств обмена информацией; - сформированы умения: обеспечивать защиту каналов передачи данных; - сформированы навыки: освоения практических приемов защиты рабочих станций и серверов в таможенных органах; использования электронных средств обмена информацией с соблюдением требований

		информационной безопасности

2. ОБЪЕМ И МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Объем дисциплины

Таблица 3

Вид учебных занятий и самостоятельной работы		**Объем дисциплины, час.**									
		Всего	**Семестр**								
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Контактная работа обучающихся с преподавателем, в том числе:		19				19						
Лекционного типа (Л)		4				4						
Лабораторные работы (ЛР)												
Практического типа (ПЗ)		6				6						
Контролируемая самостоятельная работа обучающихся (КСР):		9				9						
Самостоятельная работа обучающихся (СР) (всего):		89				89						
Промежуточная аттестация	**Форма**	экзамен				экзамен						
	Час.	27				27						
Общая трудоемкость (час./з.е.)		108/3										

Место дисциплины в структуре ОП ВО

Дисциплина «Информационная безопасность в таможенном деле» изучается на 2-ом курсе в 4-ом семестре, общая трудоемкость дисциплины 3 з.е.

Дисциплина «Информационная безопасность в таможенном деле» относится к базовой части (Б1.Б.30) подготовки специалистов по направлению 38.05.02 «Таможенное дело» специализация «Таможенные операции и таможенный контроль».

Освоение дисциплины опирается на приобретенные ранее умения и навыки использования персонального компьютера и системного и прикладного программного обеспечения.

Дисциплина «Информационная безопасность в таможенном деле» является предшествующей для дисциплин Б1.Б.07 «Информационные технологии в таможенном деле», Б1.Б.20 «Экономическая безопасность».

Количество академических часов, выделенных на контактную работу с преподавателем, - 54 часов, на самостоятельную работу - 27 часов.

Форма промежуточной аттестации в соответствии с учебным планом - экзамен.

3. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Таблица 4

Структура дисциплины

№ п/п	Наименование тем (разделов)	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости / промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
1	Теоретические основы информационной безопасности	36	2		2	2	30	О1, Т1
2	Система обеспечения информационной безопасности	38	2		2	4	30	О2, Т2
3	Технологии защиты информации	44			2	3	39	О3, Т3
Промежуточная аттестация		27						Экзамен
Всего:		108	4		6	9	89	

Примечание. Форма текущего контроля успеваемости: опрос (О), тестирование (Т).

Содержание дисциплины

Тема 1. Теоретические основы информационной безопасности

Информационная безопасность: содержание и структура понятия. Законодательный уровень информационной безопасности. Стандарты информационной безопасности. Административный уровень информационной безопасности. Процедурный уровень информационной безопасности.

Тема 2. Система обеспечения информационной безопасности

Система менеджмента информационной безопасности. Организационный уровень информационной безопасности. Программно-технический уровень информационной безопасности. Методы и средства защиты информа-

ции. Оценка уровня защищенности ИС. Оценка рисков. Классификация угроз информационной безопасности. Построение модели угроз и модели нарушителя.

Тема 3. Технологии защиты информации

Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Основные алгоритмы и стандарты симметричного шифрования. Асимметричные криптосистемы шифрования. Алгоритмы асимметричного шифрования. Функция хэширования. Электронная цифровая подпись. Алгоритмы и стандарты ЭЦП. Проблемы обеспечения безопасности операционных систем. Функции межсетевых экранов. Концепция построения виртуальных защищенных сетей VPN. Компьютерные вирусы и проблемы антивирусной защиты. Обзор современных систем управления сетевой защитой.

4. МАТЕРИАЛЫ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ ОБУЧАЮЩИХСЯ И ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации

4.1.1. В ходе реализации дисциплины «Информационная безопасность в таможенном деле» используются следующие методы текущего контроля успеваемости обучающихся:

– при проведении занятий лекционного типа: опрос, тестирование;

– при проведении практических занятий: проверка выполненного задания.

4.1.2 Промежуточная аттестация проводится с применением следующих методов (средств):

Экзамен по дисциплине «Информационная безопасность в таможенном деле» проводится в виде устного экзамена по билету, который состоит из двух теоретических вопросов.

4.2. Материалы текущего контроля успеваемости

Типовые оценочные материалы по теме:

Тема 1. Теоретические основы информационной безопасности

1. Предмет и объект изучения дисциплины.
2. Базовые свойства информации с точки зрения информационной безопасности (ИБ).
3. Основные стандарты в области ИБ.
4. Конфиденциальность, доступность, целостность информации как грани информационной безопасности.
5. Организационная зрелость предприятия с точки зрения информационной безопасности.
6. Классификация информационных активов.
7. Основные методы управления рисками.

8. Идентификация, аутентификация и авторизация пользователя.
9. Базовые признаки классификации угроз.
10. Модель нарушителя.

Тема 2. Система обеспечения информационной безопасности

1. Классификация нормативно-правовых актов, регламентирующих сферу информационной безопасности.
2. Доктрина информационной безопасности Российской Федерации.
3. Основные законодательные акты, определяющие в целом юридические аспекты защиты информации.
4. Отношения, регулируемые законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации»
5. Российские стандарты, регулирующие ИБ.
6. Стандарт ГОСТ Р ИСО/МЭК 27001-2006 «Системы менеджмента информационной безопасности».
7. Характеристика стандарта ГОСТ Р ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий».
8. Административный уровень информационной безопасности.

Тема 3. Технологии защиты информации

1. Типичная схема ЛВС организации.
2. Сетевые протоколы TCP/IP.
3. Основные функции подсистемы защиты операционной системы.
4. Классификация криптосистем.
5. Симметричные криптосистемы.
6. Обобщенная схема асимметричной криптосистемы.
7. Классификация компьютерных вирусов. Антивирусные программы
8. Функции межсетевых экранов.
9. Концепция построения виртуальных частных сетей VPN.
10. Виды резервного копирования данных.

Материалы текущего контроля успеваемости

Тема 1. Теоретические основы информационной безопасности

Практическое занятие 1 по теме 1. Исследование точности и сходимости математических моделей.

Методика выполнения:

1. Изучить теоретическую часть практического занятия и ответить на контрольные вопросы.

2. Выбрать задание в соответствии с порядковым номером студента в журнале группы.

3. Выполнить построение математической модели по заданным исходным данным.

4. Провести анализ точности и сходимости расчета.

5. Оформить отчет в соответствии с принятыми стандартами оформления документов и направить его преподавателю.

Практическое занятие 2 по теме 1. Определение характеристик безопасности при решении уравнений

Методика выполнения:

1. Изучить теоретический материал по численным методам решения уравнений.
2. Выбрать задание в соответствии с порядковым номером студента в журнале группы.
3. Выполнить расчет.
4. Определить точность расчета.
5. Определить параметры сходимости и устойчивости решения.
6. Создать файл отчета и направить его преподавателю.

Тема 2. Система обеспечения информационной безопасности

Практическое занятие 1 по теме 2. Изучение способов адресации компьютера в сети

Методика выполнения:

1. Изучить теоретический материал по модели взаимодействия открытых систем
2. Определить простое имя компьютера.
3. Определить способ подключения компьютера к сети.
4. Определить адрес сети.
5. Определить физический адрес компьютера.
6. Создать файл отчета и направить его преподавателю.

Практическое занятие 2 по теме 2. Изучение сетевых настроек компьютера

Методика выполнения:

1. Изучить теоретический материал по стеку протоколов TCP/IP.
2. Определить IP-адрес компьютера.
3. Определить маску сети, адрес шлюза и адрес DNS-сервера.
4. Трассировать маршрут до сервера вуза.
5. Создать файл отчета и направить его преподавателю.

Практическое занятие 3 по теме 2. Изучение способов защиты от несанкционированного доступа

Методика выполнения:

1. Изучить теоретический материал по угрозам конфиденциальности данных.
2. Определить уязвимость аутентификации пользователя.
3. Изучить защиту сетевых ресурсов вуза.
4. Изучить настройки антивирусной программы.
5. Выполнить антивирусную проверку.
6. Создать файл отчета и направить его преподавателю.

Практическое занятие 4 по теме 2. Определение характеристик безопасности при решении систем линейных уравнений

Методика выполнения:

1. Изучить теоретический материал по численным методам расчета систем алгебраических линейных уравнений.
2. Выбрать задание в соответствии с порядковым номером студента в журнале группы.
3. Выполнить расчет, используя матричные вычисления.
4. Определить точность расчета.
5. Определить параметры сходимости и устойчивости решения.
6. Создать файл отчета и направить его преподавателю.

Практическое занятие 5 по теме 2. Исследование устойчивости сложных систем

Методика выполнения:

1. Изучить теоретическую часть практического занятия и ответить на контрольные вопросы.
2. Выбрать задание в соответствии с порядковым номером студента в журнале группы.
3. Выполнить построение математической модели по заданным исходным данным.
4. Провести анализ точности, сходимости и устойчивости расчета.
5. Оформить отчет в соответствии с принятыми стандартами оформления документов и направить его преподавателю.

Тема 3. Технологии защиты информации

Практическое занятие 1 по теме 3. Изучение свойств численных методов расчета

Методика выполнения:

1. Изучить теоретический материал по реализации численных методов расчета.
2. Выбрать задание в соответствии с порядковым номером студента в журнале группы.
3. Выполнить расчет.
4. Определить точность расчета.
5. Определить параметры сходимости и устойчивости решения.
6. Создать файл отчета и направить его преподавателю.

Практическое занятие 2 по теме 3. Исследование методов обеспечения целостности данных

Методика выполнения:

1. Изучить теоретическую часть практического занятия и ответить на контрольные вопросы.
2. Выбрать задание в соответствии с порядковым номером студента в

журнале группы.

3. Выполнить построение математической модели задачи логистики.

4. Получить решение задачи.

5. Провести анализ точности, сходимости и устойчивости расчета.

6. Оформить отчет в соответствии с принятыми стандартами оформления документов и направить его преподавателю.

Практическое занятие 3 по теме 3. Изучение методов симметричной криптографии

Методика выполнения:

1. Изучить теоретический материал по симметричным криптосистемам.

2. Выполнить шифрование методом замены.

3. Выполнить шифрование, используя блочный метод.

4. Выполнить шифрование, используя поточный метод.

5. Выполнить расшифрование, используя ключ.

6. Создать файл отчета и направить его преподавателю.

Практическое занятие 4 по теме 3. Исследование алгоритма асимметричной криптографии Диффи-Хеллмана

Методика выполнения:

1. Изучить теоретическую часть практического занятия и ответить на контрольные вопросы.

2. Выбрать задание в соответствии с порядковым номером студента в журнале группы.

3. Выполнить построение математической модели по заданным исходным данным.

4. Провести анализ требований при использовании алгоритма Диффи-Хеллмана..

5. Оформить отчет в соответствии с принятыми стандартами оформления документов и направить его преподавателю.

Практическое занятие 5 по теме 3. Исследование метода ассиметричной криптографии RSA

Методика выполнения:

1. Изучить теоретическую часть практического занятия и ответить на контрольные вопросы.

2. Выбрать задание в соответствии с порядковым номером студента в журнале группы.

3. Выполнить построение математической модели по заданным исходным данным.

4. Провести анализ требований при использовании RSA.

5. Оформить отчет в соответствии с принятыми стандартами оформления документов и направить его преподавателю.

Типовые тестовые задания по темам

Тема 1. Теоретические основы информационной безопасности

1. Концепция национальной безопасности Российской Федерации учитывает интересы:

а) личности и общества;
б) общества и государства;
в) личности, общества и государства;
г) избирателя, партий и органов законодательной власти

2. Основы государственной политики Российской Федерации в области международной информационной безопасности действуют до:

а) 2015 г.;
б) 2020 г.;
в) 2030 г.;
г) не являются действующим документом

3. Объект защиты информации - это:

а) служебные данные;
б) информация или носитель информации или информационный процесс;
в) носитель информации;
г) персонал

4. Несанкционированный доступ к информации - это:

а) доступ к информации с нарушением установленных правил доступа;
б) изменение или уничтожение данных;
в) доступ к информации без разрешения руководства;
г) копирование данных с нарушением установленных правил доступа

5. Стандарт ГОСТ Р ИСО/МЭК 27001-2006 определяет информационную безопасность как:

а) сохранение конфиденциальности, целостности и достоверности информации;
б) сохранение подлинности, целостности и доступности информации;
в) сохранение конфиденциальности, целостности и доступности информации;
г) сохранение подлинности, целостности и достоверности информации;

6. Первым этапом разработки и внедрения системы управления информационной безопасностью является:

а) вовлеченность руководства предприятия в процесс управления ИБ;
б) оценка информационных рисков;
в) оценка защищенности информационной системы;
г) инвентаризация активов

7. Принятие информационных рисков осуществляется в случае:

а) полного устранения источника риска;
б) если уровень рисков признается приемлемым;
в) перенесения ответственности за риск за страховые компании;
г) внедрения мер по снижению вероятности ущерба

8. Стандарт ГОСТ Р ИСО/МЭК 27002-2012 к защищаемым активам предприятия <u>не относит:</u>

а) информационные ресурсы;
б) программное обеспечение;
в) финансовые активы;
г) персонал, его квалификация, навыки и опыт

9. Стандарт TCSEC (“Оранжевая книга”) к компьютерным системам с минимальной безопасностью относит группу:

а) A;
б) B;
в) C;
г) D

10. Первым этапом процедуры распознавания информационной системой пользователя является:

а) идентификация;
б) авторизация;
в) аутентификация;
г) верификация

11. В соответствии с Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации» обладатель информации <u>не обязан</u>:

а) соблюдать права и законные интересы иных лиц;
б) принимать меры к защите информации;
в) всегда проверять достоверность размещаемой общедоступной информации;
г) ограничивать доступ к информации, если это установлено федеральными законами

12. Защита информации в соответствии с Федеральным законом №149-ФЗ «Об информации, информационных технологиях и о защите информации» <u>не включает</u>:

а) обеспечение достоверности;
б) соблюдение конфиденциальности;
в) реализацию доступности;
г) оценку рисков

13. Владелец сайта обязан обеспечить соблюдение законодательства РФ, если число пользователей в сутки составляет:

а) 5000;
б) 3000;
в) 2000;
г) 1000

14. Среда для хранения и обработки данных пользователя, предоставляемая в виде онлайн-сервиса:

а) Всемирная паутина;
б) облачные технологии;
в) социальная сеть;

г) распределенные базы данных

15. Репликация данных - это:

а) проверка прав доступа к данным;

б) уничтожение данных;

в) проверка целостности;

г) копирование данных

Тема 2. Система обеспечения информационной безопасности

16. Стандарт ГОСТ Р ИСО/МЭК 27001-2006 называется:

а) Системы менеджмента информационной безопасности;

б) “Оранжевая книга”;

в) Критерии оценки безопасности информационных технологий;

г) Защита информации. Основные термины и определения

17. Стандарт ГОСТ Р ИСО/МЭК 27001-2006 определяет информационную безопасность как:

а) сохранение конфиденциальности, целостности и достоверности информации;

б) сохранение подлинности, целостности и доступности информации;

в) сохранение конфиденциальности, целостности и доступности информации;

г) защиту интересов личности, общества и государства

18. Стандарт ГОСТ Р ИСО/МЭК 27002-2012 относит к активам:

а) информационные ресурсы;

б) всё, что имеет ценность для организации;

в) программно-техническое обеспечение;

г) персонал, его квалификацию, навыки и опыт

19. Вторым этапом разработки и внедрения системы управления информационной безопасностью является:

а) инвентаризация активов;

б) оценка информационных рисков;

в) оценка защищенности информационной системы;

г) категорирование активов

20. Уклонение от информационных рисков осуществляется в случае:

а) полного устранения источника риска;

б) если уровень рисков признается приемлемым;

в) перенесения ответственности за риск за страховые компании;

г) внедрению мер по снижению вероятности ущерба

21. Вовлеченность руководства предприятия в процесс управления информационной безопасностью предполагает:

а) личный контроль и выполнение руководством требований ИБ;

б) личный контроль;

в) выполнение руководством требований ИБ;

г) постановку задач по обеспечению ИБ

22. Стандарт ГОСТ Р ИСО/МЭК 15408 называется:

а) об информации, информационных технологиях и защите информации;

б) система менеджмента информационной безопасности;
в) методы и средства обеспечения безопасности;
г) критерии оценки безопасности информационных технологий

23. Стандарт TCSEC (“Оранжевая книга”) к компьютерным системам с максимальной безопасностью относит группу:

а) A;
б) B;
в) C;
г) D

24. Процедура предоставления законному пользователю соответствующих полномочий называется:

а) идентификация;
б) авторизация;
в) аутентификация;
г) верификация

25. Контроль за созданием средств защиты информации обеспечивается посредством:

а) обязательного лицензирования деятельности;
б) обязательного лицензирования деятельности и сертификацией средств защиты;
в) сертификацией средств защиты;
г) проведением единой технической политики

26. Максимальную скорость передачи данных обеспечивают:

а) беспроводная передача данных;
б) проводные линии связи;
в) оптоволоконные линии связи;
г) сотовые технологии

27. С точки зрения защиты информации наиболее уязвимы:

а) беспроводная передача данных;
б) проводные линии связи;
в) оптоволоконные линии связи;
г) бумажные технологии

28. Криптосистема с использованием разных ключей для зашифрования и расшифрования называется:

а) неоднородной;
б) симметричной;
в) асимметричной;
г) сложной

29. Инфраструктура открытых ключей называется:

а) PKI;
б) VPN;
в) ISP;
г) DNS

30. Попытка прочесть зашифрованный текст без знания ключа называется:

а) гаммирование;
б) расшифрование;
в) зашифрование;
г) дешифрование

Тема 3. Технологии защиты информации

31. Компонент ОС, позволяющий создать виртуальную машину, называется :
а) планировщик;
б) браузер;
в) реестр;
г) гипервизор

32. Криптосистема с использованием одного и того же ключа для зашифрования и расшифрования называется:
а) однородной;
б) симметричной;
в) асимметричной;
г) простой

33. Система криптографии с открытыми ключами называется:
а) однородной;
б) симметричной;
в) асимметричной;
г) сложной

34. Шифрование с использованием некоторой ключевой последовательности (гаммы) используется:
а) в блочных шифрах;
б) в поточных шифрах;
в) не используется;
г) в подстановочных криптограммах

35. Число уровней в модели взаимодействия открытых систем, предложенной ISO:
а) 7;
б) 6;
в) 5;
г) 4

36. В стеке протоколов TCP/IP к уровню приложений относится протокол:
а) HTTP;
б) IP;
в) TCP;
г) ARP

37. Протокол сетевого уровня в стеке протоколов TCP/IP:
а) HTTP;
б) TCP;
в) IP;

г) FTP

38. DNS-сервер предназначен для:

а) преобразования доменных имен компьютеров в IP-адреса;
б) обеспечения доступа компьютеров ЛВС в Интернет;
в) авторизации пользователей;
г) репликации данных

39. Прокси-сервер предназначен для:

а) резервного копирования информации;
б) обеспечения доступа компьютеров ЛВС в Интернет;
в) авторизации пользователей;
г) защиты от компьютерных вирусов

40. Межсетевой экран также называют:

а) прокси-сервер;
б) firewall и брандмауэр;
в) хаб;
г) маршрутизатор

41. Технология VPN:

а) обеспечивает защищенную связь поверх публичной сети;
б) обеспечивает резервное копирование данных;
в) используется только внутри ЛВС;
г) используется только в глобальных сетях

42. Задача центра сертификации в криптографии:

а) подтвердить наличие документированных процедур;
б) сертифицировать предоставляемые услуги;
в) подтвердить подлинность ключей шифрования;
г) обеспечить передачу зашифрованных данных

43. К функциям электронной цифровой подписи <u>не относится</u>:

а) удостоверение авторства;
б) невозможность отказа от авторства;
в) гарантирование целостности данных;
г) восстановление исходного текста документа

44. Компьютерный вирус, маскирующийся под легальное программное обеспечение, называется:

а) червь;
б) троян;
в) бот;
г) эксплойт

45. Дисковый массив RAID, обеспечивающий распределенное хранение данных и кодов четности:

а) RAID 0;
б) RAID 1;
в) RAID 5;
г) JBOD

Ответы на типовые тестовые задания

№ вопроса	ОТВЕТ
Тема 1	
1	**В**
2	**Б**
3	**Б**
4	**А**
5	**В**
6	**Г**
7	**Б**
8	**В**
9	**Г**
10	**А**
11	**В**
12	**Г**
13	**В**
14	**Б**
15	**Г**
Тема 2	
16	**А**
17	**В**
18	**Б**
19	**Г**
20	**В**
21	**А**
22	**В**
23	**А**
24	**Б**
25	**Б**
26	**В**
27	**А**
28	**В**
29	**А**
30	**Г**
Тема 3	
31	**Г**
32	**Б**
33	**В**
34	**Б**
35	**А**
36	**А**
37	**В**
38	**А**
39	**Б**
40	**Б**

41	**А**
42	**В**
43	**Г**
44	**Г**
45	**В**

Вопросы для контроля самостоятельной работы

1. Предмет и объект изучения дисциплины.
2. Организационная зрелость предприятия с точки зрения информационной безопасности.
3. Сущность объектно-ориентированного подхода применительно к проблемам информационной безопасности.
4. Базовые свойства информации с точки зрения информационной безопасности.
5. Основные международные стандарты в области ИБ.
6. Базовые признаки классификации угроз.
7. Основные законодательные акты, определяющие в целом юридические аспекты защиты информации.
8. Стандарт ГОСТ Р ИСО/МЭК 27001-2006 «Системы менеджмента информационной безопасности».
9. Конфиденциальность, доступность, целостность информации как грани информационной безопасности.
10. Отношения, регулируемые законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации»
11. Классификация нормативно-правовых актов, регламентирующих сферу информационной безопасности.
12. Административный уровень информационной безопасности.
13. Характеристика стандарта ГОСТ Р ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий».
14. Основные этапы управления рисками.
15. Российские стандарты, регулирующие ИБ.
16. Доктрина информационной безопасности Российской Федерации.
17. Классификация криптосистем.
18. Основные функции подсистемы защиты операционной системы.
19. Режимы работы блочных шифров.
20. Обобщенная схема асимметричной криптосистемы. Алгоритм шифрования RSA.
21. Идентификация, аутентификация и авторизация субъекта доступа.
22. Российские стандарты шифрования.
23. Блочные и поточные шифры.
24. Распределение криптографических ключей.
25. Межсетевые экраны.
26. Концепция построения VPN.

27. Виды резервного копирования.

4.3 Оценочные средства для промежуточной аттестации

4.3.1 Формируемые компетенции

Таблица 5

Код этапа освоения компетенции	Результаты обучения
ОПК-3.2	- сформированы знания: современные методы и средства создания, хранения, обработки и передачи информации; в области защиты информации, хранящейся на рабочих станциях и серверах таможенных органов, подключенных к сети Интернет, а также при ее передаче по открытым каналам Интернет - сформированы умения: реализовывать способы защиты информации при работе в информационных системах; - сформированы навыки: использования компьютерной техники, программных средств и компьютерных сетей; освоения практических приемов защиты рабочих станций и серверов в таможенных органах
ПК - 17.1	- сформированы знания: об основных принципах формирования на основе научных подходов современных систем обеспечения информационной безопасности, месте и роли деятельности по выявлению, предотвращению и нейтрализации угроз экономической безопасности в данных системах; классификация угроз и составление модели нарушителя; - сформированы умения: анализировать уязвимости информационных систем, применяемых в профессиональной деятельности; - сформированы навыки: выявления на основе научных подходов потенциальных и реальных угроз экономической безопасности страны с использованием современных информационных технологий; защиты данных от внешних и внутренних угроз
ПК - 32.1	- сформированы знания: методов и приемов противодействия возможным угрозам в области состояния и сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере; применения информационных технологий в профессиональной деятельности; - сформированы умения: использовать организационные, программные и технические

	методы защиты информации; - сформированы навыки: применения информационных технологий и средств обеспечения их функционирования
ПК - 35.1	- сформированы знания: в области защиты информации, хранящейся на рабочих станциях и серверах таможенных органов, подключенных к сети Интернет, а также при ее передаче по открытым каналам Интернет; электронных средств обмена информацией; - сформированы умения: обеспечивать защиту каналов передачи данных; - сформированы навыки: освоения практических приемов защиты рабочих станций и серверов в таможенных органах; использования электронных средств обмена информацией с соблюдением требований информационной безопасности

4.3.2 Типовые оценочные средства

Вопросы к экзамену

1. Понятие и предмет информационной безопасности.
2. Основные процессы преобразования информации. Информационная деятельность в модели архитектуры предприятия.
3. Базовые свойства информации с точки зрения информационной безопасности.
4. Законодательный уровень информационной безопасности.
5. Классификация нормативно-правовых актов, регламентирующих сферу информационной безопасности.
6. Основы государственной политики Российской Федерации в сфере информационной безопасности.
7. Основные законодательные акты РФ, определяющие в целом юридические аспекты защиты информации.
8. Основные российские и международные стандарты в области информационной безопасности.
9. Конфиденциальность, доступность, целостность информации как грани информационной безопасности.
10. Отношения, регулируемые законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации»
11. Уровни информационной безопасности
12. Административный уровень информационной безопасности.
13. Характеристика стандарта ГОСТ Р ИСО/МЭК 15408-1-2012. Методы и средства обеспечения безопасности.

14. Характеристика стандарта ГОСТ Р ИСО/МЭК 27001-2006. Системы менеджмента информационной безопасности.
15. Базовые признаки классификации угроз в сфере информационной безопасности.
16. Основные подходы к управлению рисками.
17. Классификация компьютерных вирусов.
18. Классификация сетевых атак на информационные системы.
19. Элементы информационной инфраструктуры.
20. Модель взаимодействия открытых систем ИСО.
21. Состав и характеристики стека протоколов TCP/IP.
22. Модель локальной вычислительной сети организации.
23. Способы идентификации компьютера в локальной вычислительной сети.
24. Назначение и функции прокси-сервера.
25. Функции межсетевых экранов в компьютерных сетях.
26. Концепция построения виртуальных частных сетей VPN.
27. Классификация криптографических методов защиты информации.
28. Обобщенная схема симметричной криптосистемы.
29. Блочные и поточные режимы шифрования.
30. Обобщенная схема асимметричной криптосистемы. Алгоритм шифрования RSA.
31. Хеширование. Электронная цифровая подпись.
32. Основные функции подсистемы защиты операционной системы.
33. Особенности численных методов расчета с точки зрения информационной безопасности.
34. Этапы разработки и внедрения системы менеджмента информационной безопасности.
35. Политика информационной безопасности организации
36. Цели, методы и средства обеспечения информационной безопасности.
37. Общие принципы при управлении персоналом с точки зрения ИБ.
38. Основные принципы управления средствами информационно-коммуникационных технологий (ИКТ).
39. Идентификация, аутентификация и авторизация субъекта доступа.
40. Принципы управления доступом к информационной системе.
41. Методы контроля целостности данных.
42. Виды резервного копирования данных.
43. Мониторинг и аудит системы обеспечения информационной безопасности.

Промежуточная аттестация по дисциплине проводится в виде устного экзамена по билету, который состоит из двух теоретических вопросов.

Шкала оценивания экзамена: отлично, хорошо, удовлетворительно, неудовлетворительно.

Показатели, критерии и оценивание компетенций по этапам их формирования

Таблица 6

Наименование темы	Код компетенции	Критерии оценивания	Оценка
1. Теоретические основы информационной безопасности	ОПК-3, ПК-17	Студент владеет знаниями, умениями и навыками в рамках дисциплины в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину; самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивал при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи; четко формирует ответы, свободно читает результаты анализов и других исследований и решает ситуационные задачи повышенной сложности; хорошо знаком с основной литературой и методами исследования в объеме, необходимом для практической деятельности; увязывает теоретические аспекты предмета с практическими задачами; владеет знаниями основных принципов изучаемых наук.	Отлично
2. Система обеспечения информационной безопасности	ПК-17, ПК-32	Студент владеет знаниями, умениями и навыками в рамках дисциплины почти в полном объеме	Хорошо

3. Технологии защиты информации	ПК-32, ПК-35	программы (имеются пробелы знаний только в некоторых, особенно сложных разделах); самостоятельно и отчасти при наводящих вопросах дает полноценные ответы на вопросы; не всегда выделяет наиболее существенное, не допускает вместе с тем серьезных ошибок в ответах; умеет решать легкие и средней сложности ситуационные задачи; умеет трактовать лабораторные и инструментальные исследования в объеме, превышающем обязательный минимум.	
		Студент владеет основным объемом знаний, умений и навыков в рамках дисциплины; проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками; в процессе ответов допускаются ошибки по существу вопросов; способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом методов исследований.	Удовлетворительно
		Студент не освоил обязательного минимума знаний, умений и навыков в рамках дисциплины, не способен ответить на вопросы даже при дополнительных наводящих вопросах	Неудовлетворительно

4.4. Методические материалы

Изучение дисциплины завершается устным экзаменом в 4 семестре, который проводится по всему содержанию дисциплины. В самом начале учебного курса желательно ознакомиться со следующей учебно-методической документацией:

- программой дисциплины;
- перечнем знаний и умений, которыми студент должен владеть;
- тематическими планами лекций, практических занятий;

– контрольными мероприятиями;

– учебником, учебными пособиями по дисциплине, а также электронными ресурсами;

– перечнем примерных вопросов к экзамену.

Непосредственная подготовка к экзамену осуществляется по вопросам, представленным в данной рабочей программе. Необходимо тщательно изучить формулировку каждого вопроса, вникнуть в его суть, желательно составить план ответа. Обычно план включает в себя:

— показ теоретической и практической значимости рассматриваемого вопроса;

— обзор освещения вопроса в истории;

— определение сущности рассматриваемого предмета;

— основные элементы содержания и структуры предмета рассмотрения;

— факторы, логику и перспективы эволюции предмета;

— показ роли и значения рассматриваемого материала для практической деятельности.

План ответа желательно развернуть, приложив к нему ссылки на первоисточники с характерными цитатами. Необходимо отметить для себя пробелы в знаниях, которые следует ликвидировать в ходе подготовки, для чего возможно обратиться за консультацией к преподавателю.

В данном курсе изучаются вопросы обеспечения информационной безопасности в Российской Федерации и организации.

В связи с этим студенты должны хорошо понимать сущность системы обеспечения информационной безопасности, включающей в себя методы и средства обеспечения безопасности и систему менеджмента информационной безопасности.

Студенты должны хорошо представлять себе роль и место информационные безопасности в системе менеджмента качества и обеспечения непрерывности бизнес-процессов.

Обучение по дисциплине «Информационная безопасность в таможенном деле» предполагает изучение курса на аудиторных занятиях (лекционные, практические и лабораторные занятия), а также самостоятельной работы студентов. При изучении дисциплины «Информационная безопасность в таможенном деле» рекомендуется пользоваться контрольными вопросами к каждой теме, программой курса, рекомендуемой основной и дополнительной литературой.

К каждой теме занятий студентам необходимо готовиться заранее. Существенным аспектом изучения курса является знакомство с компьютерными и информационными системами, в том числе на лабораторных и практических занятиях. Основным нормативно-правовым документом при изучении курса «Информационная безопасность в таможенном деле» является Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.12.2016) "Об информации,

информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2017).

В процессе подготовки к практическим занятиям студентам предлагается выполнить следующие домашние задания:

- ознакомиться с вопросами к теме, рассматриваемой на лекции и практическом занятии.
- выполнить тестовые задания по теме.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Обучение по дисциплине «Информационная безопасность в таможенном деле» предполагает изучение курса на аудиторных занятиях (лекции, практические занятия, лабораторные работы) и самостоятельной работы студентов.

Практические занятия дисциплины «Информационная безопасность в таможенном деле» предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций с проведением контрольных мероприятий.

С целью обеспечения успешного обучения студент должен готовиться к лекции, она является важнейшей формой организации учебного процесса, поскольку:

– знакомит с новым учебным материалом;
– разъясняет учебные элементы, трудные для понимания;
– систематизирует учебный материал;
– ориентирует в учебном процессе.

Подготовка к лекции заключается в следующем:

– внимательно прочитайте материал предыдущей лекции;
– узнайте тему предстоящей лекции (по тематическому плану, по информации лектора);
– ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
– постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке;
– запишите возможные вопросы, которые вы зададите лектору на лекции.

Подготовка к практическим и лабораторным занятиям:

– внимательно прочитайте материал лекций относящихся к данному семинарскому занятию, ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
– выпишите основные термины;
– ответьте на контрольные вопросы по семинарским занятиям, готовьтесь дать развернутый ответ на каждый из вопросов;

– уясните, какие учебные элементы остались для вас неясными и постарайтесь получить на них ответ заранее (до семинарского занятия) во время текущих консультаций преподавателя;

– готовиться можно индивидуально, парами или в составе малой группы, последние являются эффективными формами работы;

– рабочая программа дисциплины в части целей, перечню знаний, умений, терминов и учебных вопросов может быть использована вами в качестве ориентира в организации обучения.

Подготовка к экзамену. К экзамену необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить дисциплину в период зачётно-экзаменационной сессии, как правило, показывают не слишком удовлетворительные результаты. В самом начале учебного курса познакомьтесь со следующей учебно-методической документацией:

– программой дисциплины;

– перечнем знаний и умений, которыми студент должен владеть;

– тематическими планами лекций, семинарских занятий;

– контрольными мероприятиями;

– учебником, учебными пособиями по дисциплине, а также электронными ресурсами;

– перечнем вопросов к экзамену.

После этого у студента должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине.

Систематическое выполнение учебной работы на лекциях и практических занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи экзамена.

6. УЧЕБНАЯ ЛИТЕРАТУРА И РЕСУРСЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

6.1. Основная литература

Основная литература

Таблица 7

Данные об издании					Печатная форма (кол-во в библиотеке)	Ссылка на ЭБС
№ п/п	Автор	Название	Издательство	Год издания		
1	Малюк А.А. Горбатов В.С. Королев В.И.	Введение в информационную безопасность	Горячая линия-Телеком	2012		http://e.lanbook.com/books/element.php?pl1_id=5171

2	Титов А.А.	Технические средства защиты информации	ТУСУР (Томский государственный университет систем управления и радиоэлектроники)	2010		http://e.lanbook.com/books/element.php?pl1_id=4960
3	Шаньгин В.Ф.	Защита информации в компьютерных системах и сетях	ДМК Пресс	2012		http://e.lanbook.com/books/element.php?pl1_id=3032
4	Афонин П.Н.	Информационная безопасность в таможенном деле	СПб.: Троицкий мост	2016		http://www.iprbookshop.ru/40859.html
5	В.Ю. Рогозин [и др.].—	Основы информационной безопасности	М.: ЮНИТИ-ДАНА	2017		http://www.iprbookshop.ru/72444.html.

6.2. Дополнительная литература

Дополнительная литература

Таблица 8

Данные об издании					Печатная форма (кол-во в библиотеке)	Ссылка на ЭБС
№ п/п	Автор	Название	Издательство	Год издания		
1	Мельников В.П., Клейменов С.А.	Информационная безопасность и защита информации	Академия	2010	3	
2	Аверченков В.И.	Аудит информационной безопасности	ФЛИНТА	2011		http://e.lanbook.com/books/element.php?pl1_id=44799
3	Коваленко Ю.И.	Правовой режим лицензирования и сертификации в сфере информационной безопасности	Горячая линия-Телеком	2012		http://e.lanbook.com/books/element.php?pl1_id=5163
4	Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Основы управления информационной безопасностью	Горячая линия-Телеком	2012		http://e.lanbook.com/books/element.php?pl1_id=5178

6.3. Учебно-методическое обеспечение самостоятельной работы

1. Николаев В.В. Основы информационной безопасности: Учебно-методическое пособие. – Орел: Изд-во СИУ РАНХиГС, 2017.

6.4. Нормативные правовые документы

1. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.12.2016) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2017). URL: http://consultant.ru.

2. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных". URL: http://consultant.ru.

3. Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" / Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru/.

4. Таможенный кодекс Таможенного союза (ред. от 08.05.2015) (приложение к Договору о Таможенном кодексе Таможенного союза, принятому Решением Межгосударственного Совета ЕврАзЭС на уровне глав государств от 27.11.2009 №17) // СЗ РФ. - 13.12.2015. - №50.

6.5. Интернет-ресурсы

1. Официальный портал ОФ РАНХиГС. URL: orel.ranepa.ru.

2. Корпоративный облачный сервис «Битрикс24». URL: www.bitrix24.ru.

3. Облачный сервис для совместной работы над документами “GoogleDocs”. URL: www.docs.google.com/?hl=ru.

4. Облачный сервис для совместной работы над документами “MSOneDrive”. URL: https://onedrive.live.com.

6.6. Иные источники

1. Барбышева Г. И., Мирзаев Ш.Ф. Обеспечение информационной безопасности таможенных органов РФ // Инновационная экономика: материалы II Междунар. науч. конф. (г. Казань, октябрь 2015 г.). — Казань: Бук, 2015. — С. 22-24.

2. Ермилов И.С., Игнатьева Г.В. Передовые информационные технологии в таможенном деле // Информационная безопасность регионов. - 2016. - № 1(22). - С.31-35.

3. Корняков, К.А. Новые технологии как средство модернизации таможенного контроля : монография / Ю.Н. Егоров, А.Н. Яцушко, К.А. Корняков .— М. : Изд-во Российской таможенной академии, 2014 .— 161 с.

4. Николаев В.В. Информационная система мониторинга защищенности образовательных учреждений // Наука вчера, сегодня, завтра: Сб. статей по материалам XXXVI Междунар. науч.-практ. конф. №7(29).- Новосибирск: Изд. АНС «СибАК», 2016.- С. 13-19.

5. Полянин А.В., Николаев В.В. О некоторых вопросах интеграции гетерогенных информационных систем на предприятии // Современные тен-

денции развития менеджмента и государственного управления. Материалы заочной всерос. научно - практ. конф.- Орел: Изд-во Среднерусского института управления – филиала РАНХиГС, 2017.- С.317-319.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

Материально-техническая база

Таблица 9

Вид помещения	Оборудование
Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мульмедийный проектор Доска Экран
Учебные аудитории для проведения практических и лабораторных занятий	Комплекты ученической мебели Мульмедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СИУ РАНХиГС
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мульмедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СИУ РАНХиГС
Помещения для самостоятельной работы	Комплекты ученической мебели Мульмедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СИУ РАНХиГС
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования.

Перечень программного обеспечения, необходимого для реализации дисциплины «Информационная безопасность в таможенном деле»

Таблица 10

Наименование программного обеспечения	Назначение и тип лицензии программного обеспечения
Microsoft Office	Интегрированный пакет прикладных программ. Лицензионная версия
NetBeans	Интегрированная среда разработки программ. Свободная лицензия
JDK	Комплект разработчика приложений на языке Java Свободная лицензия
ИПС «Гарант» URL: http://www.garant.ru/	Информационно-поисковая система, позволяющая работать с нормативно-правовыми актами, учебной и научной литературой. Бесплатная онлайн-версия
WinRAR	Архиватор файлов. Свободная лицензия
Google Chrome Mozilla FireFox Opera Yandex	Браузеры. Свободная лицензия
Rambler	Поисковая система. Лицензионная версия
Яндекс	Поисковая система. Лицензионная версия
Лань URL: e.lanbook.com	Электронная библиотечная система. Лицензионная версия
Юрайт URL: biblio-online.ru	Электронная библиотечная система. Лицензионная версия
IPR URL: iprbookshop.ru	Электронная библиотечная система. Лицензионная версия
URL: orel-ranepa.ru	Электронная информационная образовательная среда на платформе Moodle Лицензионная версия