МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы бакалавриата
по направлению подготовки
38.03.05 Бизнес-информатика,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

Направление подготовки: 38.03.05 Бизнес-информатика

Направленность (профиль): Цифровая экономика

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью освоения дисциплины является:

- комплексная и системная подготовка бакалавров, владеющих знаниями и комплексом методологических, технологических и инструментальных средств, направленных на решение задач обеспечения защиты информационного пространства в условиях цифровой экономики.

Задачи дисциплины:

- освоение методов сбора информации, связанной с производственно-хозяйтственной и финансовой деятельностью организации;

- появление навыков выполнения подготовки данных для выполнения аналитических действий;

- формирование умений по применению стандартынх методов статистического, интеллектуального анализа данных.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-2 - Способен проводить исследование и анализ рынка информационных систем и информационно-коммуникационных технологий, выбирать рациональные решения для управления бизнесом ;

ПК-6 - Способен проводить консультации по использованию и возможностям инфокоммуникационных систем и (или) их составляющих;

ПК-7 - Способен проводить сбор информации о деятельности подразделения организации с целью разработки административного регламента подразделения организации.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Уметь:

- осуществлять критический анализ проблемных ситуаций на основе системного подхода;

- вырабатывать стратегию действий;

- применять правовые,организационные, технические и программные средства защиты информации.

Знать:

- способы разработки тактических управленческих решений и процессов с учетом технологических и технико-экономических особенностей транспортных организаций и современного развития цифровых технологий;

- состав и методы организационно-правовой защиты информации;

- модели и принципы защиты информации от несанкционированного доступа.

Владеть:

- навыками работы с современными ИТ-технологиями и системами, направленными на решение профессиональных задач в сфере экономической безопасности и управления рисками транспортных организаций;

- навыками разработки административного регламента подразделений организации;

- навыками проведения консультаций по использованию и возможностям инфокоммуникационных систем и их составляющих.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №5
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 80 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован

полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Обеспечение информационной безопасности Рассматриваемые вопросы: - актуальность информационной безопасности; - методы и средства защиты информации; - объекты и субъекты защиты информации; - угрозы безопасности информации.
2	Несанкционированный доступ Рассматриваемые вопросы: - защита от несанкционированного доступа (НСД); - защита документооборота; - концепция создания защищенных компьютерных систем; - современные методы и средства защиты информации в корпорации.
3	Электронная цифровая подпись Рассматриваемые вопросы: - электронно-цифровая подпись, открытые и закрытые ключи; - таксономия нарушений информационной безопасности ВС и причины, обуславливающие их существование; - криптографические методы защиты информации, криптографические протоколы; - стеганография, концепция информационной безопасности.
4	Этапы создания комплексной системы управления защитой информационного пространства субъектов экономической деятельности . Рассматриваемые вопросы: - этапы создания комплексной системы комплексной защиты информации; - уровни защиты; - правовое регулирование обеспечения информационной безопасности.
5	Защита от неправомерного доступа Рассматриваемые вопросы: - обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения; - обеспечение защиты от иных неправомерных действий в отношении информации.
6	Стандарты информационной безопасности Рассматриваемые вопросы: - международные и отечественные стандарты информационной безопасности; - доктрина информационной безопасности.
7	Системы экономическая безопасность и управление рисками транспортных организаций Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- компьютерные преступления; - классификация компьютерных преступлений.
8	Компьютерные правонарушения Рассматриваемые вопросы: - компьютерные правонарушения; - компьютерные преступления.
9	Киберпреступления и способы борьбы с ними Рассматриваемые вопросы: - кибепреступления; - способы борьбы на государственном уровне.
10	Ответственность Рассматриваемые вопросы: - ответственность за экономические преступления; - меры по предупреждению экономических преступлений.
11	Правовое регулирование обеспечения информационной безопасности Рассматриваемые вопросы: - правовое регулирование обеспечения информационной безопасности субъектов экономической деятельности; - регламенты и правила информационной безопасности.
12	Системы экономическая безопасность и управление рисками транспортных организаций Рассматриваемые вопросы: - правовое регулирование обеспечения информационной безопасности субъектов экономической деятельности; - политика информационной безопасности.
13	Классификация преступлений Рассматриваемые вопросы: - классификация преступлений в сфере в с сфере финансов и предпринимательской деятельности; - особенности рисков ИБ
14	Классификация преступлений Рассматриваемые вопросы: - классификация преступлений в сфере внешнеэкономической деятельности; - классификация способов защиты информации.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Направления обеспечения информационной безопасности В результате работы на практическом занятии студент осваивает: - методы защиты информации от несанкционированного доступа (НСД); - реализацию методов защиты информации от НСД.
2	Направления обеспечения информационной безопасности В результате работы на практическом занятии студент осваивает: - методы защиты документооборота; - реализацию защиты документооборота.

№ п/п	Тематика практических занятий/краткое содержание
3	Направления обеспечения информационной безопасности В результате работы на практическом занятии студент осваивает криптографические методы защиты информации: - симметричные (дать описание методов и их сравнительные характеристики); - ассиметричные (дать описание методов и их сравнительные характеристики).
4	Направления обеспечения информационной безопасности В результате работы на практическом занятии студент осваивает методы: - стеганографии; - шифрования и скрытия информации.
5	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык: - проработки этапов создания комплексной системы комплексной защиты информации; - практической их реализации.
6	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык: - проработки уровней защиты; - верификацию уровней защиты.
7	Комплексные системы защиты информации В результате работы на практическом занятии изучаются методы: - технические; - программные; - криптографические; - организационные; - правовые.
8	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык: - правового регулирования обеспечения информационной безопасности; - проводится его реализация.
9	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык разработка защиты информации от: - неправомерного доступа; - уничтожения, модифицирования.
10	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык разработка защиты информации от: - блокирования; - копирования.
11	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык разработки защиты информации от: - предоставления; - распространения.
12	Комплексные системы защиты информации В результате работы на практическом занятии: - изучаются комплексные системы защиты информации; - формируется навык разработки защиты информации от иных неправомерных действий в отношении такой информации.

№ п/п	Тематика практических занятий/краткое содержание
13	Системы защиты информационного пространства субъектов экономической деятельности В результате работы на практическом занятии студент прорабатывает: - статьи УК РФ о защите информационного пространства субъектов экономической деятельности; - дополнительные законодательные акты.
14	Системы защиты информационного пространства субъектов экономической деятельности В результате работы на практическом занятии студент учится: - предусматривать возможные угрозы, нарушающие информационную безопасность; - разрабатывать комплексный подход к обеспечению ИБ.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к практическим занятиям
2	Работа с литературой
3	Работа с лекционным материалом
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2022. — 111 с. — ISBN 978-5-534-12769-0.	— Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496492 (дата обращения: 13.04.2025).
2	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — ISBN 978-5-534-03600-8.	— Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844 (дата обращения: 13.04.2025).

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

НТБ МИИТа (электронно-библиотечная система) (http://library.miit.ru)
Электронная библиотечная система «Юрайт» (https://urait.ru/)
Правовая система КонсультантПлюс (http://www.consultant.ru)

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

1. Microsoft Office;
2. Windows 8.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для проведения лекционных занятий необходима аудитория с мультимедиа аппаратурой. Для проведения практических занятий требуется аудитория, оснащенная мультимедиа аппаратурой и ПК с необходимым программным обеспечением и подключением к сети интернет.

9. Форма промежуточной аттестации:

Зачет в 5 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, доцент, к.н. кафедры
«Информационные системы
цифровой экономики» В.И. Морозова

Согласовано:

Заведующий кафедрой ИСЦЭ Л.А. Каргина

Председатель учебно-методической
комиссии М.В. Ишханян