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)

Алгоритмы обеспечения конфиденциальности информации

Направление подготовки: 09.04.03 Прикладная информатика

Направленность (профиль): Управление цифровыми активами на транспорте

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Цель - формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачи – научить студентов:

- Понимать сущность информационной безопасности;

-Понимать принципы организации защиты информации на предприятиях;

-Выявлять основные виды угроз информационной безопасности; - --- Применять программно-аппаратные средства для обеспечения информационной безопасности

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:

основные шаблоны и параметры безопасности компьютерных систем

Уметь:

Осуществлять аудит применяемого пользователями ПО с помощью политики управления приложениями AppLocker в Windows 10

Работать с с системой обнаружения атак Snort и сетевым анализатором Wiresha

Владеть:

навыком анализа сетевых ресурсов с использованием утилиты nmap

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	Основные понятия информационной безопасности Идентификация Аутентификацмия

№ п/п	Тематика лекционных занятий / краткое содержание
	Информационная гигиена Защита информации
2	Настройка шаблонов безопасности (Security templates) в Windows 10
3	Анализ и настройка параметров безопасности в Windows 10
4	Аудит применяемого пользователями ПО с помощью политики управления приложениями AppLocker в Windows 10
5	Анализ сетевых ресурсов с использованием утилиты nmap
6	Работа с системой обнаружения атак Snort
7	Работа с сетевым анализатором Wireshark

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Настройка шаблонов безопасности (Security templates) в Windows 10
2	Анализ и настройка параметров безопасности в Windows 10
3	Аудит применяемого пользователями ПО с помощью политики управления приложениями AppLocker в Windows 10
4	Анализ сетевых ресурсов с использованием утилиты nmap
5	Работа с системой обнаружения атак Snort
6	Работа с сетевым анализатором Wireshark

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с учебной литературой
2	Подготовка к промежуточной аттестации.

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

№ п/п	Библиографическое описание	Место доступа
1	Вычислительные машины, системы и сети. Учебник Пятибратов А.П., Гудыно Л.П., Кириченко А.А	НТБ МИИТ

2	Сети и системы передачи информации: телекоммуникационные сети. Учебник и практикум для академического бакалавриата Самуйлов К.Е. - отв. ред., Шалимов И.А. - отв. ред., Кулябов Д.С. - отв. ред.	НТБ МИИТ
3	Ярочкин В. И Информационная безопасность: Учебник для вузов	https://e.lanbook.com/book/132242
4	Нестеров С. А. Основы информационной безопасности:	://e.lanbook.com/book/165837
1	Архитектура ЭВМ и систем. Учебное пособие для академического бакалавриата Новожилов О.П	НТБ МИИТ

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

https://docs.microsoft.com/ru-ru/

https://www.wireshark.org/download/docs/Wireshark%20User%27s%20Guide.pdf

https://www.wireshark.org/

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

Программный пакет Microsoft Office

Google Chrome

Система виртуализация HYPER-V или VMware Workstation

Wireshark

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

Компьютер преподавателя

Intel Core i7-9700 / Asus PRIME H310M-R R2.0 / 2x8GB / SSD 250Gb / DVDRW

Компьютеры студентов

Intel Core i9-9900 / B365M Pro4 / 2x16GB / SSD 512Gb /

экран для проектора, маркерная доска,

Проектор Optoma W340UST,

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" Б.В. Игольников

Согласовано:

Заместитель директора академии Д.В. Паринов

Председатель учебно-методической комиссии Д.В. Паринов