Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.Б.32 Информационная безопасность внешнеэкономической и таможенной деятельности

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

38.05.02 Таможенное дело

Направленность (профиль)

38.05.02.06 Таможенный контроль и экспертиза в таможенном деле

Форма обучения очная

Год набора 2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили

Старший преподаватель, Романов Р.В.

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Формирование у обучающихся знаний, которые позволят уяснить теоретико-методологические основы обеспечения информационной безопасности внешнеэкономической и таможенной деятельности, концептуальные и стратегические направления информационной безопасности внешнеэкономической и таможенной деятельности.

1.2 Задачи изучения дисциплины

По итогам изучения спецкурса студенты должны:

• освоение фундаментальных понятий в области информационной безопасности и защиты информации;

• овладение базовыми знаниями и навыками, позволяющими использовать информационные таможенные технологии в условиях угроз информационной безопасности.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине
ОПК-1: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
ОПК-1: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знать: основные требования информационной безопасности уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры владеть: культурой применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности
ОПК-3: способностью владеть методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей	

ОПК-3: способностью владеть методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники,	знать: принципы обеспечения информационной безопасности;нормативные и руководящие документы управления информационной безопасностью уметь:
программно-информационных систем, компьютерных сетей	классифицировать угрозы безопасности;использовать специальную литературу и другую научно-техническую информацию для аудита информационной безопасности владеть: навыками организации доступа сресурсам сети
ПК-17: умением выявлять и анализировать угрозы экономической безопасности страны при осуществлении профессиональной деятельности	
ПК-17: умением выявлять и анализировать угрозы экономической безопасности страны при осуществлении профессиональной деятельности	знать: основные направления информационной безопасности уметь: выявлять информационные атаки владеть: способами локализации и предотвращения информационных угроз.

1.4 Особенности реализации дисциплины

Язык реализации дисциплины: Русский.

Дисциплина (модуль) реализуется без применения ЭО и ДОТ.

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	е 1
Контактная работа с преподавателем:	**1,5 (54)**	
занятия лекционного типа	0,5 (18)	
практические занятия	1 (36)	
Самостоятельная работа обучающихся:	**1,5 (54)**	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Нет	

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Контактная работа, ак. час.							
		Занятия лекционного типа		Занятия семинарского типа				Самостоятельная работа, ак. час.	
				Семинары и/или Практические занятия		Лабораторные работы и/или Практикумы			
		Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС
1. 1. Основные понятия и определения в сфере информационной безопасности.									
	1. Политика информационной безопасности	4							
	2. Стратегия развития информатизации и задачи государственного управления безопасности			8					
	3. Политика информационной безопасности							12	
2. Нормативно правовая база обеспечения информационной безопасности									
	1. Нормативно правовая база обеспечения информационной безопасности	4							
	2. Применение правовой базы обеспечения информационной безопасности			8					
	3. Применение терминов при решении практических задач обеспечения информационной безопасности							12	
3. Угрозы информационной безопасности									
	1. Угрозы информационной безопасности и их виды	4							

2. Распознавание угроз информационной безопасности			8					
3. Информационная безопасность экономических систем и локализация угроз							10	
4. Организационно-технические и режимные меры и методы								
1. Организационно-технические и режимные меры и методы	4							
2. Организационно-технические и режимные меры и методы			6					
3. Организационно-технические и режимные меры и методы							10	
5. Программно-технические способы и средства обеспечения информационной безопасности								
1. Программно-технические способы и средства обеспечения информационной безопасности	2							
2. Аппаратно-программные средства защиты информационной безопасности			6					
3. Криптографические средства защиты информации							10	
4.								
Всего	18		36				54	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Громов Ю. Ю., Драчев В. О., Иванова О. Г., Шахов Н. Г. Основы информационной безопасности: учебное пособие для студентов вузов по направлению "Информационные системы и технологии"(Старый Оскол: ТНТ).
2. Литвинов П.С. Организационное правовое обеспечение информационной безопасности: [учеб-метод. материалы к изучению дисциплины для ...10.03.01.01 Безопасность компьютерных систем] (Красноярск: СФУ).
3. Шаньгин В. Ф. Информационная безопасность и защита информации (Москва: ДМК-Пресс).

4.2 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства (программное обеспечение, на которое университет имеет лицензию, а также свободно распространяемое программное обеспечение):

1. Программное обеспечение для проведения тестирования, MicrosoftOffice, электронная почта, интернет-браузер.

4.3 Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:

1. Научная библиотека Сибирского федерального университета: Режим доступа: http://lib.sfu-kras.ru/.
2. Информационно-справочная система «КонсультантПлюс»: Режим доступа: https://www.consultant.ru/online/
3. Информационно-справочная система «Кодекс»: Режим доступа: http://www.kodeks.ru/
4. Информационно-справочная система "Гарант": Режим доступа: http://www.garant.ru/

5 Фонд оценочных средств

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническая база, соответствует действующим противопожарным правилам и нормам, и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической работы обучающихся, предусмотренной учебным планом.

В процессе преподавания дисциплины используются:

библиотечныйфонд ТЭИ СФУ;

мультимедийное оборудование для чтения лекций-презентаций.