

# КАФЕДРА КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

САНКТ - ПЕТЕРБУРГСКОГО  
ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА  
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ

## ОБЩАЯ ИНФОРМАЦИЯ

---

Созданная в 2001 году, Кафедра собрала специалистов ведущих вузов Санкт-Петербурга по теории кодирования, защите информации, а также по проектированию и разработке больших программных комплексов. Сотрудники Кафедры имеют большой опыт по работе в исследовательских и наукоемких проектах иностранных компаний, таких как Intel, EMC, HP, Siemens AG, Samsung, Nokia, Renault и др.

Аспиранты и лучшие студенты Кафедры участвуют в совместных проектах и научных разработках Кафедры. Ежегодно несколько студентов Кафедры проходят стажировку в зарубежных университетах и промышленных компаниях.

Кафедра выполняет совместные проекты с российскими и зарубежными организациями, проводящими работы в областях разработки программного обеспечения, кодирования, телекоммуникаций и различных аспектов информационной безопасности. За время работы кафедра выпустила сотни специалистов, подготовлено и успешно защищены более десяти кандидатских и три докторских диссертации.

До 2010 г. кафедра проводила подготовку специалистов по специальности 075400 «Комплексная защита объектов информатизации». Открыты магистерские программы: 23026 «Коммуникационные технологии», 230217 «Безопасность информационных систем», 210405 «Системы и сети Связи», «Защищенные телекоммуникационные системы». С общенациональным переходом на обучение по стандартам "Болонского процесса" Кафедра перешла с 2010 г. на двухступенчатую подготовку бакалавриат-магистратура по направлениям 090090 «Информационная безопасность», 210700 «Инфокоммуникационные технологии и системы связи» и 230001 «Информатика и вычислительная техника».

*Основные направления деятельности:*

- безопасность информационных систем;
- помехоустойчивое кодирование и телекоммуникационные технологии (передача, хранение и обработка информации);
- мультимедиа алгоритмы и приложения;
- разработка программных систем. системная интеграция и IT-консалтинг;
- разработка сервисов и программного обеспечения для мобильных устройств;
- оценка производительности программного обеспечения;

## БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

---

Исследование и разработка криптографических алгоритмов и протоколов, а также методов и средств защиты операционных систем и сетей.

*Направления исследований и разработок:*

- аудит безопасности систем и сетей;
- безопасность в беспроводных сетях;
- криптосистемы с публичным ключом;
- разделение секрета, пороговая криптография;
- аутентификация и электронная подпись;
- реализация алгоритмов и протоколов конфиденциальной связи;
- стеганография;
- разработка стандартов.

*Средства, стандарты, технологии:*

- HTTP/HTTPS, TLS/SSL, SSH, PGP, IEEE 802.11i
- RSA, DSS, DES, Rijndael, ГОСТ Р 34.10-94, ГОСТ Р 34.11-94, ГОСТ 34.19-2001
- OpenSSL, MS CryptoAPI, OpenCA, КриптоПро, Infotecs, VipNet
- ГОСТ Р ИСО/МЭК 15408-2-2002 («Common Criteria»)

*Примеры проектов:*

- 2010-2011 гг. Заказчик: EMC Corp. Анализ и адаптация системы RSA DLP под требования российского рынка и законодательства.
- 2009- ... Samsung Corp. Проведение исследований в области асимметричных систем ID-криптографии
- 2009 г. Заказчик: Банк ХХХ. Исследование информационной безопасности и оценка защищенности системы интернет-банкинга.
- 2008 г. Заказчик: компания ARGOS. Анализ, документирование и реинжиниринг модуля безопасности спец. системы связи (КСП КриптоПро и Infotecs)
- 2008 г. Заказчик: Администрация Петербурга. Анализ возможности передачи закрытых видео данных на мобильный телефон в режиме реального времени.
- 2006 г. Заказчик: ГОУ ВПО ГУАП. Полный цикл работ по разработке и реализации политики безопасности для АИС ГУАП. Разработка модулей аутентификации, разделения доступа, аудита, шифрования, установления соединения, протоколирования и т.д.
- 2004-2006 гг. Заказчик: Samsung Corp. Исследования алгоритмов безопасности в области сенсорных сетей, разделения доступа и др. Участие в подготовке стандартов IEEE 802.11 i/e/w, деятельность по подготовке патентов.
- 2004 г. Заказчик: Государственная компания. Разработка концепции безопасности для операционной системы ОС2000. Реализация отдельных ключевых элементов.
- 2004 г. Заказчик: Петроаэробанк (группа «ВЕФК»). Разработка и реализация иерархической схемы разделения доступа, аутентификации и создания безопасного соединения с банковской информационной системой.
- 2003 г. Заказчик: Частная компания. Разработка стеганографической системы скрытой передачи информации по открытому аудиоканалу.

## РАЗРАБОТКА И СОПРОВОЖДЕНИЕ ПРОГРАММНЫХ СИСТЕМ. СИСТЕМНАЯ ИНТЕГРАЦИЯ И IT-КОНСАЛТИНГ

---

Разработка, интеграция, внедрение и сопровождение комплексных программных и программно-аппаратных решений, в том числе:

- информационно-управляющих систем;
- автоматизированных систем управления;
- систем документооборота;
- систем сбора и обработки данных;
- телекоммуникационных систем;
- систем видеонаблюдения;
- комплексных решений по защите информации;

#### **Технологии Java2**

- Java EE: JSP, Servlets, JDBC, EJB, JMS, Struts
- Java SE: AWT, Swing, Java 2D, Java 3D, JMF, Java FX
- Сервера приложений - GlassFish, Tomcat, JBoss
- Среды разработки - IntelliJ IDEA, NetBeans

#### **Технологии Microsoft / .NET:**

- C#, CLR, CTS, CLS, MSIL, ADO.NET, ASP.NET
- C++ / WinAPI / MFC / ATL
- Среды разработки - MS .NET Studio 2005/ 2003 / 6.0

#### **Технологии WEB:**

- jQuery, GWT, PHP, AJAX, CGI, Perl, XML, XSLT, HTML, CSS
- Среды разработки - Zend Studio, NetBeans

#### **Технологии СУБД:**

- MySQL, PostgreSQL, MS SQL Server, MS Access
- Rational Rose, MS Visio

#### **Операционные Системы:**

- Windows, Linux (ASP, Gentoo, SLED, RHEL), FreeBSD

#### **Тестирование и профилировка:**

- Intel VTune, BoundsChecker, Valgrind, Mantis BugReport, SVN
- OpenMP, Platform-Oriented Compiling

#### **Языки программирования:**

- C (ANSI / GNU / Intel) / C++
- Java2
- C#
- Visual Basic
- JavaScript, VBScript
- PHP, Perl, Python
- TCL, AWK
- SQL

#### **Исследовательское ПО:**

- MatLab, Mathcad, Simulink

- NS2, Opnet
- TeX / LaTeX

*Примеры проектов:*

- 2011 г. Веб-поддержка конференции ISIT 2011: [www.isit2011.org](http://www.isit2011.org)
- 2010-2011 гг. Заказчик: EMC Corp. Проект PANAMA. Исследование методов блочной обработки данных при выполнении в ОС Linux. Оптимизация ядра Linux для выполнения таких алгоритмов.
- 2009-2010 гг. Заказчик: ГОУ ВПО СП ГУВК. Внедрение Автоматизированной Системы Управления (АИС) «Университет» в Университете водных коммуникаций. Адаптация системы, разработка дополнительных модулей.
- 2009 г. Заказчик: Финско-Российская университетская программа в области телекоммуникации. Разработка веб-трекера проектов с подключением системы контроля версий.
- 2008 г. Заказчик: Администрация Санкт-Петербурга. Разработка web-ориентированной модуля «Рабочая Книга» для мониторинга общегородских показателей для Информационно-Аналитического Центра Администрации Санкт-Петербурга.
- 2008 г. Заказчик: Администрация Санкт-Петербурга. Разработка web-системы «Лидер» для визуального представления руководству Петербурга показателей по городу в целом и по районам.
- 2008. Заказчик: компания ARGOS. Разработка нового пользовательского интерфейса и уровня данных для клиентского приложения спецоператора связи.
- 2005-2007 гг. Заказчик: ГОУ ВПО ГУАП. Разработка и внедрение Автоматизированной Системы Управления (АИС) «Университет» - многопользовательского клиент/серверного комплекса для полной автоматизации внутреннего документооборота учебного заведения. Успешно внедрена (в эксплуатации с 2007 г.), награждена почетным дипломом Профессиональной премии в области информационной безопасности «Серебряный кинжал» по итогам 2008 года.
- 2004г. Заказчик: компания Magic Systems. Дизайн системы удаленного видеонаблюдения. Автомобилей.
- 2000-2003г. Заказчик: Петроаэробанк (группа «ВЕФК»). Глубокий реинжиниринг и расширение возможностей банковской информационной системы.

## РАЗРАБОТКА АППАРАТНЫХ СИСТЕМ И ПРОТОТИПИРОВАНИЕ

RTL дизайн (Verilog) и программно-аппаратная реализация информационных и телекоммуникационных систем. Архитектура микропрограммных средств на базе технологий Texas Instruments (DSP). Полный цикл разработки телекоммуникационных систем на базе ПЛИС/ЦСП (FPGA/DSP) платформ. Разработка средств для модулирования, тестирования и профилировки телекоммуникационного оборудования.

*Средства, стандарты, технологии:*

- RTL: Verilog, ModelSim, Questasim
- FPGA design on Xilinx and Altera devices including Virtex-5, Stratix-II, -III: Xilinx ISE, Altera Quartus
- Software: Matlab, C/C++
- Embedded processor design: Xilinx Microblaze, Altera Nios-II

- DSP processors implementation: TI DSP processors including latest multi-core devices, Code Composer Studio, DSP-BIOS operation system.

*Примеры проектов:*

- 2008 - ... г. Заказчик: Institute of Applied Radio Technology (IAF, Germany). Development of 3GPP LTE Air Interface Probe hardware system. Outsource project with Institute of Applied Radio Technology (IAF, Germany). The main aim of the project is to develop intelligence PHY layer diagnostic tool for modern 3GPP LTE wireless standard. The project is implementing on FPGA/DSP based hardware platform provided by customer (IAF).
- 2004 - 2009 гг. R&D project for Intel Corporation, Communication Technology Labs
  - 2008. Беспроводной экран. Аппаратная реализация кодера/декодера H.264 низкой сложностью для работы в реальном времени.
  - 2006. Разработка, дизайн и ПЛИС-прототипирование на платформе CrownPoint алгоритмов детектирования и борьбы с интерференцией.
  - 2005. ПЛИС-прототипирование высокоскоростных декодеров помехоустойчивых кодов.

## АНАЛИЗ И ВЕРИФИКАЦИЯ ПРОГРАММНЫХ СИСТЕМ

---

Анализ и профайлинг программных систем. Предсказание производительности и выявление потенциальных проблемных мест на ранних этапах проектирования. Создание модулей сложных вычислительных и компьютерных систем.

*Направления исследований и разработок:*

- анализ производительности распределенных систем;
- верификация и анализ надежности программного обеспечения;
- анализ надежности систем и стресс-тестирование;
- разработка распределенных протоколов: сенсорные сети, ad-hoc, p2p, smart spaces;
- средства отладки, тетирования и профилирования для Embedded Linux

*Примеры проектов:*

- 2010-2011. Заказчик: EMC Corp. Анализ и разработка эффективных алгоритмов управления очередью процессора и кэшем для перспективных платформ хранения и обработки данных.
- 2008-2009. Заказчик: Nokia Corp. Стресс-тестирование, портинание и разработка средств отладки для мобильных устройств на базе ОС Maemo Linux.
- 2006-2007. Заказчик: Siemens Corp. Разработка методов верификации и анализа производительности программного обеспечения.

*Средства, стандарты, технологии:*

- Software Verification, Performance Engineering, SPIN, Embedded Linux

## МОБИЛЬНЫЕ СЕРВИСЫ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

---

Исследования и разработка мобильных сервисов, используя новейшие технологии мобильного Web'a с ориентацией кросс-платформенные решения и мобильные виджеты. Лаборатория поддерживается компанией NOKIA, отчеты о исследованиях публикуются на семинарах FRUCT (Finnish-Russian University Cooperation program in Telecommunications).

*Направления исследований и разработок:*

- разработка мобильных виджетов;

- разработка информационных web-сервисов для мобильных;
- исследования в области location-based сервисов;
- исследования в области мобильного Web'a.

*Средства, стандарты, технологии:*

- SymbianOS, S60, Maemo Linux, Windows Mobile, UIQ
- Java2 ME, Python, MOAP, Web RunTime, WidSets

*Примеры проектов:*

- 2010-... Заказчик: Nokia Corp. Разработка кросс-платформенных мультимедийных приложений с использованием технологии QtQuick
- 2009-... Заказчик: Nokia Corp. Разработка энергоэффективных алгоритмов управления очередью для беспроводных мобильных устройства
- 2009-2010. Заказчик: Nokia Corp. Организация тренингов по разработке ПО для платформ Maemo и Symbian
- 2007-2008. Заказчик: Nokia Corp. Продвижение технологии Nokia Widsets в России. Разработка более 30 мобильных приложений (игровые, новостные и т.п.) с использованием технологии Nokia Widsets.

## ТЕЛЕКОММУНИКАЦИИ

---

### **Телеком: повышение эффективности функционирования физического уровня.**

Приложения помехоустойчивого кодирования и цифровой сигнальной обработки в различных областях телекоммуникаций.

*Направления исследований и разработок:*

- разработка и реализация помехоустойчивых кодеков (Reed-Solomon, concatenated Trellis-RS, LDPC, Turbo-code codecs);
- разработка моделей проводных и беспроводных систем передачи данных (IEEE 802.3an, 802.3ap, 802.11n (WiFi), 802.15 (Bluetooth), 802.16e (WiMAX), 3GPP/LTE);
- исследование и разработка аппаратных реализаций декодеров LDPC кодов;
- применение помехоустойчивого кодирования в системах мобильной связи;
- применение помехоустойчивого кодирования в системах оптической связи;
- применение помехоустойчивого кодирования при передаче по неэкранированной витой паре;
- разработка телекоммуникационных стандартов.

*Средства, стандарты, технологии:*

- GSM/GPRS/EDGE, UMTS, 3GPP/LTE
- IEEE 802.3an, IEEE 802.3ap, IEEE 802.11n, IEEE 802.16e, 802.15.3
- MNP, FEC, HARQ
- UDPFEC, транспортное кодирование

### **Телеком: методы повышения эффективности функционирования сетевого уровня**

*Направления исследований и разработок:*

- разработка методов маршрутизации для сетей, построенных на базе стандарта 802.16;

- разработка методов маршрутизации для сенсорных сетей.

### **Телеком: методы повышения эффективности функционирования MAC уровня**

*Направления исследований и разработок:*

- исследования в области теории систем случайного множественного доступа;
- анализ функционирования MAC уровня стандарта 802.11;
- анализ функционирования MAC уровня стандарта 802.16, методики выбора параметров протокола с учетом характеристик потока сообщений формируемого большим числом мобильных абонентов;
- анализ функционирования MAC уровня стандарта 802.15a/.3с (UWB, 60GHz);
- создание радиокompаса с использованием устройств стандарта 802.11.

### **Телеком: методы повышения эффективности функционирования транспортного уровня**

*Направления исследований и разработок:*

- разработка теоретических основ применения помехоустойчивого кодирования на транспортном уровне;
- конкретных схем кодирования на транспортном уровне;
- разработки теоретических основ применения методов случайного множественного доступа на транспортном и прикладном уровнях.

### **Телеком. Примеры проектов.**

- 2008. WiMax/WiFi. Разработка радио-компаса.
- 2007. Разработка помехоустойчивых кодов для Flash памяти
- 2007. Исследование отдельного класса помехоустойчивых кодов. Оценка применимости и возможностей патентования.
- 2007. Исследования схем пространственно-временного кодирования (MIMO): Space-time coding/Spatial multiplexing schemes. Advanced decoders.
- 2006. Разработка алгоритмов детектирования и борьбы с интерференцией.
- 2006. Разработка стандартов для WiMax-II. Исследования схем переменной избыточности HARQ (внесены предложения в комитет IEEE 802.16m).
- 2005-2006. Исследования помехоустойчивых кодов и сигнальной части для сл. поколения технологий WiFi и WiMax (адаптивный битлоадинг и LDPC коды)
- 2005. Разработка высокоскоростных декодеров помехоустойчивых кодов. ПЛИС-прототипирование.
- 2004. Разработка стандартов для физического уровня 10Gbit/s Ethernet (внесены предложения в комитет IEEE 802.3an)

## **МУЛЬТИМЕДИА АЛГОРИТМЫ И ПРИЛОЖЕНИЯ**

Создание приложений для сжатия, передачи и воспроизведения речевых, аудио и видео данных. Реализация мультимедиа проигрывателей, видеотелефонов и систем видеоконференций, а также устройств передачи видео для специальных задач.

Опыт реализации существующих стандартов, исследования и разработки новых методов сжатия для хранения и передачи цифровых изображений и фильмов

*Направления исследований и разработок:*

- исследования в области алгоритмов кодирования изображений и видео
- реализация видео, речевых и аудиокодеков;
- реализация стандартов;
- разработка новых методов сжатия;
- разработка систем видеоконференций;
- разработка стандартов;

*Средства, стандарты, технологии:*

- H.263, H.263+, H.264/AVC, H.264/SVC
- MPEG 1 / 2 / 4
- JPEG2000, JPEG, GIF, PNG
- JPEG-LS, CALIC
- JPEG2000
- MP3, Ogg Vorbis, AAC-PLUS
- T.120 - T.128, H.323, SIP, RTP, HTTP/HTTPS
- OpenCL - distributed computing on CPU and GPU (Graphics Processing Unit).

*Примеры проектов:*

- 2011 – ... Заказчик: Intel Corp. Проведение исследований в области алгоритмов пре- и пост-фильтрации, CPU/GPU(OpenMP) реализация.
- 2010 – ... Заказчик: Intel Corp. Проведение исследований в области распознавания жестов.
- 2010 – ... Заказчик: Intel Corp. Разработка библиотек алгоритмов обработка видео OpenCV и IPP.
- 2009 Заказчик: Intel Research Council. Разработка алгоритмов совместного кодирования источника и канала для беспроводных систем передачи видео низкого уровня сложности
- 2006-2008. Заказчик: Intel Research Council. Разработка алгоритма сжатия изображений низкой сложности для передачи видео в реальном времени. Комплексное сравнение с аналогами. Выбор профиля для последующей аппаратной реализации. Внесение предложений в патентный комитет.
- 2007. Заказчик: Частная компания. Разработка демо-стенда для показа преимуществ технологии транспортного кодирования при передаче видео в реальном времени по беспроводному каналу (WiFi)
- 2004. Заказчик: Intel Corp. Исследование перспективных алгоритмов сжатия изображений на базе векторного и кодового квантования.
- 2002 - 2003. Заказчик: компания SoftJoys. Реализация элементов корпоративной VoIP системы.
- 2003. Заказчик: Частная компания. Разработка стеганографической системы скрытой передачи информации по открытому аудиоканалу.
- 2002. Заказчик: LG Corp. Разработка кодков и плеера для воспроизведения видео через Internet в реальном времени.

---

## КОНТАКТНАЯ ИНФОРМАЦИЯ

- *Директор:* Крук Евгений Аврамович, д.т.н. проф.
- *Телефон:* +7 (812) 494-7052
- *Факс:* +7 (812) 494-7052
- *E-mail:* [ekrouk@vu.spb.ru](mailto:ekrouk@vu.spb.ru)
- *Адрес:*
  - 190000, Санкт-Петербург, ул. Большая Морская 67, ауд. 14-49
  - 190000, Санкт-Петербург, Московский пр., 149в
- *Контактное лицо:* Прохорова Вероника Борисовна
  - *тел.* +7 (812) 950-7139,
  - *e-mail:* [vb@vu.spb.ru](mailto:vb@vu.spb.ru).