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)

Технологии обеспечения информационной безопасности

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: 22.12.2022

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины является:

изучение студентами теории и практики основ технологий обеспечения информационной безопасности в автоматизированных системах, создаваемых на базе аппаратно-программных платформ отечественного производства, предназначенных для защиты следующих видов информации:

-конфиденциальной информации;

-коммерческой тайны;

-персональных данных.

Под автоматизированной системой (далее – АС) обработки информации мы будем понимать совокупность следующих объектов:

-средств вычислительной техники, включающих в свой состав операционную систему со встроенным комплексом средств защиты информации;

-специального и прикладного программного обеспечения;

-каналов связи;

-информации на различных носителях;

-персонала и пользователей системы.

Информационная безопасность АС рассматривается как состояние системы, при котором:

-система способна противостоять дестабилизирующему воздействию внешних и внутренних угроз;

-функционирование и сам факт наличия системы не создают угроз для внешней среды и для элементов самой системы.

На практике информационная безопасность рассматривается как совокупность трех базовых свойств защищаемой информации – конфиденциальности, целостности и доступности.

Исходя из изложенного, студенты должны научиться использовать технологии из состава комплекса средств защиты информации, реализованные в отечественной защищенной операционной системе, прикладного программного обеспечения, а также предоставляемых средой разработки программного обеспечения для создания автоматизированных систем рассматриваемого класса.

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

-способность понимать основные положения теории информационной безопасности, основы формальной теории защиты информации;

-способность понимать нормативно-правовую базу и стандарты в области информационной безопасности в автоматизированных системах.

-способность понимать архитектуру состав, принципы функционирования отечественных защищенных операционных систем и аппаратно-программных платформ на их основе, а также анализировать направления развития архитектуры отечественных средств вычислительной техники и информационных технологий в области создания АС;

-способность анализировать функциональные возможности, принципы реализации, состав контролируемых функций комплексом средств защиты информации, реализованного в защищенной операционной системе;

-способность пользовательской работы, основ администрирования и управления безопасностью в защищенной операционной системе;

-способность задания требований к системе обеспечения информационной безопасности АС, а также анализировать и выбирать конфигураций комплекса средств защиты информации, удовлетворяющих требованиям руководящих документов по созданию АС рассматриваемого класса защищенности.

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

-Проектная деятельность:

сбор и анализ исходных данных для проектирования;

разработка программ для решения прикладных задач с использованием высокопроизводительных систем в соответствии с техническим заданием с использованием;

-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-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной

безопасности ;

ПК-2 - Способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности.

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 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	Сем. №1
Контактная работа при проведении учебных занятий (всего):	50	50
В том числе:		
Занятия лекционного типа	34	34
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 130 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	Основы информационной безопасности автоматизированных систем Рассматриваемые вопросы 1. Основные положения теории информационной безопасности 2.Угрозы информационной безопасности 3. Технологии обеспечения информационной безопасности Рассматриваются технологии обеспечения информационной безопасности и способы построения систем защиты от угроз нарушения конфиденциальности, целостности и доступности информации 4. Нормативно-правовые документы и стандарты в информационной безопасности
2	Основы теории защиты информации Рассматриваемые вопросы 5. Основные определения. Модели управления доступом. 6. Способы реализации моделей управления доступом
3	Отечественная защищенная операционная система Astra Linux и аппаратно-программные платформы на её основе Рассматриваемые вопросы

№ п/п	Тематика лекционных занятий / краткое содержание
	7. Обзор отечественных защищенных операционных систем (ЗОС). Назначение, состав, архитектура, характеристики и область их применения ЗОС «Astra Linux» 8. Назначение, состав, принципы функционирования, и описание контролируемых функций комплексом средств защиты информации ЗОС «Astra Linux». 9. Обзор отечественных аппаратно-программных платформ, функционирующих под управлением ЗОС «Astra Linux». Назначение, состав, архитектура, характеристики и область их применения 10. Анализ функциональных возможностей программной платформой ЗОС «Astra Linux» для создания автоматизированных систем рассматриваемого класса 11. Анализ средств разработки, предоставляемых программной платформой ЗОС «Astra Linux», а также подходов их использования для создания специального программного обеспечения автоматизированной системы
4	Классификация, создание автоматизированных и информационных систем по требования информационной безопасности Рассматриваемые вопросы 12. Классификация автоматизированных и информационных систем по требования информационной безопасности. Анализ требований по защите информации, не составляющей государственную тайну, содержащейся в информационных системах 13. Анализ состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных 14. Основные подходы к построению модели нарушителя и угроз 15. Основные подходы к разработке политики безопасности 16. Классификация средств защиты информации. 17. Порядок создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации автоматизированных и информационных систем и дальнейшего хранения содержащейся в их базах данных информации. Техническое задания на создание автоматизированной системы обработки персональных данных

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Практическая работа № 1. Основы работы в командной оболочке ОС «Эльбрус» / ОС «Astra Linux». Разработка сценариев на языке интерпретатора Borne shell. Программа должна позволять: 1. Осуществлять вывод информации об архитектуре, количестве процессоров и их характеристиках, объеме оперативной памяти, версии ярда операционной системы, а также версии установленного компилятора для языков программирования C/C++. Выполнять настройку IP-адреса и маски подсети для доступных сетевых интерфейсов ВК «Эльбрус-801РС». Значения параметров настройки сетевых интерфейсов должны задаваться через конфигурационный файл. Программа должна иметь функции проверки наличия конфигурационной файла и доступных сетевых интерфейсов. По завершению настройки сетевых интерфейсов, в зависимости от результата работы, программа должна выводить сообщение в виде строки сообщения: «Успех» или «Ошибка». Практическая работа № 2. Основы работы в командной оболочке ОС «Эльбрус» /ОС «Astra Linux». Разработка сценария на языке интерпретатора Borne shell, осуществляющего мониторинг доступа к объектам файловой системы

№ п/п	Тематика практических занятий/краткое содержание
	Практическая работа № 3. Основы работы с файловыми системами в ОС «Эльбрус» / ОС «Astra Linux». Исследование файловых объектов с правами пользователей. Разработка сценария на языке интерпретатора Borne shell, осуществляющего поиск файлов в файловой системе с заданными правами доступа и установленными идентификаторами SUID,SGID Практическая работа № 4. Основы работы с файловыми системами в ОС СН «Astra Linux». Разработка сценария на языке интерпретатора Borne shell, осуществляющего создание файловой системы, её монтирование, манипуляции с фалами и их содержимым Практическая работа № 5. «Реализация политики разграничения доступа средствами ОС СН «Astra Linux» Практическая работа № 6. «Наблюдение и аудит за объектами файловой системы в ОС СН «Astra Linux» Практическая работа № 7. Организация контроля целостности файлов в операционной системе ОС «Эльбрус» / ОС СН «Astra Linux». Разработка сценария на языке интерпретатора Borne shell, осуществляющего контроля целостности файлов Практическая работа № 8. Основы организации автоматизированной обработки архивов данных. Техническое задание на разработку программы, осуществляющей автоматическую распаковку многоуровневых архивных файлов. Разработка программы.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение стандартов в области информационной безопасности.
2	Анализ и дополнительная проработка материала.
3	Подготовка к практическим занятиям.
4	Изучение учебной литературы из приведенных источников.
5	Подготовка к экзамену
6	Подготовка к промежуточной аттестации.
7	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Нейман-заде М., Королёв С. Руководство по эффективному программированию на	http://www.mcst.ru/files/5ed39a/dd0cd8/50506b/000000/elbrus_prog_2020-05-30.pdf(дата обращения: 10.10.2022)

	платформе «Эльбрус» М.: АО МЦСТ – 2020	
2	Ким А.К., Перекатов В.И., Ермаков С.Г. Микропроцессоры и вычислительные комплексы семейства «Эльбрус». – СПб.: Питер, 2013	www.mcst.ru/files/511cea/886487/1a8f40/000000/book_elbrus.pdf.(дата обращения: 10.10.2022)
3	Криптографическая защита компьютерной информации УДК 681.3 Я.М. Голдовский, Б.В. Желенков, И.Е. Сафонова М.:МИИТ, 2013 -36 . : 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
4	Канальный уровень модели OSI : метод. указ. к лаб. раб. по дисц. "Сети ЭВМ и телекоммуникации" для студ. 4 курса спец. "Вычислительные машины, комплексы, системы и сети", напр. "Информатика и вычислительная техника" / Б.В. Желенков ; МИИТ. Каф. "Вычислительные системы и сети". - М. : МИИТ, 2011. - 50 с. : ил. - Библиогр.: с. 49. - 100 экз. - (в пер.) : 42.60 р.	- URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/03-41547.pdf.(дата обращения: 04.10.2022)Текст : непосредственный
5	Защита информации в вычислительных системах : учеб. пособие для студ. спец. "Прикладная информатика (в экономике)" / В.И. Морозова, К.Э. Врублевский; Ред. В.И. Морозова ; МИИТ. Каф. "Экономическая информатика". - М. : МИИТ, 2008. - 123 с. : ил.- URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/08-2435.pdf. - Библиогр.: с. 122. - 98.35 р. - Текст : непосредственный.	- URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/08-2435.pdf. -Текст : непосредственный.(дата обращения: 04.10.2022)

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

• Официальный сайт ФСТЭК Росси Главная - ФСТЭК России (fstec.ru)

• Форум специалистов по информационным технологиям http://citforum.ru/

• Документация на операционную систему Astra Linux http://astralinux.ru/

• Форум специалистов операционной системе Astra Linux http://forum.astralinux.ru/

• Документация на операционную систему Alt Linux http://altlinux.ru/

• Форум специалистов операционной системе Alt Linux http://forum.altlinux.ru/

• Документация на операционную систему Эльбрус http://mcst.ru/

• Форум специалистов операционной системе Эльбрус http://mcst.ru/

• 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).

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

2. Дистрибутив ОС Debian версии 10, 11.

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

1. 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

2. Учебная аудитория для проведения лабораторoный занятий

Проектор для вывода изображения на экран для студентов, акустическая система, место для преподавателя оснащенное компьютером

9. Форма промежуточной аттестации:

Экзамен в 1 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