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: 21.04.2022

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:

Знать:

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

Уметь:

осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Владеть:

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

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	Сем. №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	Направления обеспечения информационной безопасности Рассматриваемые вопросы: -Актуальность информационной безопасности. -Методы и средства защиты информации. Объекты и субъекты защиты информации. Угрозы безопасности информации. -Защита от несанкционированного доступа (НСД). Защита документооборота. Концепция создания защищенных компьютерных систем. -Современные методы и средства защиты информации в корпорации. -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.
2	Комплексные системы управления защитой информационного пространства субъектов экономической деятельности . Рассматриваемые вопросы: -Этапы создания комплексной системы комплексной защиты информации. Уровни защиты. Правовое регулирование обеспечения информационной безопасности -Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.
3	Системы экономическая безопасность и управление рисками транспортных организаций Рассматриваемые вопросы: -Международные и отечественные стандарты информационной безопасности. Доктрина информационной безопасности. -Компьютерные преступления и их классификация. -Компьютерные правонарушения и преступления. -Кибепреступления, способы борьбы на государственном уровне. -Ответственность за экономические преступления. -Правовое регулирование обеспечения информационной безопасности субъектов экономической деятельности. -Классификация преступлений в сфере экономической деятельности. (в с сфере финансов, предпринимательской, внешнеэкономической деятельности.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Направления обеспечения информационной безопасности Осуществление направления обеспечения информационной безопасности В результате работы на практическом занятии студент осваивает: -Защита от несанкционированного доступа (НСД). -Защита документооборота. -Криптографические методы защиты информации –симметричные и ассиметричные (дать описание методов и их сравнительные характеристики). -Стеганография- шифрование и скрытие информации.
2	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык

№ п/п	Тематика практических занятий/краткое содержание
	-Проработка этапов создания комплексной системы комплексной защиты информации. -Проработка уровней защиты. Методы- технические, программные, криптографические, организационные, правовые. Правовое регулирование обеспечения информационной безопасности. -Разработка защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.
3	Системы защиты информационного пространства субъектов экономической деятельности В результате работы на практическом занятии студент учится: -Проработка статей УК РФ о защите информационного пространства субъектов экономической деятельности

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.
6	Подготовка к промежуточной аттестации.
7	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	Юрайт [сайт]. — URL: https://urait.ru/bcode/496492 (дата обращения: 03.10.2022).
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	Юрайт [сайт]. — URL: https://urait.ru/bcode/498844 (дата обращения: 03.10.2022).

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

http://library.miit.ru (НТБ МИИТа (электронно-библиотечная система))

https://www.biblio-online.ru (Электронная библиотечная система «Юрайт», доступ для студентов и преподавателей РУТ(МИИТ))

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

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

MS OfficeInternet;
Microsoft Office;
Windows 8.

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»	Морозова Вера Ивановна

Лист согласования

Заведующий кафедрой ИСЦЭ	Л.А. Каргина
Председатель учебно-методической комиссии	М.В. Ишханян