МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИУЦТ

С.П. Вакуленко

30 сентября 2019 г.

Кафедра «Вычислительные системы, сети и информационная безопасность»

Автор Тельнов Георгий Геннадьевич

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита программ и данных

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2019

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 2 30 сентября 2019 г. Председатель учебно-методической комиссии  Н.А. Клычева	Протокол № 2/а 27 сентября 2019 г. Заведующий кафедрой  Б.В. Желенков

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины «Защита программ и данных» является формирование компетенций в области в области защиты программ и данных от воспроизведения, исследования, модификации.
Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности).
Эксплуатационная:
- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем.
Проектно-технологическая:
- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;
- проведение предварительного технико-экономического обоснования проектных расчетов.
Экспериментально-исследовательская деятельность:
- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств.
Организационно-управленческая деятельность:
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Защита программ и данных" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

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

2.1.1. Основы информационной безопасности :

Знания: Основные угрозы информационной безопасности и методы защиты от них

Умения: Оценивать степень угрозы информационной безопасности и использовать соответствующие методы защиты

Навыки: Владеть основными приемами обнаружения и предотвращения угроз информационной безопасности, определять ценность информации, подверженной угрозам

2.1.2. Программно-аппаратные средства защиты информации:

Знания: Возможности программно-аппаратных средств защиты информации

Умения: Выбирать программно-аппаратные средства защиты информации

Навыки: Использовать программно-аппаратные средства защиты информации

2.1.3. Теоретические основы компьютерной безопасности:

Знания: Основы криптографических алгоритмов

Умения: Реализовывать криптографические алгоритмы при создании программного обеспечения

Навыки: Применять криптографические алгоритмы для защиты информации

2.1.4. Техническая защита информации:

Знания: Возможности технических средств защиты информации

Умения: Выбирать технические средства защиты информации

Навыки: Использовать технические средства защиты информации

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Государственная итоговая аттестация

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	ОПК-4 Способен применять программные средства системного и прикладного назначения, информационно-коммуникационные технологии для решения профессиональных задач;	ОПК-4.1 Знать программные средства системного и прикладного назначения, информационно-коммуникационные технологии, необходимые для решения профессиональных задач. ОПК-4.2 Уметь выбирать необходимые программные средства системного и прикладного назначения, информационно-коммуникационные технологии для решения профессиональных задач. ОПК-4.3 Владеть навыками применения программные средства системного и прикладного назначения, информационно-коммуникационные технологии для решения профессиональных задач.
2	ПКО-12 Способность принимать участие в проведении экспериментальных исследований системы защиты информации.	ПКО-12.1 Знать принципы функционирования системы защиты информации. ПКО-12.2 Уметь проводить исследование описывая каждый этап эксперимента и обосновывать полученный результат. ПКО-12.3 Владеть методами анализа процедуры исследования и результата согласно заданным критериям.

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

4.1. Общая трудоемкость дисциплины составляет:

3 зачетных единиц (108 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 8
Контактная работа	48	48,15
Аудиторные занятия (всего):	48	48
В том числе:		
лекции (Л)	24	24
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	24	24
Самостоятельная работа (всего)	60	60
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1	ПК1
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	8	Раздел 1 ЗАЩИТА ПРИ СОЗДАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	12				20	32	
2	8	Тема 1.1 Недокументированные возможности. Закладки. Обфускация кода.	4					4	
3	8	Тема 1.1 Недокументированные возможности. Закладки. Обфускация кода.	4					4	
4	8	Тема 1.2 Методы, затрудняющие чтение исходного текста и декомпиляцию. Обфускация кода	2					2	
5	8	Тема 1.3 Тестирование программного обеспечения.	2					2	
6	8	Раздел 2 ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ	6	16			20	42	ПК1, выполнение и защита лабораторных работ №1
7	8	Тема 2.1 Классификация вредоносных программ. Основные информационные ресурсы по вредоносным программам.	2					2	
8	8	Тема 2.2 Методы обнаружения известных вредоносных программ.	2					2	
9	8	Тема 2.3 Методы обнаружения неизвестных вредоносных программ.	2					2	
10	8	Раздел 3 ЗАЩИТА КОМПЬЮТЕРНЫХ ПРОГРАММ ОТ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ	6	8			20	34	, выполнение и защита лабораторных работ №2
11	8	Тема 3.1 Основные способы защиты программного обеспечения от несанкционированного использования. Серийный номер. Привязка к аппаратной конфигурации компьютера. Online и Offline активация.	2					2	

№ 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
12	8	Тема 3.2 Аппаратные средства защиты от несанкционированного использования. USB ключ	2					2	
13	8	Тема 3.3 Сетевые средства защиты от несанкционированного использования. FlexNET.	2					2	
14	8	Раздел 4 Итоговая аттестация						0	ЗаО
15		Всего:	24	24			60	108	

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 24 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	8	РАЗДЕЛ 2 ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ	ОЦЕНКА КРИПТОСТОЙКОСТИ ПАРОЛЬНОЙ ЗАЩИТЫ	16
2	8	РАЗДЕЛ 3 ЗАЩИТА КОМПЬЮТЕРНЫХ ПРОГРАММ ОТ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ	АССИМЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ ДАННЫХ Развертывание программных продуктов фирмы Microsoft и их активация с помощью KMS сервера	8
			ВСЕГО:	24/0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы по дисциплине учебным планом не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Защита программ и данных» осуществляется в форме лекций и лабораторных занятий.

Лекции (24 часов) проводятся в традиционной организационной форме с применением проекционного оборудования.

Лабораторные занятия (24 часов) проводятся в компьютерном классе, подключенном к локальной сети кафедры. Необходим доступ в сеть МИИТа (требуется доступ к KMS серверу).

Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (51 час) относится отработка лекционного материала и подготовка к лабораторным работам

Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии.
Весь курс разбит на 3 раздела, представляющих собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и описание лабораторных работ.
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	8	РАЗДЕЛ 1 ЗАЩИТА ПРИ СОЗДАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	Самостоятельное изучение вопросов защиты при создании программного обеспечения по литературе [1, стр.1-315][2, стр. 1-12][3, стр. 501-625]	20
2	8	РАЗДЕЛ 2 ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ	Подготовка к лабораторной работе № 1 [1, стр. 327-424][2, стр. 13-24][3, стр. 223-325] Учебно-методическое обеспечение находится на CD, являющемся частью УМКД	20
3	8	РАЗДЕЛ 3 ЗАЩИТА КОМПЬЮТЕРНЫХ ПРОГРАММ ОТ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ	Подготовка к лабораторной работе № 2 [1, стр. 501-625][2, стр. 25-36][3, стр. 402-514] Учебно-методическое обеспечение находится на CD, являющемся частью УМКД	20
			ВСЕГО:	60

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	Информационная безопасность	В.Ф. Шаньгин	«ДМК Пресс», 2014	702 chttps://e.lanbook.com/book/50578Доступ к тексту возможен только из МИИТа 1, стр.1-3152, стр.327-4243, стр.501-625
2	Криптографическая защита компьютерной информации УДК 681.3	Я.М. Голдовский, Б.В. Желенков, И.Е. Сафонова	М.:МИИТ, 2013	36 cЭлектронная библиотека МИИТhttp://library.miit.ru1, стр.1-122, стр.13-24 3, стр.25-36

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
3	Защита информации в компьютерных системах и сетях	Шаньгин В.Ф.	«ДМК Пресс», 2012	592 c.https://e.lanbook.com/book/3032Доступ к тексту возможен только из МИИТа 1, стр.12-1152, стр.223-3253, стр.402-514

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

Аналитическая информация по информационным технологиям [электронный ресурс] URL: http://citforum.ru/
Интернет-университет информационных технологий [электронный ресурс] URL: http://www.intuit.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

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, лабораторных работ
№1330

Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран, 25 персональных компьютеров , 25 мониторов, 1 принтер, доска учебная.

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

Качество полученного образования сильно зависит от активности самого обучающегося в учебном процессе. Для хорошего усвоения материала важно доверие студентов к преподавателю. Поэтому во время и после занятий, включая лекции и лабораторные работы, студенты имеют право задавать любые вопросы по изучаемой дисциплине. Допускается задавать вопросы во время лекции.
Лекции гораздо лучше усваиваются, если студент перед лекцией уже познакомился с рассматриваемым на лекции материалом. Для этого в начале изучения дисциплины студент получает от преподавателя информацию о том, что и в каком порядке будет изучаться в течение всего курса, а также источники информации по рассматриваемым вопросам. К источникам информации относится литература и ресурсы в сети «Интернет».
Лабораторные работы могут быть выполнены студентом, как на занятии, так и дома на своем компьютере. Для того чтобы студент мог по своему выбору решать, где ему выполнять лабораторные работы, задания ко всем лабораторным работам предоставляются на первом лабораторном занятии. Независимо от того, где выполнялась лабораторная работа, показать результаты ее выполнения преподавателю студент должен в аудитории на лабораторном занятии. По просьбе студента допускается использовать в качестве лабораторного компьютера переносной компьютер студента.