МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
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

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-4 - Способен решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и технологий искусственного интеллекта, а также с учетом основных требований информационной безопасности;

ПК-5 - Способен принимать участие в обеспечении информационной безопасности автоматизированных систем.

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

Уметь:

- решать задачи профессиональной деятельности в области информационной безопасности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и технологий искусственного интеллекта с учетом требований информационной безопасности;
- принимать участие в обеспечении информационной безопасности автоматизированных систем, применяя современные методы и средства защиты информации.

Знать:

- основы информационной и библиографической культуры, информационно-коммуникационные технологии и технологии искусственного интеллекта, применяемые в области информационной безопасности, а также основные требования по защите информации;

- методы, средства и нормативно-правовые основы обеспечения информационной безопасности автоматизированных систем.

Владеть:

- навыками решения профессиональных задач в области информационной безопасности с применением информационно-коммуникационных технологий, технологий искусственного интеллекта и соблюдением требований по защите информации;

- навыками участия в обеспечении информационной безопасности автоматизированных систем с использованием современных методов и средств защиты.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 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):	48	48
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	16	16

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 60 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 осуществления обеспечения информационной безопасности; - направления обеспечения информационной безопасности.
2	Направления обеспечения информационной безопасности В результате работы на практическом занятии студент осваивает: - методы защиты информации от несанкционированного доступа (НСД)4 - реализацию методов защиты информации от НСД.

№ п/п	Тематика практических занятий/краткое содержание
3	Направления обеспечения информационной безопасности В результате работы на практическом занятии студент осваивает: - методы защиты документооборота; - реализацию защиты документооборота.
4	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).
5	Направления обеспечения информационной безопасности В результате работы на практическом занятии студент осваивает методы: - стеганографии; - шифрования и скрытия информации.
6	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык: - проработки этапов создания комплексной системы комплексной защиты информации; - практической их реализации.
7	Комплексные системы защиты информации В результате работы на практическом занятии формируется навык: - проработки уровней защиты; - верификацию 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; - проводится его реализация.
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: - 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 система Юрайт [сайт]. — URL: https://urait.ru/bcode/496492 (дата обращения: 18.04.2025).
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 система Юрайт [сайт]. — URL: https://urait.ru/bcode/498844 (дата обращения: 18.04.2025).

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. 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