

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 специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

**Администрирование и управление Информационной безопасностью
компьютерных систем**

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов
информатизации на базе компьютерных
систем

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: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2023

1. Общие сведения о дисциплине (модуле).

Целями изучения дисциплины «Администрирование и управление Информационной безопасности компьютерных систем» являются овладение студентами теоретических и практических основ администрирования информационных систем; способов управления информационными сетями, администрирования операционных систем, приложений, сетевых и информационных сервисов, баз данных; формирование у студентов специальных знаний в области управления современными системами информационной безопасности и защиты информации.

Задачи дисциплины: - изучение инфраструктуры вычислительной техники на железнодорожном транспорте; - изучение функционального состава автоматизированных систем в сфере: нормирования перевозочного процесса; грузовых и пассажирских перевозок; фирменного транспортного обслуживания; управления содержанием инфраструктуры; - изучение стандартов проектирования автоматизированных систем (АС), предназначенных для эксплуатации на железнодорожном транспорте; - изучение инструментальных средств проектирования АС ЖТ. Основной целью изучения учебной дисциплины «Администрирование и управление Информационной безопасности компьютерных систем» является формирование у обучающегося компетенций для следующих видов деятельности: - проектная; - контрольно-аналитическая. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности): Проектная деятельность: - разработка технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов; - разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием. Контрольно-аналитическая деятельность: - предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей; - применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты; - подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-18 - Способен принимать участие в разработке архитектуры системы защиты информации автоматизированной системы;

ПК-21 - Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой;

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла.

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

Знать:

- угроз безопасности информации, обрабатываемой беспилотными автоматизированными системами.

- угроз безопасности информации, обрабатываемой автоматизированными системами высокоскоростного транспорта.

- нормативные документы в области информационной безопасности

Уметь:

- Формулировать в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение.

- Определять ожидаемые результаты решения выделенных задач.

- Проектировать решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений.

- Решать конкретные задачи проекта заявленного качества и за установленное время.

Владеть:

- навыками анализа угроз безопасности информации, обрабатываемой автоматизированными системами высокоскоростного транспорта и обрабатываемой беспилотными автоматизированными системами.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 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. №9
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 80 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. Рассматриваемые вопросы: - Основные понятия администрирования и безопасности информационных систем. - История развития защиты информации и криптографии.
2	Администрирование операционных систем Рассматриваемые вопросы: - Математическое обеспечение АС ЖТ. - Методы и процедуры принятия решений при проектировании АС ЖТ.
3	Особенности операционных систем. Рассматриваемые вопросы: - Работа с командными строками.

№ п/п	Тематика лекционных занятий / краткое содержание
4	<p>Базовые средства администрирования Windows 2012 Server.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Управление доменом. - Active Directory
5	<p>Редактор реестра.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Редактор локальной групповой политики. - Службы Windows. Windows. - Применение знаний основ администрирования ОС Windows. - Управление инструментами администрирования ОС Windows.
6	<p>Управление ОС Windows</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Управление дисками, основные знания видов накопителей. - Диспетчер задач. - Прочие инструменты Windows для администрирования ОС.
7	<p>Управление доменом.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Контроллеры доменов. - Четыре базовые модели
8	<p>Изучение Active Directory, PowerShell.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Основы работы с Active Directory, PowerShell.
9	<p>Механизм групповой политики, служба DFS</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Технический обзор политик ограниченного использования программ.
10	<p>Служба DFS.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Управление службой DFS.
11	<p>Методы и технологии защиты информационных систем.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Многоуровневая модель системы защиты
12	<p>Виды информационных угроз</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Современные виды защиты информации.
13	<p>Политики безопасности, стандарты, процедуры и метрики, подходы к анализу рисков.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Политики безопасности, стандарты, процедуры и метрики, подходы к анализу рисков. - Lifecycle Security.
14	<p>Основные виды угроза безопасности ИС и информации.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Средства и методы защиты
15	<p>Угрозы информационной безопасности.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Источники угроз информационной безопасности.
16	<p>Системы технического нормирования перевозочного процесса.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Системы оперативного управления перевозочным процессом. - Системы фирменного транспортного обслуживания.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Структура, функции и алгоритмы систем технического нормирования перевозочного процесса и оперативного управления перевозочным процессом. - Структура, функции и алгоритмы систем фирменного транспортного обслуживания.
17	Системы резервного копирования и восстановления данных. Рассматриваемые вопросы: - Эффективность информационных систем
18	Принципы работы резервного копирования Рассматриваемые вопросы: - Эффективность информационных систем. - Российский и мировой рынки.
19	Основы администрирования баз данных Рассматриваемые вопросы: - Базы данных.
20	Основы администрирования баз данных. Рассматриваемые вопросы: - Базовые знания в работе с SQL-сервером.
21	Межсетевой экран. Рассматриваемые вопросы: - Межсетевой экран. - Классификация. - Реализация. - Система обнаружения вторжений.
22	СОВ. Рассматриваемые вопросы: - Пассивные и активные СОВ. - Сравнение межсетевых экранов и СОВ.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Функции администратора В результате выполнения лабораторной работы студент рассматривает основные функции администратора
2	Администрирование ОС Windows В результате выполнения работы студент отрабатывает применение знаний основ администрирования ОС Windows и рассматривает особенности управления инструментами администрирования ОС Windows.
3	Контролер домена В результате выполнения работы студент рассматривает особенности контролера домена
4	Модели организации доменов. В результате лабораторной работы студент рассматривает основные четыре базовые модели организации доменов.
5	Active Directory, PowerShell В результате выполнения работы студент отрабатывает умение работать с Active Directory, PowerShell
6	Службой DFS. В результате выполнения работы студент получает навык управления службой DFS.

№ п/п	Наименование лабораторных работ / краткое содержание
7	Политика безопасностей, стандартов и процедур В результате выполнения работы студент изучает политику безопасности, стандартов и процедур и рассматривает основные методы и технологии защиты информации в ИС.
8	Технологии обеспечения безопасности В результате выполнения работы студент получает навык анализа основных технологии обеспечения безопасности.
9	Защита конфиденциальной информации В результате выполнения работы студент рассматривает основные методы и технологии защиты конфиденциальности информации.
10	Потеря данных В результате выполнения работы студент рассматривает возможные причины потери данных.
11	Работа с базами данных. В результате выполнения работы студент отрабатывает умение по работе с базами данных.
12	Антивирусы и вирусы В результате выполнения лабораторной работы студент рассматривает основные антивирусы, методы обнаружения вирусов
13	Межсетевые экраны на базе устройств Palo Alto. В результате лабораторной работы студент получает навык базовых настроек и процесса мониторинга межсетевых экранов на базе устройств Palo Alto.
14	Доступ Windows (NTFS). В результате работы студент рассматривает права доступа Windows (NTFS).
15	Доступ UNIX. В результате выполнения работы студент изучает основные права доступа UNIX.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к лабораторным работам.
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.
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	Единая транспортная система. Н. А. Троицкая Академия , 2009	
2	Моделирование, анализ, реорганизация и автоматизация бизнес-процессов Г.Н. Калянов Финансы и статистика ,	НТБ (уч.6); НТБ (фб.); НТБ (чз.2)

	2007	
3	Оптимизация управления движением поездов. Л.А. Баранов Книга 2011	
1	Информационные технологии на железнодорожном транспорте Э.К. Лецкий, В.И. Панкратов, В.В. Яковлев и др.; Под ред. Э.К. Лецкого, Э.С. Поддавашкина, В.В. Яковлева Однотомное издание УМК МПС России , 2000	НТБ (уч.2); НТБ (уч.3); НТБ (уч.4); НТБ (фб.); НТБ (чз.2)
2	Управление и информационные технологии на железнодорожном транспорте Л.П. Тулупов, Э.К. Лецкий, И.Н. Шапкин и др.; Под ред. Л.П. Тулупова Однотомное издание Маршрут , 2005	НТБ (БР.); НТБ (уч.4); НТБ (фб.); НТБ (чз.1)
3	Проектирование информационных систем на железнодорожном транспорте Э.К. Лецкий, З.А. Крепкая, И.В. Маркова и др.; Под ред. Э.К. Лецкого Однотомное издание Маршрут , 2003	НТБ (ЭЭ); НТБ (уч.3); НТБ (уч.4); НТБ (фб.); НТБ (чз.1)
4	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта В.В. Яковлев, А.А. Корниенко Однотомное издание УМК МПС России , 2002	НТБ (уч.4); НТБ (фб.); НТБ (чз.1)
5	Эксплуатация железных дорог: в примерах и задачах И.Б. Сотников Однотомное издание Транспорт , 1990	НТБ (ЭЭ); НТБ (уч.1); НТБ (уч.2); НТБ (уч.4); НТБ (уч.6); НТБ (фб.); НТБ (чз.1)
6	Технико-экономические расчеты в эксплуатации железных дорог (в примерах и задачах) И.Б. Сотников, А.А. Выгнанов, Г.А. Платонов и др; Ред. И.Б. Сотников; Под Ред. И.Б. Сотников Однотомное издание Транспорт , 1983	НТБ (уч.4); НТБ (фб.)
7	Взаимодействие станций и участков железных дорог (Исследование операций на станциях) И.Б. Сотников Однотомное издание Транспорт , 1976	НТБ (уч.4); НТБ (фб.); НТБ (чз.1)

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

Официальный сайт РУТ (МИИТ) (<https://www.miit.ru/>).

Научно-техническая библиотека РУТ (МИИТ) (<http://library.miit.ru>).

Образовательная платформа «Юрайт» (<https://urait.ru/>).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (<http://e.lanbook.com/>).

Электронно-библиотечная система ibooks.ru (<http://ibooks.ru/>).

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

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

Пакет прикладных программ MATLAB,

Пакет прикладных программ MATCad,

Пакет прикладных программ LABView,

Среда визуального программирования MicroSoft Visual Studio 2013.

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

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Зачет в 9 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

профессор, профессор, д.н. кафедры
«Управление и защита информации»

В.Г. Сидоренко

Согласовано:

Заведующий кафедрой УиЗИ

Л.А. Баранов

Председатель учебно-методической
комиссии

С.В. Володин