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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Цифровые технологии защиты информации

Направление подготовки: 09.04.03 Прикладная информатика

Направленность (профиль): Управление цифровыми активами на транспорте

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью изучения дисциплины является формирование у студентов целостных представлений о всестороннем обеспечении защиты различных объектов информатизации. З

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-1 - Способен управлять проектами в области ИТ в условиях неопределенности с применением формальных инструментов управления рисками ;

ПК-4 - Способен проектировать информационно-аналитические системы, обеспечивая выполнение требований защиты информации ограниченного доступа .

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

Знать:

современные комплексы мер по обеспечению информационной безопасности, основные средства защиты информации, способы защиты информации от НСД, основные направления обеспечения информационной безопасности

Уметь:

разрабатывать предложения по совершенствованию системы защиты объектов информатизации от НСД, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, выявлять потенциальные каналы утечки информации, определять виды информации подверженные атакам потенциального злоумышленника, разрабатывать и реализовывать комплексные меры, обеспечивающие эффективность системы защиты информации

Владеть:

методологией выбора информационных ресурсов, подлежащий защите, разрабатывать предложения по совершенствованию системы защиты объектов информатизации, способностью обоснования критериев эффективности функционирования защищенных автоматизированных систем

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 2 з.е. (72 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. №3
Контактная работа при проведении учебных занятий (всего):	26	26
В том числе:		
Занятия лекционного типа	8	8
Занятия семинарского типа	18	18

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 46 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	Информация как предмет защиты. Сущность и понятие информационной безопасности. Значение информационной безопасности и ее место в системе национальной безопасности. Современная доктрина информационной безопасности

№ п/п	Тематика лекционных занятий / краткое содержание
	Российской Федерации. Понятие и назначение доктрины информационной безопасности
2	Правовое обеспечение информационной безопасности. Основные законодательные акты, содержащие правовые нормы, направленные на защиту информации. Правовая защита открытой, общедоступной информации
3	Защита и обработка конфиденциальных документов
4	Технология конфиденциального документооборота. Стадии обработки и защиты конфиденциальных документов входного потока. Стадии обработки и защиты конфиденциальных документов выходного потока.
5	Идентификация, аутентификация и авторизация. Роль, задачи и факторы аутентификации. Классификация процессов аутентификации
6	Криптографические методы и средства обеспечения информационной безопасности. Основные задачи современной криптографии. Шифры перестановки, шифры замены, шифры гаммирования. Блочные и поточные системы шифрования. Системы шифрования с открытыми ключами. Электронные цифровые подписи.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Теория информационной безопасности и методология защиты информации.
2	Правовое обеспечение информационной безопасности
3	Организационное обеспечение информационной безопасности
4	Программноаппаратная зашита информации и защита информационных процессов в компьютерных системах
5	Сущность и задачи комплексной системы защиты информации (КСЗИ).
6	Назначение, структура и содержание управления КСЗИ.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	1. Написание докладов на заданную тему 2. Подготовка к промежуточной аттестации 3. Работа с лекционным материалом 4. Подготовка к практическим занятиям
2	Подготовка к промежуточной аттестации.

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

№	Библиографическое описание	Место доступа

п/п		
1	Защита от вирусов, межсетевые экраны и другие механизмы обеспечения безопасности информационных систем [Текст] : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита инф-ции" напр. "Информатика и выч. тех." Соловьев Владимир Павлович М. : МИИТ, 2007	НТБ МИИТ
2	Методы предотвращения и обнаружения вторжений [Текст] : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита инф-ции" напр. "Информатика и выч. тех." Соловьев Владимир Павлович М. : МИИТ, 2007	НТБ МИИТ
3	Безопасность операционных систем [Текст] : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита инфции" напр. "Информатика и выч. тех." Соловьев Владимир Павлович М. : МИИТ, 2007	НТБ МИИТ

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

Современные профессиональные базы данных и информационные справочные системы не требуются.

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

Foxit Reader/Acrobat ReaderMicrosoft Office (Word)В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

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

Для проведения аудиторных занятий требуется специализированная лекционная аудитория с мультимедиа аппаратурой

9. Форма промежуточной аттестации:

Зачет в 3 семестре.

10. Оценочные материалы.

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

Авторы

Доцент, к.н. Академии "Высшая инженерная школа"	Моргунов Виталий Михайлович

Лист согласования

Заместитель директора академии	Д.В. Паринов
Председатель учебно-методической комиссии	Д.В. Паринов