



ПРОГРАММА АСПИРАНТУРЫ
«Методы и системы защиты информации, информационная безопасность (в области обеспечения безопасности объектов критической информационной инфраструктуры)»

Научная специальность 2.3.6. «Методы и системы защиты информации, информационная безопасность» (технические науки, физико-математические науки)

Выпускающая кафедра: кафедра стратегических информационных исследований (№43) научно-образовательного центра «Безопасность интеллектуальных киберфизических систем» (НОЦ «БИКС») Института интеллектуальных кибернетических систем (ИИКС).

Форма обучения: очная

Срок обучения: 3 года

Куратор программы: Дворянкин Сергей Владимирович, SVDvoryankin@mephi.ru

Цель программы:

Целью программы аспирантуры является подготовка аспирантом диссертации на соискание ученой степени кандидата технических наук в области информационной безопасности. Аспирантам предлагается участие в научно-исследовательских работах по созданию методов и средств защиты информационных систем от внутренних и внешних угроз, выявлению и нейтрализации технических каналов утечки информации, защиты цифрового мультимедийного контента от фальсификации и нелегитимного использования и др.

Направления научных исследований:

- Теория и методология защиты информации и обеспечения информационной безопасности.
- Методы, модели, системы и средства выявления уязвимостей программного и аппаратного обеспечения, протоколов взаимодействия, информационных процессов и систем.
- Методы, модели, системы и средства выявления угроз безопасности информации в автоматизированных, информационных, киберфизических и телекоммуникационных системах различного назначения, включая компьютерные сети различной архитектуры, и на других объектах информатизации.
- Методы, модели, системы и средства управления доступом, идентификация, аутентификация, разграничение и контроль доступа.
- Методы, модели, системы, средства обеспечения и контроля целостности информации, информационных потоков и процессов обработки информации.
- Методы, модели, системы и средства обнаружения вредоносного программного обеспечения.
- Методы (способы), модели, системы и средства защиты информации от утечки по техническим каналам.
- Методы, модели и средства обеспечения надежности и киберустойчивости систем защиты информации.
- Методы, модели, системы, алгоритмы и средства криптографической и стеганографической защиты информации в автоматизированных, информационных, киберфизических, телекоммуникационных и других системах.
- Системы и средства (программные, технические, программно-технические) обеспечения безопасности информации в автоматизированных, информационных, киберфизических и телекоммуникационных системах, включая компьютерные сети различной архитектуры, и на других объектах информатизации.
- Методы, модели, системы, средства анализа и оценки рисков информационной безопасности.
- Методы, модели, системы и средства аудита, контроля и мониторинга информационной безопасности, а также оценки защищенности автоматизированных, информационных,

киберфизических и телекоммуникационных систем и выделенных помещений, включая компьютерные сети различной архитектуры

- Методы, модели, системы и средства обнаружения, предупреждения и противодействия компьютерным атакам с ликвидацией их последствий, в том числе в открытых системах.
- Методы, модели, методики, системы и средства оценки эффективности защиты информации.
- Методы (способы), модели, методики и средства сертификации программного обеспечения и аппаратно-программных средств защиты информации.
- Методы, модели, методики и средства проведения специальных исследований и специальных проверок технических средств, проведения специальных обследований выделенных помещений.
- Методы, модели и системы обеспечения доверия в отношении информационной среды, электронной компонентной базы, процессов и технологий.
- Методы, модели, системы и средства обеспечения безопасности систем искусственного интеллекта и машинного обучения.
- Технологии искусственного интеллекта в задачах информационной безопасности.
- Технологии, модели, методы системы обеспечения защищенного документооборота.
- Методы и модели выявления и противодействия распространению ложной и вредоносной информации в социально-технических системах.
- Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.
- Методы, модели, системы и средства защиты цифрового контента (аудиовизуальной текстовой) информации от фальсификации и нелегитимного использования с учетом особенностей формирования, передачи, обработки и хранения в инфокоммуникационных системах, компьютерных сетях и иных каналах межличностных коммуникаций.

Организации-партнеры для проведения совместных научных исследований:

- АО НПО «ЭШЕЛОН»
- АО «ЭНПО СПЭЛС»
- АО «ИнфоТекс»
- ООО «Гексагон»

Научные группы, научные лаборатории, центры НИЯУ МИФИ:

- Научно-образовательный центр «Безопасность интеллектуальных киберфизических систем»
- Аттестационно-испытательный центр информационной безопасности и систем защиты информации

Защита в диссертационном совете НИЯУ МИФИ МИФИ.2.04

