

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

**АННОТАЦИЯ К**  
**РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Криптографические протоколы**

Направление подготовки: 10.03.01 – Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

Форма обучения: Очная

Общие сведения о дисциплине (модуле).

Целями освоения дисциплины (модуля) являются:

- ознакомление студентов с основными понятиями теории криптографических протоколов;
- овладение основными идеями и методами современной теории криптографических протоколов;
- ознакомление студентов с основными криптографическими протоколами распределения ключей, протоколами аутентификации, различными промежуточными и более развитыми протоколами;
- овладение навыком разложения любого криптографического протокола на промежуточные с целью создания программного обеспечения, обслуживающего исполнение протокола.

Задачами дисциплины являются:

- получение 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.

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов)).