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 магистратуры
по направлению подготовки
23.04.02 Наземные транспортно-технологические комплексы,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

Направление подготовки: 23.04.02 Наземные транспортно-технологические комплексы

Направленность (профиль): Пассажирский комплекс железнодорожного транспорта

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Цель: Подготовка специалистов, обладающих знаниями и навыками в области информационной безопасности, способных обеспечить защиту информационных ресурсов организаций от угроз и атак.

Задачи:

Изучение основных принципов и методов обеспечения информационной безопасности в современном информационном обществе.

Анализ угроз и уязвимостей информационных систем, разработка мер по их предотвращению и устранению.

Обучение студентов правилам и стандартам безопасной работы с информацией, включая защиту персональных данных и конфиденциальной информации.

Проведение практических занятий по симуляции атак, разработке планов реагирования на инциденты информационной безопасности и анализу уязвимостей.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1 - Способен ставить и решать научно-технические задачи в сфере своей профессиональной деятельности и новых междисциплинарных направлений с использованием естественнонаучных и математических моделей с учетом последних достижений науки и техники;

ОПК-6 - Способен оценивать социальные, правовые и общекультурные последствия принимаемых решений при осуществлении профессиональной деятельности.;

УК-6 - Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки .

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

Знать:

Основные принципы информационной безопасности и методы защиты информационных ресурсов.

Уметь:

Анализировать угрозы и уязвимости информационных систем.

Владеть:

Навыками по защите информационных систем от внешних и внутренних угроз.

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 №1
Контактная работа при проведении учебных занятий (всего):	16	16
В том числе:		
Занятия лекционного типа	8	8
Занятия семинарского типа	8	8

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 128 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	Основы информационной безопасности Введение в понятия информационной безопасности, основные угрозы и уязвимости информационных систем, принципы защиты информации, стандарты и законодательство в области информационной безопасности.
2	Методы обеспечения информационной безопасности Рассмотрение современных методов и технологий обеспечения информационной безопасности, включая шифрование данных, аутентификацию, авторизацию, аудит безопасности, мониторинг угроз и прочие.
3	Управление рисками в информационной безопасности Анализ рисков информационной безопасности, методы оценки и управления рисками, разработка стратегии обеспечения безопасности информационных ресурсов организации.
4	Инциденты информационной безопасности и реагирование на них Идентификация и классификация инцидентов информационной безопасности, разработка планов реагирования на инциденты, проведение расследования инцидентов, анализ уроков и улучшение процессов безопасности.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Криптография и защита данных Обзор основных принципов криптографии, методов шифрования данных, защиты информации от несанкционированного доступа, применение криптографии в информационной безопасности.
2	Сетевая безопасность и защита от атак Рассмотрение методов защиты сетей от внешних атак, обнаружение и предотвращение вторжений, управление доступом к сетевым ресурсам, мониторинг сетевой активности.
3	Управление доступом и аутентификация Принципы управления доступом к информационным ресурсам, методы аутентификации пользователей, ролевая модель доступа, двухфакторная аутентификация.
4	Защита персональных данных и соблюдение законодательства Обзор требований к защите персональных данных, GDPR, HIPAA и другие законы и стандарты, обеспечение конфиденциальности информации о клиентах и сотрудниках.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Анализ уязвимостей в выбранной информационной системе
2	Разработка политики информационной безопасности для малого бизнеса
3	Анализ законодательства об информационной безопасности
4	Разработка плана реагирования на инциденты информационной безопасности
5	Подготовка к промежуточной аттестации.

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

№ п/п	Библиографическое описание	Место доступа
1	Основы информационной безопасности: Учебник для вузов Н.М. Лысенко, В.В. Самойленко, А.П. Хмара. - К.: Каравела, 2019. - 432 с. - ISBN: 978-617-7535-12-3.	НТБ (МИИТ)
2	Информационная безопасность и защита информации: Учебник для вузов П.А. Баранов, В.И. Краснощеков, А.В. Кузнецов. - М.: Издательский дом "Дашков и К", 2020. - 384 с. - ISBN: 978-5-98277-578-1.	НТБ (МИИТ)
3	Актуальные проблемы информационной безопасности: Учебное пособие И.И. Иванов, Е.С. Петров, О.А. Сидоров. - СПб: БХВ-Петербург, 2021. - 320 с. - ISBN: 978-5-9775-1234-2.	НТБ (МИИТ)
4	Методы обеспечения информационной безопасности: Практическое руководство А.С. Смирнов, Е.А. Иванова, К.В. Попов. - М.: Издательство "Техника", 2022. - 256 с. - ISBN: 978-5-6040043-1-7.	НТБ (МИИТ)

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

http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ

http://rzd.ru/ - сайт ОАО «РЖД».

http://elibrary.ru/ - научно-электронная библиотека

Поисковые системы : YANDEX, GOOGLE, MAIL

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

Для проведения занятий по дисциплине необходимо наличие ПО Microsoft Office

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

Для проведения учебных занятий необходима аудитория, оснащенная доской, проектором, экраном и ПК.

9. Форма промежуточной аттестации:

Экзамен в 1 семестре.

10. Оценочные материалы.

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

Авторы:

профессор, доцент, д.н. кафедры «Управление транспортным бизнесом и интеллектуальные системы» Е.В. Копылова

Согласовано:

Заведующий кафедрой УТБиИС С.П. Вакуленко

Председатель учебно-методической комиссии Н.А. Андриянова