МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИУЦТ

С.П. Вакуленко

30 апреля 2020 г.

Кафедра «Вычислительные системы, сети и информационная безопасность»

Автор Голдовский Яков Михайлович, к.т.н.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Методы и средства обеспечения информационной безопасности

Направление подготовки:	09.03.01 – Информатика и вычислительная техника
Профиль:	Вычислительные системы и сети
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 4 30 апреля 2020 г. Председатель учебно-методической комиссии Н.А. Клычева	Протокол № 15 27 апреля 2020 г. Заведующий кафедрой Б.В. Желенков

Рабочая программа учебной 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: 27.04.2020

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина «Методы и средства обеспечения информационной безопасности» предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Организационно-управленческой
- разработка политики информационной безопасности на уровне БД
- разработка регламентов и аудит системы безопасности данных на уровне БД
- подготовка отчетов о состоянии и эффективности системы безопасности на уровне БД
-контроль использования сетевых устройств и программного обеспечения
-администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

Производственно-технологической
- разработка технических спецификаций на программные компоненты и их взаимодействие
- осуществляет разработку тестовых документов, включая план тестирования
- разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным
- разработка архитектуры ИС
- разработка прототипов ИС
- восстановление параметров программного обеспечения сетевых устройств
- размещение и соединение элементов электрических схем стандартных ячеек библиотеки

Проектной
- определение первоначальных требований заказчика к ИС и возможности их реализации в ИС на этапе предконтрактных работ;
- разработка тестовых программ или генераторов тестовых программ для модели ИС на языках программирования целевой системы.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Методы и средства обеспечения информационной безопасности" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Информатика:

Знания: современное состояние уровня и направлений развития вычислительной техники и программных средствосновные алгоритмы типовых численных методов решения математических задачязыки программирования, структуру локальных и глобальных компьютерных сетей

Умения: работать в качестве пользователя персонального компьютераиспользовать внешние носители информации для обмена данными между машинами, создавать резервные копии данных и программ, использовать языки и системы программированияработать с программными средствами общего назначения; использовать основные приемы обработки экспериментальных данныхподготовить проектно-конструкторскую документацию разрабатываемых изделий и устройств с применением электронно-вычислительных машин

Навыки: методами поиска и обмена информацией в глобальных и локальных компьютерных сетях, техническими и программными средствами защиты информации при работе с компьютерными сетями, включая навыками работы с программными средствами общего назначения, соответствующими современным требованиям мирового рынка, включая приемы антивирусной защиты.

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

2.2.2. Преддипломная практика

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ПКР-3 Способность администрировать процесс управления безопасностью сетевых устройств, программного обеспечения, средств обеспечения безопасности удаленного доступа.	ПКР-3.1 Знать общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; инструкции по установке администрируемых сетевых устройств; инструкции по эксплуатации администрируемых сетевых устройств; инструкции по установке администрируемого программного обеспечения; инструкции по эксплуатации администрируемого программного обеспечения; протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; модель ISO для управления сетевым трафиком; модели IEEE; защищенные протоколы управления; основные средства криптографии; регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе; требования охраны труда при работе с сетевой аппаратурой администрируемой сети. ПКР-3.2 Уметь подключать и настраивать современные межсетевые экраны; пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; работать с контрольно-измерительными аппаратными и программными средствами. ПКР-3.3 Владеть навыками параметризации операционных систем средств удаленного доступа; установки дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация; настройки средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов); документирования настроек средств обеспечения безопасности удаленного.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

4 зачетные единицы (144 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 6
Контактная работа	80	80,15
Аудиторные занятия (всего):	80	80
В том числе:		
лекции (Л)	48	48
практические (ПЗ) и семинарские (С)	32	32
Самостоятельная работа (всего)	64	64
ОБЩАЯ трудоемкость дисциплины, часы:	144	144
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	4.0	4.0
Текущий контроль успеваемости (количество и вид текущего контроля)	КР (1), ПК1, ПК2	КР (1), ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЗаО	ЗаО

4.3. Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	6	Раздел 1 Введение в управление информационной безопасностью	10		6		10	26	
2	6	Тема 1.1 Основные понятия. Управление информационными рисками Международные стандартизирующие организации и стандарты в области управления информационной безопасностью.	8					8	
3	6	Раздел 2 Основные функции систем управления информационной безопасностью	10		6		10	26	
4	6	Тема 2.1 Понятие систем управления информационной безопасностью (СУИБ) Функции систем управления информационной безопасностью. Выявление и анализ рисков информационной безопасности; планирование и практическая реализация процессов, направленных на минимизацию рисков ИБ; контролирование этих процессов; внесение в процессы минимизации информационных рисков необходимых корректировок.	8					8	ПК1, выполнение и защита лабораторных работ №1-3
5	6	Раздел 3 Принципы качественного управления информационной безопасностью	8		6		10	24	
6	6	Тема 3.1 Качественное управление информационной безопасностью.	6					6	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Комплексный подход; рискообразующие факторы; согласованность с бизнес-задачами и стратегией предприятия; уровень управляемости; адекватность используемой и генерируемой информации; эффективность СУИБ как баланс между возможностями, производительностью и издержками; непрерывность управления; процессный подход.							
7	6	Раздел 4 Криптографическая защита	4		4		10	18	
8	6	Тема 4.1 Классификация криптографических алгоритмов. Основные определения. Назначение шифрования. Принципы криптографического закрытия информации. Простые методы шифрования. Таблица Вижинера. Шифрование с открытым и закрытым ключами. Основные виды атак на криптоалгоритмы. Симметричные криптоалгорит-мы.Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования. Асимметричные криптоалгоритмы.Алгоритм RSA. Алгоритм ДиффиХэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и область его применения.	4					4	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
9	6	Раздел 5 Защита от несанкционированного доступа.	8		4		12	24	
10	6	Тема 5.1 Аутентификация, авторизация и администрирование действий пользователей. Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA. Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран. Технология Zone-based farewall. Основные схемы применения межсетевых экранов. Методы анализа сетевой информации. Сигнатуры. Системы обнаружения вторжений (IDS). Системы предотвращения вторжений (IPS).	4					4	ПК2, выполнение и защита практических работ № 4-6, выполнение курсовой работы
11	6	Раздел 6 Иерархическая организация процессов управления информационной безопасностью	8		6		12	26	
12	6	Тема 6.1 Иерархия процессов управления информационной безопасностью. Замкнутый жизненный цикл системы управления информационной безопасностью. Системный подход к созданию системы управления информационной безопасностью.	4					4	КР
13	6	Раздел 7 Итоговая аттестация						0	ЗаО
14		Всего:	48		32		64	144	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 32 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	6	РАЗДЕЛ 1 Введение в управление информационной безопасностью	«ИЗУЧЕНИЕ МЕТОДОВ ШИФРОВАНИЯ»	6
2	6	РАЗДЕЛ 2 Основные функции систем управления информационной безопасностью	«ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДОВ ШИФРОВАНИЯ»	6
3	6	РАЗДЕЛ 3 Принципы качественного управления информационной безопасностью	«СОВРЕМЕННЫЕ СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ»	6
4	6	РАЗДЕЛ 4 Криптографическая защита	«НАСТРОЙКА АДМИНИСТРАТИВНОГО ДОСТУПА К МАРШРУТИЗАТОРУ»	4
5	6	РАЗДЕЛ 5 Защита от несанкционированного доступа.	«НАСТРОЙКА ПОЛИТИКИ БЕЗОПАСНОСТИ СЕТИ»	4
6	6	РАЗДЕЛ 6 Иерархическая организация процессов управления информационной безопасностью	«НАСТРОЙКА ПРОТОКОЛА БЕЗОПАСНОСТИ IPSec»	6
			ВСЕГО:	32/0

4.5. Примерная тематика курсовых проектов (работ)

4.5. Примерная тематика курсовых проектов (работ)

1. Технология защиты и безопасность телефонной базы данных
2. Технология защиты и безопасность базы данных поставщиков товаров и услуг
3. Технология защиты и безопасность базы данных технической библиотеки
4. Технология защиты и безопасность базы данных отгрузки товаров
5. Технология защиты и безопасность базы данных канц.товаров
6. Технология защиты и безопасность базы данных кадрового агенства.
7. Технология защиты и безопасность базы данных инвентаря спротивного клуба
8. Технология защиты и безопасность базы данных оборудования сетевых лабораторий
9. Технология защиты и безопасность базы данных микропроцессоров
10. Технология защиты и безопасность базы данных студентов факультата ВУЗа

11. Технология защиты и безопасность базы данных сетвого оборудования
12. Технология защиты и безопасность базы данных интегральных микросхем
13. Технология защиты и безопасность базы данных периферийного оборудования ПК

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Методы и средства обеспечения информационной безопасности» осуществляется в форме лекций, практических занятий и выполнения курсовой работы.

Лекции проводятся в традиционной классно-урочной организационной форме в объеме 32 часа, по типу управления познавательной деятельностью на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративными).

Практические занятия (32 часа) организованы с использованием технологий развивающего обучения.

Самостоятельная работа студента (72 часа) организована с использованием традиционных видов работы. К традиционным видам работы относится отработка лекционного материала и отработка отдельных тем по учебным пособиям.

Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 6 разделов, представляющих собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путем применения таких организационных форм, как индивидуальные и групповые опросы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	6	РАЗДЕЛ 1 Введение в управление информационной безопасностью	1. Анализ и дополнительная проработка материала. 2. Подготовка к выполнению практической работы №1. Изучение учебной литературы из приведенных источников: [1, стр.1-4], [2 стр. 14-25]. 3. Подготовка к выполнению курсовой работы.	10
2	6	РАЗДЕЛ 2 Основные функции систем управления информационной безопасностью	1. Анализ и дополнительная проработка материала. 2. Подготовка к выполнению практической работы №2. Изучение учебной литературы из приведенных источников: [1, стр.4-8], [2 стр. 25-32]. 3. Подготовка к выполнению курсовой работы.	10
3	6	РАЗДЕЛ 3 Принципы качественного управления информационной безопасностью	1. Анализ и дополнительная проработка материала.. 2. Подготовка к выполнению практической работы №3. Изучение учебной литературы из приведенных источников: [1, стр.9-12], [2 стр. 33-187]. 3. Подготовка и выполнение курсовой работы.	10
4	6	РАЗДЕЛ 4 Криптографическая защита	1. Анализ и дополнительная проработка материала. 2. Подготовка к выполнению работы №4. Изучение учебной литературы из приведенных источников: [1, стр.13-16], [2 стр. 188-204]. 3. Выполнение курсовой работы.	10
5	6	РАЗДЕЛ 5 Защита от несанкционированного доступа.	1. Анализ и дополнительная проработка материала. 2. Подготовка к выполнению практической работы №5. Изучение учебной литературы из приведенных источников: [1, стр.17-20], [2 стр. 205-236]. 3. Выполнению курсовой работы.	12
6	6	РАЗДЕЛ 6 Иерархическая организация процессов управления информационной безопасностью	1. Анализ и дополнительная проработка материала. 2. Подготовка к выполнению практической работы №6. Изучение учебной литературы из приведенных источников: [1, стр.21-36], [2 стр. 259-270]. 3. Выполнение курсовой работы и подготовка к защите курсовой работы.	12
			ВСЕГО:	64

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Криптографическая защита компьютерной информации	Я.М. Голдовский, Б.В. Желенков, И.Е. Сафонова	М.:МИИТЭлектронная библиотека МИИТ,http://library.miit.ru, 2013	36 сЭлектронная библиотека МИИТhttp://library.miit.ruРазделы 1-6

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
2	Информационная безопасность: защита и нападение.	Бирюков А.А.	Издательство "ДМК Пресс"Электронная библиотека МИИТ,http://library.miit.ru, 2012	474 сЭлектронная биб-лиотека МИИТhttp://library.miit.ruРазделы 1-6

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

• Форум специалистов по информационным технологиям http://citforum.ru/
• Интернет-университет информационных технологий http://www.intuit.ru/
• Тематический форум по информационным технологиям http://habrahabr.ru/

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Microsoft Windows
Microsoft Office
Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014
Microsoft Windows
Microsoft Office
Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014

Putty
Бесплатное использование (MIT)

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций №1329
Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран проекционный Аудитория подключена к интернету МИИТ.
Учебная аудитория для проведения занятий лекционного типа, практических занятий

№1327
Рабочие станции для студентов 17шт, коммутатор CISCO – 9шт, маршрутизатор CISCO – 9шт, сетевое оборудование, рабочая станция преподавателя, проектор, экран, доска

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающимся необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе. Обучающийся должен быть нацелен на максимальное усвоение подаваемого лектором мате-риала, после лекции и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы.
Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.
Главная задача лекционного курса – сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответст-вующей научно-практической области, а также методов применения полученных знаний, умений и навыков.
Основные функции лекций:
- познавательно-обучающая;
- развивающая;
- ориентирующе-направляющая;
- активизирующая;
- воспитательная;
- организующая;
- информационная.

При подготовке студента важна не только серьезная теоретическая подготовка, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. Самостоятельная работа может быть успешной при опре-деленных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.
Каждому студенту следует составлять еженедельный семестровый план работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтра. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были – по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной работы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.
Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к экзамену. Фонд оценочных средств является составной частью учебно-методического обеспечения процедуры оценки качества освоения образовательной программы и обеспечивает повышение качества

образовательного процесса и входит, как приложение, в состав рабочей программы дисциплины.
Основные методические указания для обучающихся по дисциплине указаны в разделе основная и дополнительная литература.