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: 12.11.2025

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:

сбор и анализ исходных данных для проектирования;

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

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:

- методические подходы к разработке моделей нарушителя и угроз безопасности информации;
- методические подходы к разработке решений 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;
- навыками 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 6 з.е. (216 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 №1
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
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 168 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: - основные положения теории информационной безопасности; - угрозы информационной безопасности;
2	Основы информационной безопасности автоматизированных систем(продолжение) - технологии обеспечения информационной безопасности - нормативно-правовые документы и стандарты в информационной безопасности
3	Основы теории защиты информации Рассматриваемые вопросы: - основные определения. Модели управления доступом;
4	Основы теории защиты информации (продолжение) Рассматриваемые вопросы: - способы реализации моделей управления доступом.
5	Отечетсвенные защищенные программные платформы Рассматриваемые вопросы: - обзор отечественных операционных систем;

№ п/п	Тематика лекционных занятий / краткое содержание
	- понятие защищенной операционной системы и программной платформы. Обзор защищенных операционных систем и программных платформ семейства Linux, основные характеристики, сферы их применения;
6	Отечетсвенные защищенные программные платформы(продолжение) Рассматриваемые вопросы: - требования, предъявляемые к операционной системе, программному обеспечению и информационным технологиям, входящим в состав защищенной программной платформы, предназначенной для обработки персональных данных
7	Отечественная защищенная операционная система Astra Linux и аппаратно-программные платформы на её основе Рассматриваемые вопросы: - назначение, состав, архитектура, характеристики и область их применения ЗОС «Astra Linux» - принципы функционирования, и описание контролируемых функций комплексом средств защиты информации ЗОС «Astra Linux».
8	Отечественная защищенная операционная система Astra Linux и аппаратно-программные платформы на её основе (продолжение) Рассматриваемые вопросы: - обзор отечественных аппаратно-программных платформ, функционирующих под управлением ЗОС «Astra Linux»
9	Отечественная защищенная операционная система Astra Linux. Функциональные возможности и средства разработки программного обеспечения Рассматриваемые вопросы: - функциональные возможности программной платформой ЗОС «Astra Linux» для создания информационных и автоматизированных систем обработки персональных данных;
10	Отечественная защищенная операционная система Astra Linux. Функциональные возможности и средства разработки программного обеспечения (продолжение) Рассматриваемые вопросы: - средства разработки, предоставляемые программной платформой ЗОС «Astra Linux», а также подходы их использования для создания специального программного обеспечения информационной и автоматизированной систем обработки персональных данных.
11	Классификация, создание автоматизированных и информационных систем по требования информационной безопасности Рассматриваемые вопросы: - Руководящие документы ФСТЭК России по классификации и предъявляемым требованиям к автоматизированным системам по информационной безопасности;
12	Классификация, создание автоматизированных и информационных систем по требования информационной безопасности (продолжение) Рассматриваемые вопросы: - требований по защите информации, не составляющей государственную тайну - состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных и автоматизированных системах.
13	Методические подходы к разработке модели нарушителя и угроз безопасности Рассматриваемые вопросы: - основные подходы к построению модели нарушителя и угроз безопасности; - основные подходы к разработке политики безопасности;
14	Методические подходы к разработке модели нарушителя и угроз безопасности(продолжение) Рассматриваемые вопросы: - классификация и обоснование выбора средств защиты информации

№ п/п	Тематика лекционных занятий / краткое содержание
15	Порядок создания автоматизированных и информационных систем Рассматриваются вопросы: - порядок создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации. - анализ ГОСТ серии 34 по созданию автоматизированных систем, основные подходы к формированию требований на создание автоматизированной системы;
16	Порядок создания автоматизированных и информационных систем(продолжение) Рассматриваются вопросы: - этапы по созданию, ввода в эксплуатацию, развитию, эксплуатации и вывода из эксплуатации информационных и автоматизированных систем; - основные подходы к разработке технического задания на создание автоматизированной систем.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
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».
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.
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.
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
5	«Реализация политики разграничения доступа средствами ОС СН «Astra Linux» Разработка сценария на языке интерпретатора Borne shell, осуществляющего демонстрацию разграничения доступа к объктам файловой системы
6	«Наблюдение и аудит за объектами файловой системы в ОС СН «Astra Linux» Разработка сценария на языке интерпретатора Borne shell, осуществляющего наблюдение и логирование событий доступа к объектам файловой системы
7	Организация контроля целостности файлов в операционной системе ОС «Эльбрус» / ОС СН «Astra Linux»

№ п/п	Наименование лабораторных работ / краткое содержание
	Разработка сценария на языке интерпретатора Borne shell, осуществляющего контроля целостности файлов .
8	Основы организации автоматизированной обработки архивов данных Основы организации автоматизированной обработки архивов данных.

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 промежуточной аттестации.
6	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Хеннесси Д.Л., Паттерсон Д.А. Компьютерная архитектура. Количественный подход. Издание 5-е. – М.: ТЕХНОСФЕРА, 2016- 936 с. : ил. - (Мир радиоэлектроники). - Библиогр.: с. 839-868. - 1500 экз. - ISBN 978-5-94836-413-1	Научно-техническая библиотека МИИТ(дата обращения 04.10.2024) полочный шифр004 Х 38 Текст : непосредственный.10 экз.
2	Программирование на языке Си: практикум для студ. напр. 09.03.01 Информатика и вычислительная техника (Системы автоматизированного проектирования) / М. А. Гуркова, Э. Р. Резникова; МИИТ. Каф. Системы автоматизированного проектирования. - М.: РУТ (МИИТ), 2020. - 70 с. - Б. ц.	https://library.miit.ru/bookscatalog/metod/DC-1351.pd (дата обращения: 22.10.2025)

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 12.

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

- Учебная аудитория для проведения учебных занятий (занятий лекционного типа, практических занятий):

- компьютер преподавателя, рабочие станции студентов, мультимедийное оборудование, доска.

- Аудитория подключена к сети «Интернет».

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. Андриянова