

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 сентября 2019 г.

Кафедра «Цифровые технологии управления транспортными процессами»

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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптографические протоколы

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

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
--	---

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: 5665
Подписал: Доцент Нутович Вероника Евгеньевна
Дата: 27.04.2020

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В курсе " Криптографические протоколы" изучаются известные протоколы, обеспечивающие защиту информации. Знания, приобретаемые студентами в процессе изучения этой дисциплины, используются в дисциплинах профессионального цикла, связанных с информационной защитой. Цель преподавания дисциплины – обеспечить студентам знания в области теоретической и прикладной криптографии, 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: применение стандартных криптопротоколов и интернет-технологий, средств и методов хранения и передачи аутентификационной информации, основных протоколов идентификации и аутентификации абонентов, протоколов дистанционного принятия решений, математических моделей шифров, использование криптографических стандартов.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Криптографические протоколы" 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: кольца, конечные поля

Умения: владение арифметикой конечных полей

Навыки: Навыки: нахождение произведений и обратных элементов в полях

2.1.2. Криптографические методы защиты информации:

Знания: основные принципы криптографии и защиты информации, алгоритмы шифрования RSA и Эль-Гамала

Умения: моделирование систем RSA и Эль-Гамала, построение больших простых чисел

Навыки: работа в кольцах вычетов и кольцах многочленов

2.1.3. Числовые методы криптографии:

Знания: группы обратимых элементов в кольцах вычетов, подстановки

Умения: владение алгоритмом быстрого возведения в степень по модулю

Навыки: работа в кольцах вычетов

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-2 Способен использовать совокупность необходимых математических методов для решения задач обеспечения защиты информации.	ОПК-2.1 Знать необходимые математические методы для решения задач обеспечения защиты информации. ОПК-2.2 Уметь совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-2.3 Владеть навыками применения совокупности необходимых математических методов для решения задач обеспечения защиты информации.

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 7
Контактная работа	54	54,15
Аудиторные занятия (всего):	54	54
В том числе:		
лекции (Л)	36	36
практические (ПЗ) и семинарские (С)	18	18
Самостоятельная работа (всего)	54	54
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	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	7	Раздел 1 Понятие протокола, базовые протоколы	12		6		18	36	ПК1, Контр. работа №1
2	7	Тема 1.1 Понятие протокола, отличия от криптосистем	4					4	
3	7	Тема 1.8 Протокол Диффи- Хеллмана	4					4	
4	7	Тема 1.9 Протокол Блюма	4					4	
5	7	Раздел 2 Стандартные протоколы	12		6		18	36	ПК2, Контр. работа №2
6	7	Тема 2.2 Протоколы аутентификации	4					4	
7	7	Тема 2.3 Электронная подпись	4					4	
8	7	Тема 2.4 Разделение секрета	4					4	
9	7	Раздел 3 Другие виды протоколов	12		6		18	36	
10	7	Тема 3.5 Протоколы электронных платежей	4					4	
11	7	Тема 3.6 Электронные деньги с купюрами разного номинала	4					4	
12	7	Тема 3.7 Криптографические хэш-функции	4					4	
13	7	Раздел 4 Итоговая аттестация						0	ЗаО
14		Всего:	36		18		54	108	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 18 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего ча- сов/ из них часов в интерак- тивной форме
1	2	3	4	5
1	7	РАЗДЕЛ 1 Понятие протокола, базовые протоколы	Понятие протокола, отличия от криптосистем	2
2	7	РАЗДЕЛ 1 Понятие протокола, базовые протоколы	Протокол Диффи-Хеллмана	2
3	7	РАЗДЕЛ 1 Понятие протокола, базовые протоколы	Протокол Блюма	2
4	7	РАЗДЕЛ 2 Стандартные протоколы	Протоколы аутентификации	2
5	7	РАЗДЕЛ 2 Стандартные протоколы	Электронная подпись	2
6	7	РАЗДЕЛ 2 Стандартные протоколы	Разделение секрета	2
7	7	РАЗДЕЛ 3 Другие виды протоколов	Протоколы электронных платежей	2
8	7	РАЗДЕЛ 3 Другие виды протоколов	Электронные деньги с купюрами разного номинала	2
9	7	РАЗДЕЛ 3 Другие виды протоколов	Криптографические хэш-функции	2
ВСЕГО:				18/0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины Б1.Б.32 «Криптографические протоколы» осуществляется в форме лекций и практических занятий.

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. Проведение практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач) в объеме 16 часов.

Возможен разбор и анализ конкретных ситуаций, дискуссии (решение проблемных поставленных задач и исследование моделей); технологий, основанных на коллективных способах обучения (возможны видеоконференции при подготовке курсовых работ).

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. К

интерактивным (диалоговым) технологиям относится отработка отдельных тем по электронным пособиям, подготовка к текущему и промежуточному контролю, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.

Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. 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 заданий с использованием компьютеров или на бумажных носителях.

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	7	РАЗДЕЛ 1 Понятие протокола, базовые протоколы	Понятие протокола, отличия от криптосистем [1], [2]. Подготовка дом. заданий	4
2	7	РАЗДЕЛ 1 Понятие протокола, базовые протоколы	Понятие протокола, отличия от криптосистем [1], [2]. Подготовка дом. заданий	6
3	7	РАЗДЕЛ 1 Понятие протокола, базовые протоколы	Протокол Блюма [1], [2]. Подготовка дом. заданий	4
4	7	РАЗДЕЛ 1 Понятие протокола, базовые протоколы	Протокол Диффи-Хеллмана [1], [2]. Подготовка дом. заданий	4
5	7	РАЗДЕЛ 2 Стандартные протоколы	Протокол аутентификации Шнорра [1], [2]. Подготовка дом. заданий/докладов	6
6	7	РАЗДЕЛ 2 Стандартные протоколы	Электронная подпись [1], [2]. Подготовка дом. заданий/докладов	6
7	7	РАЗДЕЛ 2 Стандартные протоколы	Разделение секрета [1], [2]. Подготовка дом. заданий/докладов	6
8	7	РАЗДЕЛ 3 Другие виды протоколов	Протоколы электронных платежей [1], [2]. Подготовка дом. заданий/докладов	6
9	7	РАЗДЕЛ 3 Другие виды протоколов	Электронные деньги с купюрами разного номинала [1], [2]. Подготовка дом. заданий/докладов	6
10	7	РАЗДЕЛ 3 Другие виды протоколов	Криптографические хэш-функции [1], [2]. Подготовка дом. заданий/докладов	6
ВСЕГО:				54

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.	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	М.: Гелиос АРВ, 2005	НТБ МИИТ
6	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.miiit.ru/> - электронно-информационная система НТБ МИИТ

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

- пакет прикладных обучающих программ: MATHCAD, Maple.

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

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

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.