МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

СОГЛАСОВАНО:	УТВЕРЖДАЮ:
Выпускающая кафедра ВССиИБ	Директор ИУЦТ
Заведующий кафедрой ВССиИБ	
Б.В. Желенков	С.П. Вакуленко
30 апреля 2020 г.	30 апреля 2020 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	2017

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 № 1 27 апреля 2020 г. Доцент В.Е. Нутович

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В курсе _____ Б1.Б.32 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-Гамаля

Умения: моделирование систем RSA и Эль-Гамаля, 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

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: стандартные криптопротоколы, основы Интернет-технологий, средства и методы хранения и передачи аутентификационной информации, основные протоколы идентификации и аутентификации абонентов, протоколы дистанционного принятия решений, математические модели шифров, криптографические стандарты. Уметь: : применять стандартные криптопротоколы, основные схемы электронной подписи, протоколы идентификации, протоколы передачи и распределения ключей, строить криптографические хеш-функции. Владеть: криптографической терминологией; навыками анализа безопасности криптографических протоколов

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

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 7
Контактная работа	36	36,15
Аудиторные занятия (всего):	36	36
В том числе:		
лекции (Л)	18	18
практические (ПЗ) и семинарские (С)	18	18
Самостоятельная работа (всего)	45	45
Экзамен (при наличии)	27	27
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)	ЭК	ЭК

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, виды протоколов	6		6/2		15	27/2	ПК1
2	7	Тема 1.1 Понятие протокола, отличия от криптосистем, примеры	2					2	
3	7	Тема 1.8 Протоколы с разделением секрета	2					2	
4	7	Тема 1.9 Аутентификация в информационных системах	2					2	
5	7	Раздел 2 Стандарт. криптопротоколы	6		6/2		15	27/2	ПК2
6	7	Тема 2.2 Протоколы Блюма и выработки общего ключа	2					2	
7	7	Тема 2.3 Протокол аутентификации Шнорра	2					2	
8	7	Тема 2.4 Электронная подпись	2					2	
9	7	Раздел 3 Другие виды криптопротоколов	6		6/2		15	27/2	
10	7	Тема 3.5 Протоколы, связанные с эл. платежами	2					2	
11	7	Тема 3.6 Протоколы голосования	2					2	
12	7	Тема 3.7 Разделение секрета	2					2	
13	7	Экзамен						27	ЭК
14		Всего:	18		18/6		45	108/6	

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 часов/ из них часов в интерактивной форме
1	2	3	4	5
1	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов	Понятие протокола, отличия от криптосистем, примеры	2
2	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов	Протоколы с разделением секрета(интерактив)	2 / 2
3	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов	Аутентификация в информационных системах	2
4	7	РАЗДЕЛ 2 Стандарт. криптопротоколы	Протоколы Блюма и выработки общего ключа	2
5	7	РАЗДЕЛ 2 Стандарт. криптопротоколы	Протокол аутентификации Шнорра	2 / 2
6	7	РАЗДЕЛ 2 Стандарт. криптопротоколы	Электронная подпись	2
7	7	РАЗДЕЛ 3 Другие виды криптопротоколов	Протоколы, связанные с эл. платежами	2
8	7	РАЗДЕЛ 3 Другие виды криптопротоколов	Протоколы, связанные с эл. платежами.	2 / 2
9	7	РАЗДЕЛ 3 Другие виды криптопротоколов	Протоколы голосования	2
			ВСЕГО:	18/6

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, 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. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач) в объёме 12 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. Также предполагается, что студенты могут делать небольшие 15-20-минутные доклады-презентации по разбираемым темам (возможны видеоконференции при подготовке докладов).
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. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 3 раздела, представляющих собой логически завершенный 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	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов	Протоколы с разделением секрета [1], [2]. Подготовка дом. заданий	5
2	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов	Аутентификация в информационных системах [1], [2]. Подготовка дом. заданий	5
3	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов	Понятие протокола, отличия от криптосистем, примеры [1], [2]. Подготовка дом. заданий	5
4	7	РАЗДЕЛ 2 Стандарт. криптопротоколы	Протоколы Блюма и выработки общего ключа [1], [2]. Подготовка дом. заданий/докладов	5
5	7	РАЗДЕЛ 2 Стандарт. криптопротоколы	Протокол аутентификации Шнорра [1], [2]. Подготовка дом. заданий/докладов	5
6	7	РАЗДЕЛ 2 Стандарт. криптопротоколы	Электронная подпись [1], [2]. Подготовка дом. заданий/докладов	5
7	7	РАЗДЕЛ 3 Другие виды криптопротоколов	Протоколы, связанные с эл. платежами [1], [2]. Подготовка дом. заданий/докладов	5
8	7	РАЗДЕЛ 3 Другие виды криптопротоколов	Разделение секрета [1], [2]. Подготовка дом. заданий/докладов	5
9	7	РАЗДЕЛ 3 Другие виды криптопротоколов	Протоколы голосования [1], [2]. Подготовка дом. заданий/докладов	5
			ВСЕГО:	45

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. Ященко	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.miit.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)

Не требуется

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.