

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
09.03.01 Информатика и вычислительная техника,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): IT-сервисы и технологии обработки данных на транспорте

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: 170737
Подписал: заместитель директора академии Паринов Денис Владимирович
Дата: 29.12.2021

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-2 - Способен осуществлять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности ;

ПК-3 - Способен осуществлять разработку требований и проектирование программного обеспечения;

ПК-8 - Способен обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации;

ПК-9 - Способен обеспечивать информационную безопасность на уровне БД.

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

Знать:

основные понятия и принципы информационной безопасности
основные шаблоны и параметры безопасности компьютерных систем

Уметь:

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

Работать с системой обнаружения атак Snort и сетевым анализатором Wireshark для выявления и анализа сетевых атак

Настраивать основные шаблоны и параметры безопасности компьютерных систем

Создавать и анализировать личные базы данных параметров безопасности в оснастке Security Configuration and Analysis 5

Владеть:

навыком анализа сетевых ресурсов с использованием утилиты nmap
навыками настройки и применения политик безопасности в операционных системах Windows

навыками реагирования на сетевые атаки

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	Сем. №6
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 44 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 Рассматриваемые вопросы: -Идентификация -Аутентификация -Информационная гигиена -Защита информации
2	Информационная безопасность в системе Windows Рассматриваемые вопросы: -Настройка шаблонов безопасности (Security templates) в Windows 10 - Анализ и настройка параметров безопасности в Windows 10 - Аудит применяемого пользователями ПО с помощью политики управления приложениями AppLocker в Windows 10
3	Безопасность сетей Рассматриваемые вопросы: - Анализ сетевых ресурсов с использованием утилиты nmap - Работа с системой обнаружения атак Snort - Работа с сетевым анализатором Wireshark

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Информационная безопасность в системе Windows Рассматриваемые вопросы: -Настройка шаблонов безопасности (Security templates) в Windows 10 - Анализ и настройка параметров безопасности в Windows 10 - Аудит применяемого пользователями ПО с помощью политики управления приложениями AppLocker в Windows 10
2	Безопасность сетей Рассматриваемые вопросы: - Анализ сетевых ресурсов с использованием утилиты nmap - Работа с системой обнаружения атак Snort - 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.
3	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Ярочкин В. И Информационная безопасность: Учебник для вузов. Издательство «Академический Проект» - 544 стр.- 2020	https://e.lanbook.com/book/132242
2	Нестеров С. А. Основы информационной безопасности. Издательство "Лань"-324 стр.- 2021	https://e.lanbook.com/book/165837

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

Техническая документация Майкрософт. <https://docs.microsoft.com/ru-ru/>

Справочное руководство Nmap. <https://nmap.org/man/ru/>

Основы работы с

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

Сетевой анализатор Wireshark <https://www.wireshark.org/>

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

MS Office (Excel, Word)

Браузер Chrome

Текстовый редактор (Notepad++)

Система виртуализация HYPER-V или VMware Workstation

Wireshark

Snort

nmap

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

2 учебных класса (столы, стулья - по 25 ед)

Компьютер преподавателя

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

Компьютеры студентов (24 ед)

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

Монитор (25 ед)

Клавиатура (25 ед)

Мышка (25 ед)

Лазерный принтер (2 ед)

Проектор Optoma W340UST

Экран для проектора

Маркерная доска

9. Форма промежуточной аттестации:

Экзамен в 6 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