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
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защищенные программные платформы

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины является:

изучение студентами теории и практики основ построения архитектуры защищенных программных платформ.

В процессе освоения данной дисциплины обучаемый формирует и демонстрирует следующие профессиональные профильно-специализированные компетенции:

- способность понимать архитектуру построения современных отечественных защищенных программных платформ и анализировать направления развития архитектуры отечественных средств вычислительной техники и информационных технологий;

- способность применять методы создания программного обеспечения информационных и автоматизированных систем;

- способность применять основные методы управления вычислительным процессом при обработке данных.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Проектная деятельность:

сбор, обработку и анализ научно-технической информации по теме исследования;

разработка планов и программ проведения научных исследований и технических разработок;

обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

разработка программ для решения прикладных задач с использованием отечественных защищенных операционных систем в соответствии с техническим заданием.

Научно-исследовательская деятельность:

изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

составление отчета по выполненному заданию, участие во внедрении результатов исследований и разработок.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-4 - Способен осуществлять сбор, обработку и анализ научно-

технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;

ПК-1 - Способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.

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

Знать:

- основные угрозы безопасности информации и модели нарушителя организационные меры по защите информации;
- назначение, состав, принципы функционирования отечественных защищенных операционных систем и аппаратно-программных платформ на их основе.

Уметь:

- анализировать направления развития архитектуры отечественных средств вычислительной техники и информационных технологий;
- анализировать компьютерную систему с целью определения уровня защищенности и доверия; разрабатывать предложения по устранению выявленных уязвимостей;
- анализировать проблемную ситуацию и применять системный подход к ее решению, прогнозировать и оценивать последствия принятых решений.

Владеть:

-навыками выявление основных уязвимостей и угроз безопасности информации в автоматизированных системах;

-навыками определения уровня защищенности и доверия в компьютерных системах, оценки рисков, связанных с осуществлением угроз безопасности, формулирования предложений по устранению выявленных уязвимостей.

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. №3
Контактная работа при проведении учебных занятий (всего):	32	32
В том числе:		
Занятия лекционного типа	16	16
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 76 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	Раздел 1. Введение в защищенные программные платформы Тема 1. Основные направления развития защищенных программных платформ и информационных технологий. Рассматриваются: виды программного обеспечения, нормативно-правовая база в сфере импортозамещения программного обеспечения госсекторе России. Обзор отечественные программные платформы. Понятие защищенной программной платформы. Обзор основных защищенных программных платформ, состав, основные характеристики, способы и сфер их применения. Тема 2. Основные требования, предъявляемые к защищенным программным платформам.

№ п/п	Тематика лекционных занятий / краткое содержание
	Рассматриваются требования, предъявляемые к операционной системе, программному обеспечению и информационным технологиям, входящим в состав защищенной программной платформы, предназначенной для обработки персональных данных. Тема 3. Обеспечение безопасности операционных систем семейства Linux Раздел 2. Защищенная программная платформа «Astra Linux Special Editions» Тема 4. Отечественная программная платформа «Astra Linux». Назначение, функции, состав и основные характеристики Рассматриваются архитектура, состав, характеристики, функциональные возможности, операционной системы «Astra Linux Special Edition», средств виртуализации, системы управления базами данных, а также области их применения. Тема 5. Основы пользовательской работы и администрирования операционной системы Тема 6. Модели управления доступом и информационными потоками в операционной системах семейства Linux Тема 7. Управление безопасностью в операционной системе «Astra Linux Special Edition» Тема 8. Средства разработки программ. Принципы построения программного обеспечения информационных и автоматизированных систем на базе платформы «Astra Linux» Рассматриваются средства разработки программ, возможности и принципы построения программного обеспечения информационных и автоматизированных систем на базе платформы «Astra Linux»

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	1 Лабораторная работа № 1. Администрирование учетных записей пользователей и групп с использованием командной строки и графического интерфейса. Обучаемые получат навыки администрирования учетных записей пользователей и групп с использованием командной строки и графического интерфейса. 2 Лабораторная работа № 2. Настройка параметров мандатного управления доступом и контроля целостности Обучаемые получат навыки по настройке параметров мандатного управления доступом и контроля целостности. 3 Лабораторная работа № 3. Организация файловой системы операционной системы для работы пользователей в рамках мандатного управления доступом и контроля целостности Обучаемые получат навыки по организации файловой системы операционной системы для работы пользователей в рамках мандатного управления доступом и контроля целостности. 4 Лабораторная работа № 4. Администрирование операционной системы в рамках реализации мандатного контроля целостности. Обучаемые получат навыки по администрированию операционной системы в рамках реализации мандатного контроля целостности. 5. Лабораторная работа № 5. Настройка механизмов организации замкнутой программной среды. Контроль целостности КСЗ. Обучаемые получат навыки по настройке механизмов организации замкнутой программной среды и контролю целостности КСЗ.

№ п/п	Наименование лабораторных работ / краткое содержание
	6. Лабораторная работа № 6. Настройка сетевого взаимодействия. Обучаемые получат навыки по настройке сетевого взаимодействия.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	1. Изучение основ программирования на языке интерпретатора Borne shell/Python/php 2. Изучение основ работы с СУБД и разработки баз данных. 3. Подготовка к лабораторным работам. 4. Изучение учебной литературы из приведенных источников.
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	Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 284 с. // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/110336 (дата обращения: 04.10.2022). — Режим доступа: для авториз. пользователей. — Текст : электронный
2	Мэйволд Эрик Безопасность сетей : курс лекций / Мэйволд Эрик — Москва : Интуит НОУ, 2016. — 571 с. — ISBN 978-5-9570-0046-9.	URL: https://book.ru/book/917577 (дата обращения: 04.10.2022). — Текст : электронный.
3	В.П. Соловьев, А.Е. Шубарев, Н.Н. Пуцко.Безопасность коммуникационных сетей : учеб. пособие для студ., обуч. по	- URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/04-35188.pdf.(дата обращения: 04.10.2022)Текст : непосредственный.

	магистерской программе "Безопасность и защита информации" напр. "Информатика и выч. Тех МИИТ. Центр компетентности "Защита и безопасность информации". - М. : МИИТ, 2007. - 86 с. : ил. - (Инновационная образовательная программа - МИИТ). - Библиогр.: с. 84 (4 назв.). - Б. ц. -	
4	Голдовский Я.М.,Желенков Б.В.,Сафонова И.Е.Криптографическая защита компьютерной информации : метод. указ. к лаб. раб. по дисц. "Теоретические основы компьютерной безопасности" для студ., обуч. по напр. "Информационная безопасность" / МИИТ. Каф. "Вычислительные системы и сети". - М. : МГУПС(МИИТ), 2013. - 36 с. : ил. - Библиогр.: с. 46. - 100 экз. - (в пер.) : 39.78 р.	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/03-42764.pdf. (дата обращения 04.10.2022)Текст : непосредственный. 004 Г60

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

Разделы «Главное», «Наука и образование», «Публикации» на сайте «МЦСТ «Эльбрус». Российские микропроцессоры и вычислительные комплексы», http://www.mcst.ru

ООО «РусБИТех-Астра», https://astralinux.ru/products/astra-linux-common-edition/

Интернет-университет информационных технологий http://www.intuit.ru/

Тематический форум по информационным технологиям http://habrahabr.ru/

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

Дистрибутив ОС «Эльбрус-Linux» в составе комплекта поставки ВК «Эльбрус-801РС», ВК «Эльбрус-804».

Дистрибутив ОС Astra Linux Special Edition 1.6

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

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

Проектор для вывода изображения на экран для студентов, акустическая система, место для преподавателя оснащенное компьютером (CP UCorei3, 8GBRAM, 1Tb HDD, GeForce GTSeries).

Учебная аудитория для проведения лабораторoный занятий

Проектор для вывода изображения на экран для студентов, акустическая система, место для преподавателя оснащенное компьютером (CP UCorei3, 8GBRAM, 1Tb HDD, GeForce GTSeries).

20 ВК «Эльрус-801РС»

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

Допускается замена оборудования его виртуальными анало

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. кафедры
«Вычислительные системы, сети и
информационная безопасность» Н.А. Шаменков

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Клычева