

Аннотация магистерской программы

Теоретическая и практическая криптография

Направление подготовки 10.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Цель программы: подготовка высококвалифицированных кадров с целью обеспечения защиты национальной безопасности в интересах государственных структур, в том числе специальных служб и вооруженных сил Российской Федерации. Программа обеспечивает формирование профессиональных компетенций, необходимых для проведения теоретических и прикладных исследований криптографических средств защиты информации, а также использующих их программных и аппаратных систем. Выпускники магистратуры также обладают компетенциями в области разработки и анализа защищенных программно-аппаратных комплексов. Программа предназначена только для граждан Российской Федерации.

Уровень образования / Срок обучения: Магистр / 2 года.

Выпускающее подразделение: кафедра криптологии и кибербезопасности (42)

Область профессиональной деятельности: профессиональная деятельность выпускников связана с решением задач обеспечения информационной безопасности государства, связанных с использованием криптографических методов.

Особенности учебного плана: основные конкурентные преимущества программы заключаются в том, что в ней учтены многолетние традиции подготовки высококвалифицированных специалистов в МИФИ, а также опыт отечественной криптографической школы, позволившие разработать уникальные курсы.

Программа состоит из трех основных частей: 1) фундаментальная математическая подготовка; 2) специальная криптографическая подготовка; 3) специальная подготовка в области вычислительной техники и программирования, предназначенная для решения практических задач.

Математическая часть программы включает курсы, обязательные для освоения современных криптографических дисциплин. Студенты изучают: алгебраические, вероятностные и комбинаторные методы криптографии; криптографические свойства булевых функций; теорию автоматов; основы квантовой информатики. Криптографическая часть подготовки также включает следующие необходимые

специалисту дисциплины: основы криптографии; асимметричные и симметричные криптосистемы; теоретико-числовые методы криптографии; криптографические протоколы; основы блокчейн-технологии; современные методы криптоанализа; квантовая криптография; основы защиты речевых и факсимильных сообщений. В рамках специальной подготовки в области вычислительной техники и программирования изучаются: современные технологии и методы программирования; операционные системы; низкоуровневое программирование; безопасность вычислительных сетей; основы дизассемблирования и реинжиниринга.

Научно-исследовательская работа студентов осуществляется в тесной связи с исследованиями, интересующими специальные подразделения государственных организаций.

Выпускники магистратуры могут продолжить обучение в аспирантуре для получения высшей квалификации по направлениям: методы и системы защиты информации, информационная безопасность; информатики и вычислительной техника.

Перечень предприятий для трудоустройства выпускников:

1. **Государственные организации:** специальные службы РФ, министерство обороны РФ, ФСТЭК России, ФГУП НТЦ «Атлас», институты РАН, предприятия и институты государственной корпорации «Росатом».
2. **Негосударственные российские организации, специализирующиеся в области защиты информации:** ИнфоТеКС, Крипто-ПРО, лаборатория Касперского, Информзащита, Актив.