

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

СОГЛАСОВАНО:

Выпускающая кафедра ВССиИБ
Заведующий кафедрой ВССиИБ



Б.В. Желенков

30 апреля 2020 г.

УТВЕРЖДАЮ:

Директор ИУЦТ



С.П. Вакуленко

30 апреля 2020 г.

Кафедра «Цифровые технологии управления транспортными процессами»

Автор Семенов Юрий Станиславович, к.ф.-м.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2018

Одобрено на заседании Учебно-методической комиссии института Протокол № 4 30 апреля 2020 г. Председатель учебно-методической комиссии  Н.А. Клычева	Одобрено на заседании кафедры Протокол № 1 27 апреля 2020 г. Доцент  В.Е. Нутович
---	--

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В курсе Б1.Б.24 «Криптографические методы защиты информации» изучаются основные математические методы криптографии. Знания, приобретаемые студентами в процессе изучения этой дисциплины, используются в дисциплинах профессионального цикла, связанных с защитой информации. Цель преподавания дисциплины – обеспечить студентам знания в области теоретической криптографии и ее прикладных методов, необходимые для профессиональной деятельности специалистов по компьютерной и информационной безопасности.

Компетенции, приобретаемые студентами, применяются для научно-исследовательской деятельности.

Дисциплина предназначена для получения знаний при решении следующих профессиональных задач: основные задачи и понятия криптографии, понятие шифрования, применение принципов шифрования, построение криптографических систем и алгоритмов, применение алгоритмов при защите информации.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Криптографические методы защиты информации" 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. Дискретная математика. Алгебра и теория чисел (дополнительные главы):

Знания: современную информационную картину мира в образовательной и профессиональной деятельности; основные методы, способы и средства получения, хранения, переработки информации; способы работы с информацией в глобальных компьютерных сетях.

Умения: решать задачи, связанные с делимостью чисел, строить конечные поля, работать с группами обратимых элементов конечных полей.

Навыки: различными методами обработки информации, теоретического и экспериментального исследования; методами компьютерной обработки информации; методами поиска информации в глобальных компьютерных сетях; методами соблюдения требований информационной безопасности.

2.1.2. Числовые методы криптографии:

Знания: основные теоремы и формулы алгебры, основные понятия теории групп, строение мультипликативной группы колец вычетов, свойства символов Лежандра и Якоби, тесты на простоту для натуральных чисел; методы разложения чисел и многочленов на множители.

Умения: решать задачи, связанные с делимостью чисел, строить конечные поля, работать с группами обратимых элементов конечных полей.

Навыки: методами решения задач теории чисел, алгебры и теории групп

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Криптографические протоколы

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	ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знать и понимать: основные задачи и понятия криптографии, понятие шифрования, принципы шифрования, принципы построения криптографических систем и алгоритмов, применение алгоритмов при защите информации. Уметь: использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки, применять стандарты в области криптографических методов информационной безопасности для проектирования, разработки и анализа защищенности информационных систем, разбираться в современной литературе по криптографии. Владеть: криптографическими понятиями, стандартными криптографическими алгоритмами, реализуемыми на компьютерах, приемами математического моделирования в шифровании.
2	ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знать и понимать: основы методов анализа информационной безопасности объектов и систем. Уметь: применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования. Владеть: приемами и навыками работы с объектами и системами информационной безопасности с использованием отечественных и зарубежных стандартов.
3	ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Знать и понимать: основы и методику проведения анализа и экспериментально-исследовательских работ системы защиты информации. Уметь: проводить часть экспериментально-исследовательских работ системы защиты Владеть: техникой проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности.

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 6
Контактная работа	42	42,15
Аудиторные занятия (всего):	42	42
В том числе:		
лекции (Л)	28	28
практические (ПЗ) и семинарские (С)	14	14
Самостоятельная работа (всего)	66	66
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
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 промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	6	Раздел 1 История и основные понятия криптографии	10		4/2		22	36/2	ПК1
2	6	Тема 1.1 История и основы криптографии	1					1	
3	6	Тема 1.2 Основные понятия криптографии	1					1	
4	6	Тема 1.3 Виды шифров. Результаты К. Шеннона	2					2	
5	6	Тема 1.4 Криптостойкость шифров. Атаки	2					2	
6	6	Тема 1.5 Статистический анализ шифр-текстов	2					2	
7	6	Тема 1.6 Псевдослучайные последовательности и шифрование	2					2	
8	6	Раздел 2 Матем. принципы шифрования	10		5/4		20	35/4	ПК2
9	6	Тема 2.7 Стандартные вспомогательные алгоритмы	2					2	
10	6	Тема 2.8 Генерирование случайных подстановок, шифры перестановок	2					2	
11	6	Тема 2.9 Простые числа, из распр-ние, псевдопростые числа	2					2	
12	6	Тема 2.10 Тесты на простоту. Тест Рабина-Миллера	2					2	
13	6	Тема 2.11 Построение больших простых чисел	2					2	
14	6	Раздел 3 Криптосистемы и понятие протокола	8		5		24	37	ЗаО, КР
15	6	Тема 3.12 Блочное шифрование. Поточные	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
		шифры							
16	6	Тема 3.13 Алгоритм шифрования RSA	2					2	
17	6	Тема 3.14 Алгоритм шифрования Эль-Гамала	1					1	
18	6	Тема 3.15 Алгоритм шифрования Рабина	1					1	
19	6	Тема 3.16 Криптографические хэш-функции	1					1	
20	6	Тема 3.17 Понятие криптопротокола	1					1	
21		Всего:	28		14/6		66	108/6	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 14 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 История и основные понятия криптографии	Виды шифров. Результаты К. Шеннона	1 / 2
2	6	РАЗДЕЛ 1 История и основные понятия криптографии	Криптостойкость шифров. Атаки	1
3	6	РАЗДЕЛ 1 История и основные понятия криптографии	Статистический анализ шифр-текстов	1
4	6	РАЗДЕЛ 1 История и основные понятия криптографии	Псевдослучайные последовательности и шифрование	1
5	6	РАЗДЕЛ 2 Матем. принципы шифрования	Стандартные вспомогательные алгоритмы	1 / 2
6	6	РАЗДЕЛ 2 Матем. принципы шифрования	Простые числа, из распр-ние, псевдопростые числа	1 / 2
7	6	РАЗДЕЛ 2 Матем. принципы шифрования	Генерирование случайных подстановок, шифры перестановок	1
8	6	РАЗДЕЛ 2 Матем. принципы шифрования	Тесты на простоту. Тест Рабина-Миллера	1
9	6	РАЗДЕЛ 2 Матем. принципы шифрования	Построение больших простых чисел	1
10	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола	Блочное шифрование. Поточные шифры	1
11	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола	Алгоритм шифрования RSA	1
12	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола	Алгоритм шифрования Эль-Гамала	1
13	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола	Алгоритм шифрования Рабина	1
14	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола	Криптографические хэш-функции	1
ВСЕГО:				14/6

4.5. Примерная тематика курсовых проектов (работ)

Построение больших простых чисел, алгоритмы шифрования RSA, алгоритмы шифрования Эль-Гамала, схемы цифровой подписи на основе RSA и др. криптосистемы

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины Б1.Б.24 «Криптографические методы защиты информации» осуществляется в форме лекций, практических занятий и курсовой работы.

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

Практические занятия организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач) в объёме 28 часов. Остальная часть практического курса (6 часов) проводится с использованием интерактивных (диалоговые) технологий, в том числе разбор и анализ конкретных ситуаций, дискуссии (решение проблемных поставленных задач и исследование моделей); технологий, основанных на коллективных способах обучения (возможны видеоконференции при подготовке курсовых проектов).

Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям.

Предполагаются консультации студентов по курсовой работе.

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 задания практического содержания для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые решения задач, решение индивидуальных лабораторных заданий с использованием.

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 История и основные понятия криптографии	История и основы криптографии [1], [2]. Подготовка дом. заданий	2
2	6	РАЗДЕЛ 1 История и основные понятия криптографии	Основные понятия криптографии [1], [2]. Подготовка дом. заданий	4
3	6	РАЗДЕЛ 1 История и основные понятия криптографии	Виды шифров. Результаты К. Шеннона [1], [2]. Подготовка дом. заданий	4
4	6	РАЗДЕЛ 1 История и основные понятия криптографии	Криптостойкость шифров. Атаки [1], [2]. Подготовка дом. заданий	4
5	6	РАЗДЕЛ 1 История и основные понятия криптографии	Статистический анализ шифр-текстов [1], [2]. Подготовка дом. заданий	4
6	6	РАЗДЕЛ 1 История и основные понятия криптографии	Псевдослучайные последовательности и шифрование [1], [2]. Подготовка дом. заданий	4
7	6	РАЗДЕЛ 2 Матем. принципы шифрования	Стандартные вспомогательные алгоритмы [1], [2]. Подготовка дом. заданий, курсовой работы	4
8	6	РАЗДЕЛ 2 Матем. принципы шифрования	Простые числа, из распр-ние, псевдопростые числа [1], [2]. Подготовка дом. заданий, курсовой работы	4
9	6	РАЗДЕЛ 2 Матем. принципы шифрования	Генерирование случайных подстановок, шифры перестановок [1], [2]. Подготовка дом. заданий, курсовой работы	4
10	6	РАЗДЕЛ 2 Матем. принципы шифрования	Тесты на простоту. Тест Рабина-Миллера [1], [2]. Подготовка дом. заданий, курсовой работы	4
11	6	РАЗДЕЛ 2 Матем. принципы шифрования	Построение больших простых чисел [1], [2]. Подготовка дом. заданий, курсовой работы	4
12	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола	Блочное шифрование. Поточные шифры [1], [2]. Подготовка дом. заданий, курсовой работы	4
13	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола	Алгоритм шифрования RSA [1], [2]. Подготовка дом. заданий, курсовой	4

			работы	
14	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола	Алгоритм шифрования Эль-Гамала [1], [2]. Подготовка дом. заданий, курсовой работы	4
15	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола	Алгоритм шифрования Рабина [1], [2]. Подготовка дом. заданий, курсовой работы	4
16	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола	Криптографические хэш-функции [1], [2]. Подготовка дом. заданий, курсовой работы	4
17	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола	Понятие криптопротокола [1], [2]. Подготовка дом. заданий, курсовой работы	4
ВСЕГО:				66

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	Основы современной криптографии: Учебный курс	Баричев С.Г., Гончаров В.В., Серов Р. Е.	М: «Горячая линия – телеком», 2011	НТБ МИИТ
2	Введение в криптографию	Под редакцией В.В.Яценко	М: МЦНМО, 2012	НТБ МИИТ
3	Введение в теоретико-числовые методы криптографии.	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.	СПб: «Лань», 2010	НТБ МИИТ
4	Введение в криптосистемы с открытым ключом	Молдовян Н. А., Молдовян А.А	СПб.: БХВ-Петербург, 2005	НТБ МИИТ

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
5	Современная криптография: теория и практика	Венбо Мао	Вильямс, 2005	НТБ МИИТ
6	Классическое введение в современную теорию чисел	К. Айерлэнд,	М: МИР, 1987	НТБ МИИТ
7	Криптография в задачах и упражнениях.	Осипян В. О., Осипян К.В.	М.: Гелиос АРВ, 2004	НТБ МИИТ

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

<http://library.mii.ru/> - электронно-информационная система НТБ МИИТ

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

Не требуется

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

10.1. Требования к аудиториям (помещениям, кабинетам) для проведения занятий с указанием соответствующего оснащения

- Доска, мел, тряпка (губка) для стирания; компьютерное и мультимедийное оборудование: компьютер, проектор, экран;

10.2. Требования к программному обеспечению при прохождении учебной дисциплины

- пакет прикладных обучающих программ: MATHCAD, Maple

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

Регулярно выполнять домашние задания, изучать дополнительные материалы, повторять темы из предыдущих семестров. Интересующимся студентам рекомендуется участвовать в студенческих олимпиадах.

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 соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.

Выполнение практических заданий служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.

Проведение практических занятий не сводится только к органическому дополнению лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.

При подготовке специалиста важны не только серьезная теоретическая подготовка. Этому способствует форма обучения в виде практических занятий. Задачи практических занятий: закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.

Самостоятельная работа может быть успешной при определенных 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 и семестровый планы 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 учебы. 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 и тестовые материалы, где

каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания.

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.