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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Администрирование и управление Информационной безопасности 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: 01.06.2022

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:

Уметь:

Проводит моделирование автоматизированных систем с целью анализа уязвимостей.

Уметь:

На основании проведенного моделирования определяет эффективность средств и способов защиты информации.

Уметь:

Проводит анализ угроз безопасности информации, обрабатываемой автоматизированными системами высокоскоростного транспорта.

Уметь:

Проводит анализ угроз безопасности информации, обрабатываемой беспилотными автоматизированными системами.

Уметь:

Формулирует в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Определяет ожидаемые результаты решения выделенных задач.

Уметь:

Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничении?.

Уметь:

Решает конкретные задачи проекта заявленного качества и за установленное время.

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	Семестр №9
Контактная работа при проведении учебных занятий (всего):	68	68
В том числе:		
Занятия лекционного типа	34	34
Занятия семинарского типа	34	34

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	Введение.
2	Основные понятия администрирования и безопасности информационных систем. История развития защиты информации и криптографии.
3	Администрирование операционных систем Математическое обеспечение АС ЖТ. Методы и процедуры принятия решений при проектировании АС ЖТ.
4	Особенности операционных систем. Работа с командными строками.
5	Базовые средства администрирования Windows 2012 Server. Управление доменом. Active Directory

№ п/п	Тематика лекционных занятий / краткое содержание
6	администрирования. Редактор реестра. Редактор локальной групповой политики. Службы Windows. Windows. ЛР № 1. Применение знаний основ администрирования ОС Windows. Управление инструментами администрирования ОС Windows.ОС Windows.
7	Управление ОС Windows. Управление дисками, основные знания видов накопителей. Диспетчер задач. Прочие инструменты Windows для администрирования ОС.
8	Управление доменом. Контроллеры доменов. ПЗ №2 Контролер домена. ПЗ №3. Четыре базовые модели организации доменов
9	Изучение Active Directory, PowerShell. ЛР №2. Основы работы с Active Directory, PowerShell
10	Механизм групповой политики, служба DFS
11	Технический обзор политик ограниченного использования программ.
12	Технический обзор политик ограниченного использования программ.
13	Служба DFS. ЛР №3. Управление службой DFS.
14	Методы и технологии защиты информационных систем. Многоуровневая модель системы защиты
15	Виды информационных угроз. Современные виды защиты информации.
16	Политики безопасности,стандарты, процедуры и метрики, подходы к анализу рисков. Lifecycle Security.
17	Основные виды угроза безопасности ИС и информации. Средства и методы защиты
18	Угрозы информационной безопасности. Источники угроз информационной безопасности.
19	Системы технического нормирования перевозочного процесса. Системы оперативного управления перевозочным процессом. Системы фирменного транспортного обслуживания.Структура, функции и алгоритмы систем технического нормирования перевозочного процесса и оперативного управления перевозочным процессом. Структура, функции и алгоритмы систем фирменного транспортного обслуживания.
20	Системы резервного копирования и восстановления данных. Эффективность информационных систем.
21	Принципы работы резервного копирования. Эффективность информационных систем. Российский и мировой рынки.
22	Основы администрирования баз данных
23	Базы данных.
24	Основы администрирования баз данных. Базовые знания в работе с SQL-сервером.
25	Межсетевой экран. Система обнаружения вторжений.
26	Межсетевой экран. Классификация. Реализация
27	СОВ. Пассивные и активные СОВ. Сравнение межсетевых экранов и СОВ.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	ЛР1 Основные функции администратора
2	ЛР2 Применение знаний основ администрирования ОС Windows. Управление инструментами администрирования ОС Windows.
3	ЛР3 Контролер домена
4	ЛР4 Четыре базовые модели организации доменов.
5	ЛР5 Основы работы с Active Directory, PowerShell
6	ЛР6 Управление службой DFS.
7	ЛР7 Изучение политик безопасностей, стандартов и процедур. Методы и технологии защиты информации в ИС.
8	ЛР8 Технологии обеспечения безопасности
9	ЛР9 Методы и технологии защиты конфиденциальности информации.
10	ЛР10 Возможные причины потери данных.
11	ЛР11 Работа с базами данных.
12	ЛР12 Антивирусы, методы обнаружения вирусов
13	ЛР13 Базовая настройка и процесс мониторинга межсетевых экранов на базе устройств Palo Alto.
14	ЛР14 Права доступа Windows (NTFS).
15	ЛР15 Права доступа UNIX.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 Повторение лекционного материала. Изучение учебной литературы из приведенных источников: [1], [4, стр. 3-9, 35-82, 152], [6, стр. 5-14] Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. Конспектирование изученного материала.

№ п/п	Вид самостоятельной работы
2	СР2 Повторение лекционного материала. Изучение учебной литературы из приведенных источников: [4, стр. 85-130, 177-186], [5, стр. 3-4, 13-14, 40-54], [6, стр. 25-39, 63-80, 87-89, 346-391], [8], [9], [10]. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. Конспектирование изученного материала.
3	СР3 Повторение лекционного материала. Изучение учебной литературы из приведенных источников: [3, стр. 5-22], [4, стр. 143-144]. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. Конспектирование изученного материала.
4	СР4 Подготовка к практическим занятиям. Повторение лекционного материала. Изучение учебной литературы из приведенных источников: [3, стр. 5-22], [4, стр. 143-144]. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины.
5	СР5 Повторение лекционного материала. Подготовка к лабораторным работам. Изучение учебной литературы из приведенных источников: [3, стр. 23-157]. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины.
6	СР6 Подготовка к первому текущему контролю по разделам 1-5 (8 сем) Повторение лекционного материала. Подготовка к лабораторным работам. Изучение учебной литературы из приведенных источников: [4, стр. 19-21, 28-32,82-88, 130-177, 187-658], [5, стр. 28-32, 36-40, 250-290], [6, стр. 15-23, 24-37, 39-55, 80-87, 90-375, 392-402]. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. Конспектирование изученного материала.
7	СР7 Подготовка первому текущему контролю по разделам 2-6 (9 сем). Подготовка к практическим занятиям. Повторение лекционного материала. Изучение учебной литературы из приведенных источников: [2], [4, стр. 15-17], [5, стр. 15-28, 54-57, 71-250], [6, стр. 89, 331-338], [7]. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. Конспектирование изученного материала.
8	СР8 Повторение лекционного материала. Изучение учебной литературы из приведенных источников: [2], [4, стр. 15-17], [5, стр. 15-28, 54-57, 71-250], [6, стр. 89, 331-338], [7]. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. Конспектирование изученного материала.
9	СР9 Повторение лекционного материала. Изучение учебной литературы из приведенных источников Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. Конспектирование изученного материала.
10	СР10 Повторение лекционного материала. Подготовка к лабораторным работам. Изучение учебной литературы из приведенных источников Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины Конспектирование изученного материала.
11	СР11 Повторение лекционного материала. Изучение учебной литературы из приведенных источников Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины Конспектирование изученного материала.

№ п/п	Вид самостоятельной работы
12	Повторение лекционного материала. Подготовка к практическим занятиям. Изучение учебной литературы из приведенных источников Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины Конспектирование изученного материала.
13	Подготовка к промежуточной аттестации.
14	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 бизнесс-процессов Г.Н. Калянов Финансы и статистика , 2007	НТБ (уч.6); НТБ (фб.); НТБ (чз.2)
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;	НТБ (уч.4); НТБ (фб.)

	Под Ред. И.Б. Сотников Однотомное издание Транспорт , 1983	
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).

http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ. http://elibrary.ru/ - научно-электронная библиотека. http://robotosha.ru/ www.chipinfo.ru. http://siblec.ru/ http://www.intuit.ru http://twirpx.com http://habrahabr.ru http://semestr.ru scholar.google.ru http://www.intersystems.ru http://www.comprog.ru http://www.ocv.ru/ http://vniias.ru http://vniigt.ru http://rzd.ru Поисковые системы: Yandex, Google, Mail.

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

Для проведения лекционных занятийнеобходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.Для проведения практических занятийнеобходимы компьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами: - Microsoft Office не ниже Microsoft Office 2007 (2013), - 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).

Для проведения аудиторных занятий и самостоятельной работы требуется:

1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET. 2. Специализированная лекционная аудитория с мультимедиа аппаратурой и

интерактивной доской. 3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANET

Для проведения практических занятий:

компьютерный класс; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

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