ПРОГРАММА АСПИРАНТУРЫ
«Методы и системы защиты информации, информационная безопасность (в области криптологии и кибербезопасности)»

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

Выпускающая кафедра: кафедра «Криптология и кибербезопасность» (№ 42)
Форма обучения: очная
Срок обучения: 3 года
Куратор программы:

- к.т.н., доцент Епишкина Анна Васильевна, AVEpishkina@mephi.ru

Цель программы:

Целью программы аспирантуры является подготовка аспирантом диссертации на соискание ученой степени кандидата технических наук в области криптологии и кибербезопасности. Аспирантам предлагается участие в НИОКР в сфере разработке и анализа криптографических методов и средств защиты информации, обеспечения безопасности данных, компьютерных систем и сетей (преимущественно программными методами), а также приобретение необходимого для осуществления профессиональной деятельности уровня знаний, умений и навыков.

Направление научных исследований:

- Теория и методология обеспечения информационной безопасности и защиты информации в компьютерных системах и сетях;
- Методы, аппаратно-программные средства и организационные меры защиты систем формирования и предоставления пользователям информационных ресурсов различного вида;
- Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в корпоративных и открытых компьютерных сетях, включая Интернет;
- Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях;
- Модели и методы оценки защищенности информации в компьютерных системах и информационной безопасности объектов защиты;
- 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 и контроля доступа;
- Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности;
- 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;
- Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов. Разработка и обоснование стойкости криптографических алгоритмов, примитивов и протоколов для решения прикладных задач.

Организации-партнеры для проведения совместных научных исследований:

- ФГУП СНПО «Элерон»;
- АО «РАСУ»;
- ФГУП КЦ «Атомбезопасность»;
- ЗАО «Гринатом»;
- ООО «КРИПТО-ПРО»;
- ООО «Код Безопасности»;
- ООО «ЦБИ «МАСКОМ».

Научные группы, научные лаборатории, центры НИЯУ МИФИ:

- Научно-образовательный центр «Безопасность интеллектуальных киберфизических систем»;
- «Диджитал-центр» НИЯУ МИФИ.

Защита в диссертационном совете НИЯУ МИФИ.