

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

Кафедра «Цифровые технологии управления транспортными процессами»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Криптографические протоколы»

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>2018</u>

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.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
------	---

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

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. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1

Понятие протокола, виды протоколов

Тема: Понятие протокола, отличия от криптосистем, примеры

Тема: Протоколы с разделением секрета

Тема: Аутентификация в информационных системах

РАЗДЕЛ 2

Стандарт. криптопротоколы

Тема: Протоколы Блума и выработки общего ключа

Тема: Протокол аутентификации Шнорра

Тема: Электронная подпись

РАЗДЕЛ 3

Другие виды криптопротоколов

Тема: Протоколы, связанные с эл. платежами

Тема: Протоколы голосования

Тема: Разделение секрета

РАЗДЕЛ 4

Итоговая аттестация