

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

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: 4196
Подписал: заведующий кафедрой Желенков Борис
Владимирович
Дата: 02.06.2024

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 выявления 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 5 з.е. (180 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 №3
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	16	16
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 132 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	Введение в защищенные программные платформы Рассматриваются вопросы: - виды программного обеспечения; - единый реестр российских программ для электронных вычислительных машин и баз данных; - основные нормативно-правовые документы в сфере импортозамещения программного обеспечения; - обзор отечественных операционных систем; - понятие защищенной операционной системы и программной платформы. Обзор защищенных операционных систем и программных платформ семейства Linux, основные характеристики, сферы их применения.
2	Основные требования, предъявляемые к защищенным программным платформам Рассматриваются вопросы: - требования, предъявляемые к операционной системе, программному обеспечению и информационным технологиям, входящим в состав защищенной программной платформы, предназначенной для обработки персональных данных.

№ п/п	Тематика лекционных занятий / краткое содержание
3	<p>Основные принципы построения автоматизированных и информационных систем</p> <p>Рассматриваются вопросы:</p> <ul style="list-style-type: none"> - назначение, классификация автоматизированных и информационных систем, основные принципы их построения; - предъявляемые требования к средствам вычислительной техники для их применения в автоматизированных и информационных системах.
4	<p>Порядок создания автоматизированных и информационных систем</p> <p>Рассматриваются вопросы:</p> <ul style="list-style-type: none"> - обзор ГОСТ по созданию автоматизированных систем, основные подходы к формированию требований на создание автоматизированной системы; - этапы по созданию, вводу в эксплуатацию, развитию, эксплуатации и вывода из эксплуатации информационных и автоматизированных систем; - основные подходы к разработке технического задания на создание автоматизированной системы
5	<p>Защищенная программная платформа Astra Linux. Назначение, функции, состав и основные характеристики</p> <p>Рассматриваются:</p> <ul style="list-style-type: none"> - назначение, архитектура, область применения, возможности защищенной программной платформы Astra Linux; - варианты установки операционной системы; - модели управления доступом и информационными потоками в операционной системах семейства Linux
6	<p>Защищенная программная платформа Astra Linux. Основы пользовательской работы и администрирования в операционной системе</p> <p>Рассматриваются:</p> <ul style="list-style-type: none"> - варианты загрузки, экраны входа и выхода из операционной системы; - основные приемы работы с защищенной графической подсистемой; - менеджер пакетов, дистрибутив операционной системы; - терминал и командная строка, процессы, учетные записи пользователей, файловая система, права доступа к объектам файлов системы; - службы сервера; - основные задачи администрирования операционной системы; - управление безопасностью в операционной системе.
7	<p>Защищенная программная платформа Astra Linux. Средства разработки и отладки программ</p> <p>Рассматриваются:</p> <ul style="list-style-type: none"> - состав средств разработки и отладки программ; - основные подходы к разработке программного обеспечения; - принципы построения программного обеспечения информационных и автоматизированных систем на базе платформы «Astra Linux»
8	<p>Защищенная программная платформа «Astra Linux». Средства виртуализации</p> <p>Рассматриваются:</p> <ul style="list-style-type: none"> - назначение, состав, характеристик средств виртуализации, сферы их применения; - принципы функционирования средств виртуализации; - основы работы со средствами виртуализации из состава дистрибутива операционной системы

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Установка операционных систем В результате выполнения работы студент получает навыки по установке операционной системы «Astra Linux».
2	Основы работы с пакетным менеджером apt В результате выполнения работы студент получает навыки по работе с пакетным менеджером apt.
3	Исследование файловых объектов с правами пользователя В результате выполнения работы студент получает навыки работы с файловыми объектами, а также навыки по разработке сценария выполнения лабораторной работы на интерпретируемом языке программирования Borne shell/Python
4	Исследование архитектуры файловых систем ext*fs В результате выполнения работы студент получает навыки по разработке сценария выполнения лабораторной работы на интерпретируемом языке программирования Borne shell/Python.
5	Исследование процессов и служб в операционной системе В результате выполнения работы студент получает навыки по разработке сценария выполнения лабораторной работы на интерпретируемом языке программирования Borne shell/Python
6	Администрирование учетных записей пользователей и групп с использованием командной строки и графического интерфейса Обучаемые получают навыки администрирования учетных записей пользователей и групп с использованием командной строки и графического интерфейса.
7	Настройка параметров мандатного управления доступом и контроля целостности Обучаемые получают навыки по настройке параметров мандатного управления доступом и контроля целостности.
8	Организация файловой системы операционной системы для работы пользователей в рамках мандатного управления доступом и контроля целостности Обучаемые получают навыки по организации файловой системы операционной системы для работы пользователей в рамках мандатного управления доступом и контроля целостности.
9	Администрирование операционной системы в рамках реализации мандатного контроля целостности Обучаемые получают навыки по администрированию операционной системы в рамках реализации мандатного контроля целостности.
10	Настройка механизмов организации замкнутой программной среды. Контроль целостности КСЗ Обучаемые получают навыки по настройке механизмов организации замкнутой программной среды и контролю целостности КСЗ.
11	Настройка сетевого взаимодействия Обучаемые получают навыки по настройке сетевого взаимодействия.
12	Исследование средств виртуализации В результате выполнения работы студент получает навыки по установке и настройке средств виртуализации, а также разработке сценариев на интерпретируемом языке программирования Borne shell/Python
13	Исследование интерфейсов взаимодействия веб-приложений с СУБД. Разработка сценария выполнения лабораторной работы на интерпретируемых языках программирования Borne shell/Python/php В результате выполнения работы студент получает навыки разработки веб-приложения с программным интерфейсом взаимодействия с базой данных. Работа выполняется с использованием СУБД Postgres и языка Python
14	Установка (обновление) ядра Linux. Исследование способов обновления версии ядра

№ п/п	Тематика практических занятий/краткое содержание
	Linux, загрузки и конфигурирования исходных текстов ядра Linux, сборки и его установки в операционной системе Debian В результате выполнения работы студент получает навыки установки (обновления) ядра Linux, загрузки и конфигурирования исходных текстов ядра Linux, сборки и его установки в операционной системе Debian
15	Исследование способов доступа к системным вызовам ядра Linux. В результате выполнения работы студент получает навыки использования интерфейса системных вызовов ядра Linux на примере операционной системе Debian
16	Установка, настройка и использование программного средства для тестирования системных вызовов ядра В результате выполнения работы студент получает навыки установки, настройки и применения современного инструментального средства для тестирования системных вызовов ядра операционной системы Linux

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение основ программирования на языке интерпретатора Borne shell/Python/php
2	Изучение основ работы с СУБД и разработки баз данных
3	Подготовка к практическим занятиям
4	Изучение учебной литературы из приведенных источников
5	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Операционные системы Astra Linux. справочный центр	https://wiki.astralinux.ru/?ysclid=luta22mptp223657256 (дата обращения: 10.05.2024)
2	Astra linux документация	https://astragroup.ru/info/documents/ (дата обращения: 10.04.2024)

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

- Операционные системы Astra Linux. Полезные материалы. Разделы: «Правовая информация», «Документация», «Библиотека», «Сертификаты», «Полезные ресурсы»
- <https://astragroup.ru/info/>

- Документация на ОС Astra Linux, <https://astragroup.ru/info/documents>
- 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-801PC», ВК «Эльбрус-804».

Дистрибутив операционной системы Astra Linux 1.7

Дистрибутив операционной системы Debian 12.x

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

Учебная аудитория для проведения занятий лекционного типа, лабораторный занятия, 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).

20 ВК «Эльбрус-801PC»

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:

Н.А. Шаменков

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической
комиссии

Н.А. Андриянова