

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ

13 июля 1970 г. приказом Министерства высшего и среднего специального образования РСФСР в составе Томского университета был создан факультет прикладной математики. В начале 80-х гг. он был переименован в факультет прикладной математики и кибернетики.

Структура факультета

Кафедра исследования операций (зав. – проф. А. М. Горцев). Открыта в 1978 г.

Кафедра прикладной математики (зав. – проф. Ю. И. Параев). Открыта в 1970 г.

Кафедра теоретической кибернетики (зав. – проф. Ю. Г. Дмитриев). Открыта в 1970 г.

Кафедра теории вероятностей и математической статистики (зав. – проф. А. А. Назаров). Открыта в 1974 г.

Кафедра высшей математики и математического моделирования (зав. – проф. В. В. Конев). Открыта в 1970 г.

Кафедра программирования (зав. – проф. А. Ю. Матросова). Открыта в 1970 г.

Кафедра защиты информации и криптографии (зав. – проф. Г. П. Агибалов). Открыта в 1999 г.

Вычислительный центр (нач. – Б.И.Савинков). Открыт в 1985 г.

Направления и специальности: «прикладная математика и информатика» (010501), «математические методы в экономике» (080116), «компьютерная безопасность» (090102). Научные направления, развиваемые коллективом преподавателей факультета, и основные полученные результаты посвящены глобальным проблемам кибернетики: оптимизация извлечения, переработки и использования информации.

Кадровый состав: 55 преподавателей, их них 17 профессоров – докторов наук, 28 доцентов–кандидатов наук, в аспирантуре обучается 31 человек.

Факультет в 2007 г.

В 2007 г. факультет прикладной математики и кибернетики реализовал следующие мероприятия по Инновационной образовательной программе.

1. Модернизация аудиторного фонда

Отремонтированы компьютерные классы ФПМК (ауд. 206, 208, 210, 217, 212-а 2-го учебного корпуса ТГУ).

2. Материально–техническое оснащение

В компьютерных классах ФПМК установлена новая мебель, произведено дооснащение этих классов 15 современными компьютерами.

3. Создание новых специализаций

Реализована новая специализация «анализ безопасности компьютерных систем» в рамках существующей специальности «компьютерная безопасность». Разработаны программы дисциплин: 1) Языки безопасного программирования, 2) Криптографически защищенные операционные системы, 3) Безопасные распределенные вычисления, 4) Защита в ОС, 5) Защита в компьютерных сетях, 6) Защита баз данных.

4. Разработка программного обеспечения, включающая электронные образовательные ресурсы, учебно-методические комплексы, автоматизированные информационные системы

1. Параев Ю.И. Теория оптимального управления.

2. Смагин В.И. Численные методы.

3. Горцев А.М. Комплекс обучающих программ “Оптимизация” для выполнения лабораторных работ.
4. Назаров А.А. Теория случайных процессов.
5. Терпугов А.Ф. Имитационное моделирование.
6. Матросова А.Ю. Дискретная математика.
7. Матросова А.Ю. Тестирование программного обеспечения.
8. Матросова А.Ю. Сортировка и поиск данных: методы и алгоритмы.
9. Останин С.А. Базы данных.
10. Седов Ю.В. Ассемблер для Linux.
11. Седов Ю.В. Интернет программирование.
12. Тимошевская Н.Е. Элементы комбинаторики и комбинаторные алгоритмы.
13. Панкратова И.А. Теоретико-числовые методы в криптографии.
14. Агибалов Г.П. Избранные теоремы начального курса криптографии.
15. Агибалов Г.П. Лекции по математической логике и теории алгоритмов.

5. Развитие кадрового потенциала факультета в области ИКТ

Восемнадцать преподавателей ФПМК прошли повышение квалификации в области ИКТ.

По результатам повышения квалификации, в частности, проделана следующая работа:

- новые результаты в области ИКТ включены в дисциплины “Верификация программного обеспечения” и “Графовые представления булевых функций”;
- новые результаты в области контролепригодного проектирования включены в дисциплины “Диагностика дискретных устройств” и “Дополнительные главы дискретной математики”;
- модернизация курса лекций по дисциплине “Булевы функции в криптографии”.

6. Выполнение НИР «Исследование, разработка и реализация математических методов обеспечения компьютерной безопасности и создание на их основе криптографически защищенной операционной системы» (науч. рук. Г.П.Агибалов)

Сформулирована политика безопасности, адекватная угрозам в системах выполнения коллективных проектов, и разработан проект криптографически защищенной ОС, реализующей эту политику. Проект осуществлен путем подходящей модификации ОС MINIX.



Выпускники-криптографы

Создан инструмент для разработки защищенных операционных систем, в которых, кроме основных функций по управлению вычислительным процессом, реализуется еще и заданная политика безопасности. В его составе три компонента: 1) интерпретируемый объектно-ориентированный язык программирования, поддерживающий механизмы метаклассов и асинхронного выполнения алгоритмов объектов; 2) интерпретатор этого языка и 3) служебная ОС, управляющая интерпретатором.

Имея эти средства, желающий спроектировать защищенную ОС сначала описывает ее основные функции

на данном языке, затем с помощью механизма метаклассов присоединяет к этому описанию алгоритмы требуемой политики безопасности, после чего под управлением служебной ОС отлаживает полученное описание защищенной ОС путем его интерпретации и, наконец, отлаженный проект ОС отдает в производство или в эксплуатацию в режиме интерпретации. С помощью этой технологии разработана демоверсия защищенной ОС.

Результаты исследований опубликованы в:

1. Куликов М.Л., Ромашкин Е.В., Стефанцов Д.А. О разработке криптографически защищенной ОС для безопасного выполнения коллективных проектов // Вестник Томского государственного университета. Приложение. – 2006. №17. С.161–167.

2. Куликов М.Л., Ромашкин Е.В., Стефанцов Д.А. Разработка средств моделирования политик безопасности операционных систем // Вестник Томского государственного университета. Приложение. – 2007, № 23. С. 189–193.

Запланированные мероприятия по инновационной образовательной программе факультетом выполнены.

*А.М.Горцев,
декан ФПМК*