

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:	<u>10.03.01 – Информационная безопасность</u>
Профиль:	<u>Безопасность компьютерных систем</u>
Квалификация выпускника:	<u>Бакалавр</u>
Форма обучения:	<u>очная</u>
Год начала подготовки	<u>2017</u>

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 2 30 сентября 2019 г. Председатель учебно-методической комиссии</p>  <p style="text-align: right;">Н.А. Клычева</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p>Протокол № 2/а 27 сентября 2019 г. Заведующий кафедрой</p>  <p style="text-align: right;">Б.В. Желенков</p>
---	--

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины «Защита программ и данных» является формирование компетенций 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

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-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знать и понимать: Основные принципы, лежащие в основе защиты программного обеспечения, способы защиты. Уметь: Определять необходимые способы защиты программного обеспечения. Владеть: Навыками анализа информационных ресурсов, подлежащих защите.
2	ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Знать и понимать: Методы защиты программного обеспечения от несанкционированного использования Уметь: Устанавливать в сети защищенное программное обеспечение. Владеть: Навыками установки отдельных видов защиты программного обеспечения.

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

4.1. Общая трудоемкость дисциплины составляет:

3 зачетные единицы (108 ак. ч.).

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

Вид учебной работы	Количество часов	
	Всего по учебному плану	Семестр 8
Контактная работа	44	44,15
Аудиторные занятия (всего):	44	44
В том числе:		
лекции (Л)	18	18
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	26	26
Самостоятельная работа (всего)	64	64
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 промежуточной 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	6				22	28	
2	8	Тема 1.1 Недокументированные возможности. Закладки. Обфускация кода.	1					1	
3	8	Тема 1.2 Методы, затрудняющие чтение исходного текста и декомпиляцию. Обфускация кода	1					1	
4	8	Тема 1.3 Тестирование программного обеспечения.	2					2	
5	8	Тема 1.4 Соккрытие присутствия программы в системе. Исполнение данных как кода. Повышение привилегий.	2					2	
6	8	Раздел 2 ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ	8	16/6			22	46/6	
7	8	Тема 2.1 Классификация вредоносных программ. Основные информационные ресурсы по вредоносным программам.	1					1	
8	8	Тема 2.2 Методы обнаружения известных вредоносных программ.	1					1	
9	8	Тема 2.3 Методы обнаружения неизвестных вредоносных программ.	1					1	
10	8	Тема 2.4 Настройка операционной системы, повышающая ее безопасность.	1					1	
11	8	Тема 2.5 Сетевые средства борьбы с вредоносными программами.	2					2	
12	8	Тема 2.6 Средства защиты от вредоносных программ. Сравнение основных средств защиты.	2					2	ПК1, Выполнение лабораторной работы № 1
13	8	Раздел 3	4	10/3			20	34/3	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		ЗАЩИТА КОМПЬЮТЕРНЫХ ПРОГРАММ ОТ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ							
14	8	Тема 3.1 Основные способы защиты программного обеспечения от несанкционированного использования. Серийный номер. Привязка к аппаратной конфигурации компьютера. Online и Offline активация.	1					1	
15	8	Тема 3.2 Аппаратные средства защиты от несанкционированного использования. USB ключ	1					1	
16	8	Тема 3.3 Сетевые средства защиты от несанкционированного использования. FlexNET.	2					2	
17	8	Раздел 4 Дифференцированный зачет						0	ЗаО
18		Всего:	18	26/9			64	108/9	

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 26 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 / 6
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	10 / 3
ВСЕГО:				26/9

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

Лабораторные занятия (26 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 (64 часа) 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 завершённый объём 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.

Проведении занятий по дисциплине (модулю) возможно с применением электронного обучения и дистанционных образовательных технологий, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

В процессе проведения занятий с применением электронного обучения и дистанционных образовательных технологий применяются современные образовательные технологии, такие как (при необходимости):

- использование современных средств коммуникации;
- электронная форма обмена материалами;
- дистанционная форма групповых и индивидуальных консультаций;
- использование компьютерных технологий и программных продуктов, необходимых для сбора и систематизации информации, проведения требуемых программой расчетов и т.д.

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]	22
2	8	РАЗДЕЛ 2 ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВРЕДНОСНЫХ 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	22
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:				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	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 сЭлектронная 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 с.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

При организации обучения по дисциплине (модулю) с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».

В случае проведения занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

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.

В случае проведения занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

Допускается замена оборудования его виртуальными аналогами.

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 ознакомился 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 относятся 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.