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
09.03.03 Прикладная информатика,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль): Прикладная информатика в экономике и бизнесе

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 564169
Подписал: заведующий кафедрой Каргина Лариса Андреевна
Дата: 27.02.2023

1. Общие сведения о дисциплине (модуле).

Целью освоения дисциплины состоит в:

-комплексной и системной подготовке магистров, 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-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ПК-6 - Способен принимать участие в обеспечении информационной безопасности автоматизированных систем.

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: - Компьютерные преступления; - Классификация компьютерных преступлений.
8	Компьютерные правонарушения Рассматриваемые вопросы: -Компьютерные правонарушения; - Компьютерные преступления.
9	Киберпреступления и способы борьбы с ними Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- 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 осуществление направления обеспечения информационной безопасности.
2	Направления обеспечения информационной безопасности В результате работы на практическом занятии студент осваивает защиту от несанкционированного доступа (НСД).
3	Направления обеспечения информационной безопасности В результате работы на практическом занятии студент осваивает защиту документооборота.
4	Направления обеспечения информационной безопасности В результате работы на практическом занятии студент осваивает криптографические методы защиты информации –симметричные и ассиметричные (дать описание методов и их сравнительные характеристики).
5	Направления обеспечения информационной безопасности В результате работы на практическом занятии студент осваивает стеганографию, шифрование и скрытие информации.
6	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык проработки этапов создания

№ п/п	Тематика практических занятий/краткое содержание
	комплексной системы комплексной защиты информации.
7	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык проработки уровней защиты.
8	Комплексные системы защиты информации В результате работы на практическом занятии изучаются методы- технические, программные, криптографические, организационные, правовые.
9	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык правового регулирования обеспечения информационной безопасности.
10	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык разработка защиты информации от неправомерного доступа, уничтожения, модифицирования.
11	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык разработка защиты информации от блокирования, копирования, предоставления, распространения.
12	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык разработка защиты информации от иных неправомерных действий в отношении такой информации.
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.
14	Системы защиты информационного пространства субъектов экономической деятельности В результате работы на практическом занятии студент учитс предусматривать возможные угрозы, нарушающие информационную безопасность.

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. —	https://urait.ru/bcode/496492 (дата обращения:

	Москва : Издательство Юрайт, 2022. — 111 с. — ISBN 978-5-534-12769-0.	13.04.2023).— Текст : электронный
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.	https://urait.ru/bcode/498844 (дата обращения: 13.04.2023). — Текст : электронный

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

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

КонсультантПлюс: http://www.consultant.ru/

Гарант: http://www.garant.ru/

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

1. Microsoft Office;
2. Операционная система Windows.

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

Лекция – мультимедиа, практические работы – компьютерный класс.

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