

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

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

**Технологии киберзащиты в современных сетях**

Направление подготовки: 11.03.02 – Инфокоммуникационные технологии и системы связи

Направленность (профиль): Системы мобильной связи и сетевые технологии на транспорте

Форма обучения: Очная

**Общие сведения о дисциплине (модуле).**

Целью освоения учебной дисциплины «Технологии киберзащиты в современных сетях» является формирование у обучающихся компетенций в соответствии с требованиями образовательного стандарта базового высшего образования по направлению подготовки «Инфокоммуникационные технологии и системы связи».

Задачами дисциплины являются:

- ознакомление обучающихся с архитектурой, принципами построения и эволюцией систем защиты информации в современных телекоммуникационных и инфокоммуникационных сетях;

- изучение современных методов и средств криптографической защиты данных, аутентификации, управления доступом и обеспечения конфиденциальности в гетерогенных сетевых средах;

- освоение технологий защиты сетевого и транспортного уровней, включая конфигурирование межсетевых экранов (NGFW), систем

обнаружения и предотвращения вторжений (IDS/IPS), а также механизмов безопасной маршрутизации и коммутации;

- формирование практических навыков развертывания систем мониторинга информационной безопасности, анализа защищенности сетей, выявления уязвимостей и автоматизированного реагирования на инциденты (SIEM/SOC);

- приобретение умений по обеспечению кибербезопасности специализированных сегментов, включая системы мобильной связи (4G/5G), беспроводные сети доступа, IoT-устройства и транспортные инфокоммуникационные системы;

- развитие компетенций в области нормативно-правового регулирования информационной безопасности, защиты критической информационной инфраструктуры (КИИ) и применения современных концепций (Zero Trust, SASE) в корпоративных сетях связи.

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 академических часа(ов)).