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

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.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОПК-2	Способен использовать совокупность необходимых математических методов для решения задач обеспечения 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 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 объёме 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. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1
Понятие протокола, базовые протоколы

Контр. работа №1

Тема: Понятие протокола, отличия от криптосистем

Тема: Протокол Диффи-Хеллмана

Тема: Протокол Блюма

РАЗДЕЛ 2
Стандартные протоколы

Контр. работа №2

Тема: Протоколы аутентификации

Тема: Электронная подпись

Тема: Разделение секрета

РАЗДЕЛ 3
Другие виды протоколов

Тема: Протоколы электронных платежей

Тема: Электронные деньги с купюрами разного номинала

Тема: Криптографические хэш-функции

РАЗДЕЛ 4
Итоговая аттестация