АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИНСТИТУТ МЕЖДУНАРОДНЫХ ЭКОНОМИЧЕСКИХ СВЯЗЕЙ»
INSTITUTE OF INTERNATIONAL ECONOMIC RELATIONS

Принята на заседании
Учёного совета ИМЭС
(протокол от 27 марта 2025 г. № 8)

УТВЕРЖДАЮ
Ректор ИМЭС Ю.И. Богомолова
27 марта 2025 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0264F3EC0000B36E8C480AA1B8325C8407
Владелец: АНО ВО "ИНСТИТУТ МЕЖДУНАРОДНЫХ ЭКОНОМИЧЕСКИХ СВЯЗЕЙ", ИНСТИТУТ МЕЖДУНАРОДНЫХ ЭКОНОМИЧЕСКИХ СВЯЗЕЙ, ИМЭС
Действителен: с 18.06.2025 до 18.09.2026

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

по специальности
38.05.02 Таможенное дело

Направленность (профиль)
«Таможенное регулирование и логистика»

Москва – 2025

Приложение 4
к основной профессиональной образовательной программе
по специальности 38.05.02 Таможенное дело,
направленность (профиль) «Таможенное регулирование и логистика»

Рабочая программа дисциплины «Информационная безопасность и защита информации» входит в состав основной профессиональной образовательной программы высшего образования по специальности 38.05.02 Таможенное дело, направленность (профиль) «Таможенное регулирование и логистика» и предназначена для обучающихся очной и очно-заочной форм обучения.

СОДЕРЖАНИЕ

1. Цель и задачи дисциплины

Целью дисциплины «Информационная безопасность и защита информации» является получение теоретических знаний и практических навыков, необходимых для понимания основ и принципов защиты информации, применения способов защиты информации на практике, включая защиту компьютерных систем, защиту информации в сети Интернет и корпоративных сетях.

Задачи изучения дисциплины:

- приобретение понимания основных принципов организации защиты информации;
- приобретение понимания современных технологий защиты информации;
- изучение основных процедур и инструментов, используемых для обеспечения информационной безопасности на практике.

2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования

Дисциплина «Информационная безопасность и защита информации» входит в обязательную часть учебного плана по специальности 38.05.02 Таможенное дело, направленность (профиль) «Таможенное регулирование и логистика».

3. Объем дисциплины в зачетных единицах и академических часах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость дисциплины составляет 3 зачётные единицы, всего – 108 часов.

Вид учебной работы	**Всего часов**	
	очная форма обучения	очно-заочная форма обучения
Контактная работа с преподавателем (всего)	**28**	**8**
В том числе:		
Занятия лекционного типа	14	6
Занятия семинарского типа (семинары)	14	2
Самостоятельная работа (всего)	**80**	**100**
Форма контроля	Зачет с оценкой	
Общая трудоёмкость дисциплины	**108**	

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

Код и наименование компетенции(ий) выпускника	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-2 Способен осуществлять сбор, обработку, анализ данных для решения профессиональных задач, информирования органов государственной власти и общества на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИОПК-2.1 Ориентируется в методах сбора, обработки и анализа данных. ИОПК-2.2 Анализирует необходимую для решения профессиональных задач и информирования органов государственной власти и общества информацию из различных источников. ИОПК-2.3 Применяет безопасные информационно-коммуникационные технологии при решении профессиональных задач.	**Знать:** основы информационной безопасности и защиты информации. **Уметь:** осуществлять сбор, обработку, анализ данных для решения профессиональных задач с учетом основных требований информационной безопасности. **Владеть**: навыками выполнения профессиональных задач с учётом основных требований информационной безопасности.

5. Содержание дисциплины

Наименование тем (разделов)	Содержание тем (разделов)
Тема 1. Введение в информационную безопасность	Цели и принципы информационной безопасности. Типы угроз и атак на информационные системы. Основные принципы защиты информации. Информационная безопасность таможенных органов РФ.
Тема 2. Основы криптографии	Принципы криптографии и методы шифрования. Симметричное и асимметричное шифрование. Хэширование. Электронно-цифровые подписи. Сертификаты безопасности. Аппаратные криптографические устройства.
Тема 3. Защита компьютерных систем	Организация безопасности операционных систем. Защита от вредоносного программного обеспечения (вирусы, трояны и пр.). Основы сетевой безопасности (межсетевые экраны, системы обнаружения и предотвращения вторжений, VPN).
Тема 4. Защита информации в сети Интернет	Основы безопасности веб-приложений. Защита от атак на веб-сайты (SQL-инъекции, межсайтовый скриптинг и др.). Протокол TLS. Защита конфиденциальности данных при передаче по сети. Использование автоматизированных информационных таможенных технологий, обеспечивающих защиту информации.
Тема 5. Защита информации в корпоративной среде	Политики безопасности. Процедуры реагирования на инциденты. Защита информации в базах данных и хранилищах. Физическая безопасность информационных систем.

6. Структура дисциплины по темам с указанием отведенного на них количества академических часов и видов учебных занятий

Очная форма обучения

№ п/п	Наименование тем (разделов) дисциплины	Контактная работа, час.		Самостоятельная работа, час.	Всего, час.
		Занятия лекционного типа	Семинары		
1.	Информационная безопасность	2	2	17	21
2.	Основы криптографии	2	2	17	21
3.	Защита компьютерных систем	2	2	18	22
4.	Защита информации в сети Интернет	4	4	15	23
5.	Защита информации в корпоративной среде	4	4	13	21
Итого:		**14**	**14**	**80**	**108**

Очно-заочная форма обучения

№ п/п	Наименование тем (разделов) дисциплины	Контактная работа, час.		Самостоятельная работа, час.	Всего, час.
		Занятия лекционного типа	Семинары		
1.	Информационная безопасность	1	-	20	21
2.	Основы криптографии	1	-	20	21
3.	Защита компьютерных систем	1	1	20	22
4.	Защита информации в сети Интернет	2	1	20	23
5.	Защита информации в корпоративной среде	1	-	20	21
Итого:		**6**	**2**	**100**	**108**

7. Перечень учебно-методического обеспечения для самостоятельной работы и текущего контроля обучающихся по дисциплине

Самостоятельная работа является одним из основных видов учебной деятельности, составной частью учебного процесса и имеет своей целью: глубокое усвоение материала дисциплины, совершенствование и закрепление навыков самостоятельной работы с литературой, рекомендованной преподавателем, умение найти нужный материал и самостоятельно его использовать, воспитание высокой творческой активности, инициативы, привычки к постоянному совершенствованию своих знаний, к целеустремленному научному поиску.

Контроль самостоятельной работы, является важной составляющей текущего контроля успеваемости, осуществляется преподавателем во время лекционных и

практических (семинарских) занятий и обеспечивает оценивание хода освоения изучаемой дисциплины.

Вопросы для самостоятельного изучения

1. Уязвимости программного обеспечения и принципы «безопасного» программирования.
2. Методы социальной инженерии для получения несанкционированного доступа к информации.
3. Аутентификация и методы аутентификации.
4. Авторизация и методы авторизации.
5. Протокол шифрования Triple DES.
6. Протокол шифрования AES.
7. Протокол шифрования RSA.
8. Протокол шифрования ECDSA.
9. Способы обеспечения безопасности в беспроводных сетях.
10. Безопасность данных в операционной системе Windows.
11. Безопасность данных в iOS.
12. Безопасность данных в Android.
13. Способы шифрования информации в базах данных.
14. Резервное копирование данных и его значение для безопасности информации.
15. Меры безопасности для защиты конфиденциальной информации при передаче по сети.
16. Обеспечение информационной безопасности таможенных органов.

Примерная тематика рефератов (докладов)

1. Основные средства и системы, содержащие потенциальные источники опасных сигналов.
2. Виды угроз безопасности информации.
3. Процедура идентификации, как основа процесса обнаружения объекта
4. Методы синтеза информации.
5. Методы несанкционированного доступа к информации
6. Понятия скрытия информации, виды скрытий. Информационный портрет.
7. Способы и средства противодействия подслушиванию.
8. Потенциальные каналы утечки информации.
9. Угрозы сохранности данных в компьютере случайного характера.
10. Информационные технологии и их основные свойства.
11. Информация и информационная безопасность в современной системе таможенных органов.
12. Способы нарушения информационной безопасности таможенных органов.
13. Автоматизированные информационные системы таможенных органов.
14. Программное обеспечение транспортной логистики.
15. Обеспечение информационной безопасности ЕАИС.

Распределение самостоятельной работы

Виды, формы и объемы самостоятельной работы студентов при изучении данной дисциплины определяются ее содержанием и отражены в следующей таблице:

№ п/п	Наименование тем (разделов) дисциплины	Вид самостоятельной работы	Объем самостоятельной работы	
			очная форма обучения	очно-заочная форма обучения
1.	Введение в информационную безопасность	подготовка к аудиторным занятиям, написание рефератов	17	20
2.	Основы криптографии	подготовка к аудиторным занятиям, написание рефератов	17	20
3.	Защита компьютерных систем	подготовка к аудиторным занятиям, написание рефератов	18	20
4.	Защита информации в сети Интернет	подготовка к аудиторным занятиям, написание рефератов	15	20
5.	Защита информации в корпоративной среде	подготовка к аудиторным занятиям, написание рефератов	13	20
ИТОГО:			**80**	**100**

8. Перечень вопросов и типовые задания для подготовки к промежуточной аттестации

8.1. Перечень вопросов для подготовки к зачету с оценкой

1. Цели и принципы информационной безопасности.
2. Типы угроз и атак на информационные системы.
3. Основные принципы защиты информации.
4. Информационная безопасность таможенных органов РФ.
5. Основные угрозы информационной безопасности.
6. Методы шифрования.
7. Электронно-цифровые подписи (ЭЦП).
8. Сертификаты безопасности.
9. Хэширование.
10. Аппаратная криптография.
11. Антивирусы.
12. Методы обнаружения вторжений (IDS).
13. Методы предотвращения вторжений (IPS).
14. Преимущества использования VPN.
15. Защита от атак на веб-сайты.
16. Принципы работы протокола TLS.
17. Защита периметра и методы защиты сети.
18. Использование автоматизированных информационных таможенных технологий, обеспечивающих защиту информации.
19. Роль политик безопасности в организации.
20. Принцип наименьших привилегий.
21. Защита информации в базах данных и хранилищах.
22. Физическая безопасность информационных систем.

8.2. Типовые задания для оценки знаний

1. Алгоритм хэширования, наиболее часто используемый в настоящее время:
а) DES;
б) MD5;
в) SHA-1;
г) SHA-2.

2. В контексте информационной безопасности термин IPS означает:
а) In-Plane Switching;
б) Intruder Protection System;
в) Internal Power Supply;
г) IP Screening.

3. Наиболее безопасен для обмена данными в сети Интернет-протокол:
а) HTTP;
б) HTTPS;
в) SHA-1;
г) SHA-256.

4. Первый сервис удаленной уплаты таможенных платежей для физических лиц за товары, ввозимые в Российскую Федерацию:
а) IPPAY;
б) APPLE;
в) IP;
г) ALE.

8.3. Типовые задания для оценки умений

Задание 1.
Организации необходимо хранить конфиденциальную информацию в базе данных. Предлагается делать это в зашифрованном виде. Выберите алгоритм шифрования для решения этой задачи. Обоснуйте свой выбор.

Задание 2.
Создайте базу данных с информацией о запрещенных или ограниченных товарах, которые могут попытаться пронести через таможенный контроль. Обеспечьте доступ к этой базе только определенным сотрудникам с соответствующими полномочиями.

8.4. Типовые задания для оценки навыков

Задание 1. Разработайте рекомендации по созданию безопасных паролей, учитывая их длину, сложность и регулярную смену.

Задание 2. Опишите основные шаги, которые необходимо сделать при проведении анализа безопасности конфигурации и обновлений системы таможенного контроля, с целью обнаружения уязвимости, связанной с устаревшими версиями ПО или неправильной конфигурацией системы.

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

9.1. Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567915

2. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567672

9.2. Дополнительная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560516

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2025. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/563862

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. https://urait.ru - ЭБС «Образовательная платформа Юрайт»
2. https://coderwall.com/ - Coderwall «Сообщество программистов»

Лицензионное программное обеспечение:

- Windows (зарубежное, возмездное);
- MS Office (зарубежное, возмездное);
- Adobe Acrobat Reader (зарубежное, свободно распространяемое);
- КонсультантПлюс: «КонсультантПлюс: Студент» (российское, свободно распространяемое);
- 7-zip – архиватор (зарубежное, свободно распространяемое);
- Comodo Internet Security (зарубежное, свободно распространяемое);
- Apache NetBeans – свободная интегрированная среда разработки приложений (IDE) на языках программирования Java, Java, PHP, JavaScript, C, C++, Ада и ряда других (зарубежное, свободно распространяемое).

11. Методические рекомендации по организации изучения дисциплины

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) – русский.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачёт соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

Образовательные технологии

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

Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

Занятия семинарского типа

Семинарские (практические) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на практических занятиях оценивается по следующим критериям:

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

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание практических заданий входит в накопленную оценку.

Самостоятельная работа обучающихся

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;

- формирование умений использовать нормативную и справочную документацию, специальную литературу;
- развитие познавательных способностей, активности студентов, ответственности и организованности;
- формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов образовательного учреждения.

Перед выполнением обучающимися самостоятельной работы преподаватель может проводить инструктаж по выполнению задания. В инструктаж включается:

- цель и содержание задания;
- сроки выполнения;
- ориентировочный объем работы;
- основные требования к результатам работы и критерии оценки;
- возможные типичные ошибки при выполнении.

Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Контроль результатов самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

При самостоятельной проработке курса обучающиеся должны:

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

Рекомендации по обучению инвалидов и лиц с ОВЗ

Освоение дисциплины инвалидами и лицами с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования инвалидами и лицами с ОВЗ.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ОВЗ, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. № АК-44/05вн) в курсе предполагается использовать социально-активные и

рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Медиаматериалы также следует использовать и адаптировать с учетом индивидуальных особенностей обучения инвалидов и лиц с ОВЗ.

Освоение дисциплины инвалидами и лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам инвалидов и лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов и лиц с ОВЗ устанавливается с учетом индивидуальных психофизических особенностей. Для инвалидов и лиц с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью и лицам с ОВЗ увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью и лиц с ОВЗ процедура оценивания результатов обучения может проводиться в несколько этапов.

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

Учебная аудитория «Лаборатория информационно-коммуникационных технологий», предназначенная для проведения учебных занятий, предусмотренных настоящей рабочей программой дисциплин, оснащенная оборудованием и техническими средствами обучения, в состав которых входят: комплекты специализированной учебной мебели, доска классная, мультимедийный проектор, экран, принтер, компьютер преподавателя и компьютеры для работы обучающихся с установленным лицензионным программным обеспечением, с выходом в сеть «Интернет» и доступом в электронную информационно-образовательную среду.

Помещение для самостоятельной работы обучающихся – аудитория, оснащенная следующим оборудованием и техническими средствами: специализированная мебель для преподавателя и обучающихся, доска учебная, мультимедийный проектор, экран, звуковые колонки, компьютер (ноутбук), персональные компьютеры для работы обучающихся с установленным лицензионным программным обеспечением, с выходом в сеть «Интернет» и доступом в электронную информационно-образовательную среду.