



УТВЕРЖДЕНО

решением Ученого совета ИЭиБ

от «22» июня 2023 г., протокол № 9/261

Председатель

И.Б. Романова

«22» июня 2023 г..

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Информационная безопасность
Факультет	Управления
Кафедра	Таможенного дела и правового обеспечения внешнеэкономической деятельности
Курс	4

Направление (специальность) **38.05.02 Таможенное дело**
код направления (специальности), полное наименование

Направленность (профиль/специализация) **Таможенные платежи**

Форма обучения: очная, заочная

Дата введения в учебный процесс УЛГУ: «01» сентября 2023 г.

Программа актуализирована на заседании кафедры: протокол № _____ от _____ 20 ____ г.

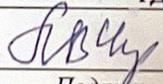
Программа актуализирована на заседании кафедры: протокол № _____ от _____ 20 ____ г.

Программа актуализирована на заседании кафедры: протокол № _____ от _____ 20 ____ г.

Программа актуализирована на заседании кафедры: протокол № _____ от _____ 20 ____ г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Сандальникова Е.В.	ТД и ПО ВЭД	Доцент, к.ю.н.

СОГЛАСОВАНО	
Заведующий выпускающей кафедрой ГД и ПО ВЭД	
	Чувашлова М.В./
Подпись	ФИО
«22» июня 2023 г.	

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

Цели освоения дисциплины:

- формирование у обучающихся комплекса знаний, умений и навыков в сфере правового регулирования и реализации информационной безопасности.

Задачи освоения дисциплины:

- овладение обучаемыми системой научных знаний и практических навыков в сфере правового регулирования общественных отношений, которые возникают в связи с обеспечением и реализацией информационной безопасности;

- развитие умения мыслить (овладевать такими мыслительными операциями, как классификация, анализ, синтез, сравнение и др.), развитие творческих и познавательных способностей, а также таких психологических качеств, как восприятие, воображение, память, внимание с применением знаний об информационной безопасности как объекте регулирования;

- формирование у будущих специалистов комплексных знаний о правовом регулировании различных форм, средств, методов обеспечения и реализации информационной безопасности;

- приобретение студентами навыков и умений по решению ситуационных задач, связанных с регулированием информационной безопасности, на практических занятиях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП:

Дисциплина «Информационная безопасность» входит в часть дисциплин учебного плана, являющихся факультативными дисциплинами, и имеет код ФТД.02. Предшествующими дисциплинами для изучения данной дисциплины выступают «Информационные таможенные технологии», «Информационная безопасность».

В дальнейшем является основой для изучения дисциплин «Практикум по таможенному декларированию», «Ознакомительная практика», «Преддипломная практика», «Практика по получению профессиональных умений и опыта профессиональной деятельности», «Проектная деятельность», «Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты», «Подготовка к сдаче и сдача государственного экзамена».

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1. Код и наименование реализуемой компетенции	2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ПК-8 - Способен применять информационные технологии, электронные способы обмена информацией с учетом требований информационной безопасности в целях информационного сопровождения профессиональной деятельности	ИД-1. Знать организационные и технические меры, связанные с разработкой, внедрением и применением информационно-технических средств в деятельности таможенных органов; ИД-2. Уметь анализировать состояние, перспективные направления развития информационных технологий и систем в таможенном деле ИД-3. Уметь анализировать бизнес-процессы и обрабатывать экономическую и управленческую информацию с использованием программных средств; ИД-4. Владеть навыками организации экономической и управленческой деятельности с учетом требований информационной безопасности в целях информационного сопровождения профессиональной деятельности в обла-

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

	сти таможенного дела.
--	-----------------------

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 2

4.2. Объем дисциплины по видам учебной работы (в часах)

Вид учебной работы	Количество часов (форма обучения - очная)	
	Всего по плану	в т.ч. по се- местрам
		7
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	36/36*	36/36*
Аудиторные занятия:	36/36*	36/36*
лекции	0/0*	0/0*
практические занятия	36/36*	36/36*
лабораторные работы, практикумы	-	-
Самостоятельная работа	36	36
Форма текущего контроля знаний и контроля самостоятельной работы	Устный опрос, проверка реферата, решение тестов	Устный опрос, проверка реферата, решение тестов
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	Зачет	Зачет
Всего часов по дисциплине	72	72

* В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, в таблице через слэш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

Вид учебной работы	Количество часов (форма обучения - заочная)	
	Всего по плану	в т.ч. по се- местрам
		4
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	8/8*	8/8*
Аудиторные занятия:	8/8*	8/8*
лекции	0/0*	0/0*
семинары и практические занятия	8/8*	8/8*
лабораторные работы, практикумы		
Самостоятельная работа	60	60
Форма текущего контроля знаний и контроля самостоятельной работы:	Устный опрос, проверка реферата, решение тестов	Устный опрос, проверка реферата, решение тестов
Курсовая работа	-	-
Виды промежуточной аттестации	4/4* Зачет	4/4* Зачет

Форма

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

Всего часов по дисциплине	72	72
---------------------------	----	----

* В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

4.3. Содержание дисциплины (модуля.) Распределение часов по темам и видам учебной работы:

Форма обучения очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний	
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа		
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы				
1	2	3	4	5	6	7		
1. Введение информационную безопасность	6		3				3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
2. Правовое обеспечение информационной безопасности	6		3				3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
3. Организационное обеспечение информационной безопасности	6		3				3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
4. Технические средства и методы защиты информации	6		3				3	Устный опрос, проверка реферата, решение тестов,

Форма

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

							консультирование, самоконтроль
5. Программно-аппаратные средства и методы обеспечения информационной безопасности	6		3			3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
6. Криптографические методы защиты информации	6		3			3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
7. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	6		3			3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
8. Использование криптографических средств защиты информации	6		3			3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
9. Реализация работы инфраструктуры открытых ключей	6		3			3	Устный опрос, проверка реферата, решение тестов, консультирование,

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

							самоконтроль
10. Средства стеганографии для защиты информации	6		3			3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
11. Настройка безопасного сетевого соединения	6		3			3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
12. Антивирусные средства защиты информации	6		3			3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
Зачет							
Итого	72		36			36	

Форма обучения заочная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	
Раздел 1. Общая часть							
1. Введение информационную безопасность	8	-	1			5	Устный опрос, проверка реферата, решение тестов, консультирование,

Форма

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

							самоконт роль
2. Правовое обеспечение информационной безопасности	8	1	-			5	Проверка реферата, решение тестов, консультирование, самоконт роль
3. Организационное обеспечение информационной безопасности	9	1	1			5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконт роль
4. Технические средства и методы защиты информации	8	-	1			5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконт роль
5. Программно-аппаратные средства и методы обеспечения информационной безопасности	9	1	-			5	Проверка реферата, решение тестов, консультирование, самоконт роль

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

6. Криптографические методы защиты информации	9	-	1			5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
7. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	9	1	-			5	Проверка реферата, решение тестов, консультирование, самоконтроль
8. Использование криптографических средств защиты информации	9	-	1			5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
9. Реализация работы инфраструктуры открытых ключей	9	-	1			5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
10. Средства стеганографии для защиты информации	9	-	1			5	Устный опрос, проверка реферата, решение тестов, консультирование,

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

							самоконт роль
11. Настройка безопасного сетевого соединения	8	-	-			5	Проверка реферата, решение тестов, консульты рование, самоконт роль
12. Антивирусные средства защиты информации	9	-	1			5	Устный опрос, проверка реферата, решение тестов, консульты рование, самоконт роль
Зачет							4
Итого	72		8			60	4

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Тема 1: Введение в информационную безопасность.

- В-1. Понятия и составляющие информационной безопасности
- В-2. Классификация угроз.
- В-3. Примеры угроз.

Тема 2: Правовое обеспечение информационной безопасности.

- В-1. Понятие информационной безопасности и ее содержание
- В-2. Характеристика угроз информационной безопасности
- В-3. Общий обзор нормативных правовых актов защиты информации
- В-4. Доктрина информационной безопасности Российской Федерации, как основной документ в сфере обеспечения информационной безопасности

Тема 3. Организационное обеспечение информационной безопасности.

- В-1. Основные группы функций системы обеспечения информационной безопасности.
- В-2. Система обеспечения информационной безопасности РФ и ее составляющие
- В-3. Задачи, на которые нацелено стратегическое планирование

Тема 4. Технические средства и методы защиты информации.

- В-1. Методы и средства организационно-правовой защиты информации
- В-2. Методы и средства инженерно-технической защиты
- В-3. Криптографические методы защиты и шифрование

Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

- В-1. Средства архивации информации
- В-2. Антивирусные программы.
- В-3. Идентификация и аутентификация пользователя.
- В-4. Защита информации в КС от несанкционированного доступа
- В-5. Другие программные средства защиты информации

Тема 6. Криптографические методы защиты информации.

- В-1. Классификация криптографических методов защиты информации
- В-2. Симметричное шифрование.
- В-3. Сертификаты открытых ключей.

Тема 7. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.

- В-1. Специфика информационных технологий, используемых в правовой сфере.
- В-2. Информационная безопасность на предприятии.
- В-3. Средства обеспечения информационной безопасности в Интернет.

Тема 8. Использование криптографических средств защиты информации.

- В-1. Общие положения
- В-2. Порядок применения СКЗИ
- В-3. Порядок управления ключевой системой
- В-4. Мониторинг и контроль применения СКЗИ

Тема 9. Реализация работы инфраструктуры открытых ключей.

- В-1. Компоненты инфраструктуры открытых ключей
- В-2. Принципы работы PKI

Тема 10. Средства стеганографии для защиты информации.

- В-1. Классическая стеганография
- В-2. Компьютерная стеганография
- В-3. Использование протоколов в NTFS
- В-4. Цифровая стеганография

Тема 11. Настройка безопасного сетевого соединения.

- В-1. Беспроводные сети.
- В-2. Современные беспроводные технологии.
- В-3. Вопросы безопасности беспроводных соединений.

Тема 12. Антивирусные средства защиты информации.

- В-1. Сканирование
- В-2. Эвристический анализ

ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Тема 1. Введение в информационную безопасность. (форма проведения – практическое занятие)

- Вопросы по темам раздела (для обсуждения на занятии и для самостоятельного изучения)
- В-1. Понятия и составляющие информационной безопасности
 - В-2. Классификация угроз.

Форма

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

В-3. Примеры угроз.

Тема 2. Правовое обеспечение информационной безопасности. (форма проведения – практическое занятие)

Вопросы по темам раздела (для обсуждения на занятии и для самостоятельного изучения)

- В-1. Понятие информационной безопасности и ее содержание
- В-2. Характеристика угроз информационной безопасности
- В-3. Общий обзор нормативных правовых актов защиты информации
- В-4. Доктрина информационной безопасности Российской Федерации, как основной документ в сфере обеспечения информационной безопасности

Тема 3. Организационное обеспечение информационной безопасности. (форма проведения – практическое занятие)

Вопросы по темам раздела (для обсуждения на занятии и для самостоятельного изучения)

- В-1. Основные группы функций системы обеспечения информационной безопасности.
- В-2. Система обеспечения информационной безопасности РФ и ее составляющие
- В-3. Задачи, на которые нацелено стратегическое планирование

Тема 4. Технические средства и методы защиты информации. (форма проведения – практическое занятие)

Вопросы по темам раздела (для обсуждения на занятии и для самостоятельного изучения)

- В-1. Методы и средства организационно-правовой защиты информации
- В-2. Методы и средства инженерно-технической защиты
- В-3. Криптографические методы защиты и шифрование

Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности. (форма проведения – практическое занятие)

Вопросы по темам раздела (для обсуждения на занятии и для самостоятельного изучения)

- В-1. Средства архивации информации
- В-2. Антивирусные программы.
- В-3. Идентификация и аутентификация пользователя.
- В-4. Защита информации в КС от несанкционированного доступа
- В-5. Другие программные средства защиты информации.

Тема 6. Криптографические методы защиты информации. (форма проведения – практическое занятие)

Вопросы по темам раздела (для обсуждения на занятии и для самостоятельного изучения)

- В-1. Классификация криптографических методов защиты информации
- В-2. Симметричное шифрование.
- В-3. Сертификаты открытых ключей.

Тема 7. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности. (форма проведения – практическое занятие)

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

Вопросы по темам раздела (для обсуждения на занятии и для самостоятельного изучения)

В-1. Специфика информационных технологий, используемых в правовой сфере.

В-2. Информационная безопасность на предприятии.

В-3. Средства обеспечения информационной безопасности в Интернет.

Тема 8. Использование криптографических средств защиты информации. (форма проведения – практическое занятие)

Вопросы по темам раздела (для обсуждения на занятии и для самостоятельного изучения)

В-1. Общие положения

В-2. Порядок применения СКЗИ

В-3. Порядок управления ключевой системой

В-4. Мониторинг и контроль применения СКЗИ

Тема 9. Реализация работы инфраструктуры открытых ключей. (форма проведения – практическое занятие)

Вопросы по темам раздела (для обсуждения на занятии и для самостоятельного изучения)

В-1. Компоненты инфраструктуры открытых ключей

В-2. Принципы работы PKI

Тема 10. Средства стеганографии для защиты информации. (форма проведения – практическое занятие)

Вопросы по темам раздела (для обсуждения на занятии и для самостоятельного изучения)

В-1. Классическая стеганография

В-2. Компьютерная стеганография

В-3. Использование протоколов в NTFS

В-4. Цифровая стеганография

Тема 11. Настройка безопасного сетевого соединения. (форма проведения – практическое занятие)

Вопросы по темам раздела (для обсуждения на занятии и для самостоятельного изучения)

В-1. Беспроводные сети.

В-2. Современные беспроводные технологии.

В-3. Вопросы безопасности беспроводных соединений.

Тема 12. Антивирусные средства защиты информации. (форма проведения – практическое занятие)

Вопросы по темам раздела (для обсуждения на занятии и для самостоятельного изучения)

В-1. Сканирование

В-2. Эвристический анализ

5. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

- не предусмотрены учебным планом.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

6. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

По данной дисциплине предусматривается написание рефератов. Курсовые работы по данной дисциплине УП по специальности «Таможенное дело» не предусмотрены.

Примерная тематика рефератов

1. Понятие информационной безопасности и защиты информации.
2. Государственная система защиты информации в России.
3. Классификация тайн по характеру относимых к ним сведений.
4. Классификация компьютерных преступлений.
5. Базовые свойства информации, подлежащие защите.
6. Основные уровни обеспечения информационной безопасности.
7. Классификация угроз информационной безопасности.
8. Концептуальные нормативно-правовые акты в области защиты информации.
9. Понятие политики информационной безопасности и основные этапы её разработки.
10. Базовые виды политики информационной безопасности и их краткое описание.
11. Основные угрозы компьютерным системам.
12. Методики оценки рисков для информационных систем.
13. Стандарты в области разработки политики информационной безопасности и анализа рисков.
14. Инструментальные средства для анализа рисков и управления ими.
15. Основные сервисы программных средств защиты информации в информационных системах.
16. Базовые группы методов аутентификации.
17. Основные рекомендации по формированию паролей.
18. Биометрические системы идентификации пользователей.
19. Основные виды управления доступом к информации.
20. Классификация компьютерных вирусов.
21. Симметричные и ассиметричные криптосистемы.
22. Основные методы шифрования данных.
23. Базовые криптографические стандарты.
24. Сервисы безопасности для реализации защитных функций в сети.

Требования к содержанию, объему и оформлению работ.

Содержание реферата должно включать

- введение, в котором определяются цели, задачи исследования;
- основную часть, в которой важно отразить нормативную основу исследования, раскрыть вопросы, соответствующие задачам исследования;
- заключение, в котором необходимо подвести итоги исследования, сделать вывод о достижении поставленной цели и задач;
- список использованных источников.

Объем работы должен составлять 10-12 страниц (шрифт Times New Roman, 14, интервал 1,5).

7. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа.
Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.
20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.

8. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Форма обучения – очная

Название разделов и тем	Вид самостоятельной работы (проработка учебного материала, решение задач, реферат, доклад, контрольная работа, подготовка к сдаче зачета, экзамена и др.)	Объем в часах	Форма контроля (проверка решения задач, реферата и др.)
1. Введение информационную безопасность	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
2. Правовое обеспечение информационной безопасности	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	3	Устный опрос, проверка реферата, решение тестов,

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

			консультирование, самоконтроль
3. Организационное обеспечение информационной безопасности	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
4. Технические средства и методы защиты информации	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
5. Программно-аппаратные средства и методы обеспечения информационной безопасности	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
6. Криптографические методы защиты информации	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
7. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
8. Использование криптографических средств защиты информации	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
9. Реализация работы инфраструктуры открытых ключей	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
10. Средства стеганографии для защиты информации	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	3	Устный опрос, проверка реферата, решение тестов,

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

			консультирование, самоконтроль
11. Настройка безопасносетевого соединения	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
12. Антивирусные средствазащиты информации	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	3	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль

Форма обучения - заочная

Название разделов и тем	Вид самостоятельной работы (проработка учебного материала, решение задач, реферат, доклад, контрольная работа, подготовка к сдаче зачета, экзамена и др.)	Объем в часах	Форма контроля (проверка решения задач, реферата и др.)
1. Введение информационную безопасность	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
2. Правовое обеспечение информационной безопасности	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	5	Проверка реферата, решение тестов, консультирование, самоконтроль
3. Организационное обеспечение информационной безопасности	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
4. Технические средства иметоды защиты информации	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
5. Программно-аппаратные средства и методы	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	5	Проверка реферата, решение тестов,

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

обеспечения информационной безопасности			консультирование, самоконтроль
6. Криптографические методы защиты информации	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
7. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	5	Проверка реферата, решение тестов, консультирование, самоконтроль
8. Использование криптографических средств защиты информации	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
9. Реализация работы инфраструктуры открытых ключей	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
10. Средства стеганографии для защиты информации	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль
11. Настройка безопасного сетевого соединения	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	5	Проверка реферата, решение тестов, консультирование, самоконтроль
12. Антивирусные средства защиты информации	Проработка учебного материала, реферат, тестирование, подготовка к сдаче зачета	5	Устный опрос, проверка реферата, решение тестов, консультирование, самоконтроль

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

Основная

1. Корабельников Сергей Маркович. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. - Москва : Юрайт, 2023. - 111 с. - (Высшее образование). - URL: <https://urait.ru/bcode/519079>
2. Жарова Анна Константиновна. Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации : монография / А. К. Жарова. - Москва : Юрайт, 2023. - 301 с. - (Актуальные монографии). - URL: <https://urait.ru/bcode/519998>

Дополнительная:

1. Агамагомедова, С. А. Таможенный контроль товаров, содержащих объекты интеллектуальной собственности : монография / С.А. Агамагомедова. — Москва : ИНФРА-М, 2023. - 160 с. — (Научная мысль). — DOI 10.12737/5619. - ISBN 978-5-16-010146-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1894020>
2. Жиленкова, Т. В. Право интеллектуальной собственности : практикум / Т. В. Жиленкова. - Москва : РГУП, 2023. - 172 с. - ISBN 978-5-500209-026-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2069316>
3. Бирюков Павел Николаевич. **Право интеллектуальной собственности** : учебник и практикум для вузов / П. Н. Бирюков. - 3-е изд. ; пер. и доп. - Москва : Юрайт, 2023. - 315 с. - (Высшее образование). - URL: <https://urait.ru/bcode/511201>

Учебно-методическая:

1. Сандальникова Е. В. Методические указания по организации самостоятельной работы обучающихся студентов по дисциплине «Информационная безопасность» для специальности 38.05.02 «Таможенное дело» всех форм обучения / Ульян. гос. ун-т, ИЭиБ. - 2022. - 36 с. - Неопубликованный ресурс. - URL: <http://lib.ulsu.ru/MegaPro/Download/MObject/14100>. - Режим доступа: ЭБС УлГУ. - Текст : электронный.

Согласовано:

Главный библиотекарь / Должность сотрудника научной библиотеки _____ / Голосова М.Н. / МН / 2023 г.
ФИО _____ подпись _____

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2023]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство «ЮРАЙТ». – Москва, [2023]. - URL: <https://urait.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО «Политехресурс». – Москва, [2023]. – URL: <https://www.studentlibrary.ru/cgi-bin/mb4x>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС «Лань». – Санкт-Петербург, [2023]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - URL: <http://znanium.com> . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. / ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: <https://id2.action-media.ru/Personal/Products>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: <http://www.edu.ru>. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Mega-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

СОГЛАСОВАНО:

Шинкев Вадим
Должность сотрудника УИТИТ

Щуренко ЮВ
ФИО

Иванов
подпись

01.06.2023
дата

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций и семинарских занятий, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций.

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для предоставления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе.

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

– в случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик



подпись

доцент

должность

Е.В. Сандальникова

ФИО