



ПРОГРАММА АСПИРАНТУРЫ «Методы и системы защиты информации, информационная безопасность»

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

Выпускающая кафедра: научно-образовательный центр «Безопасность интеллектуальных киберфизических систем» - кафедры криптографии и безопасности компьютерных систем" (№41), криптологии и кибербезопасности (№ 42), стратегических информационных исследований (№43), информационной безопасности банковских систем (№44).

Форма обучения: очная

Срок обучения: 3 года

Куратор программы: Епишкина Анна Васильевна, avepishkina@mephi.ru

Цель программы:

Целью программы аспирантуры является подготовка аспирантом диссертации на соискание ученой степени кандидата технических или физико-математических в области информационной безопасности. Аспирантам предлагается участие в научно-исследовательских работах по созданию методов защиты информационных систем от внутренних и внешних угроз, математических моделей и методов криптографических доказательств, обладающих свойством нулевого разглашения, по разработке стойких криптографических протоколов.

Направление научных исследований:

- Теория и методология обеспечения информационной безопасности и защиты информации.
- Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.
- Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.
- Системы документооборота (вне зависимости от степени их компьютеризации) и средства защиты циркулирующей в них информации.
- Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.
- Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.
- Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования.
- Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения.
- Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.
- Модели и методы оценки защищенности информации и информационной безопасности объекта.
- Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.

- Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.
- Методы и модели выявления и противодействия распространению ложной и вредоносной информации.
- Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.
- Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.
- Модели, методы и средства обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах.
- Методы, модели и средства разработки безопасного программного обеспечения, выявления в нем дефектов безопасности, противодействия скрытым каналам передачи данных и выявления уязвимостей в компьютерных системах и сетях.
- Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании.
- Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

Организации-партнеры для проведения совместных научных исследований:

- ООО «КРИПТО-ПРО»

Научные группы, научные лаборатории, центры НИЯУ МИФИ:

- Лаборатория информационной безопасности
- Лаборатория искусственного интеллекта

