3. *Лучинин В.В.* Нанотехнологии: физика, процессы, диагностика, приборы. – М.: Физматлит, 2006. – 552 с.
4. *Асеев А.Л.* Нанотехнологии в полупроводниковой электронике. – Новосибирск: Изд-во СО РАН, 2004. – 368 с.
5. *Неволин В.К.* Зондовые нанотехнологии в электронике. – М.: Техносфера, 2006. – 160 с.

УДК 681.324

Л.К. Бабенко, О.Б. Макаревич

ИССЛЕДОВАНИЯ ПО ПРОБЛЕМАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЮЖНОМ ФЕДЕРАЛЬНОМ УНИВЕРСИТЕТЕ И ИХ РЕАЛИЗАЦИЯ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

Как определено Концепцией защиты информации в Южном федеральном округе (ЮФО) одной из основных задач развития системы защиты информации является формирование и совершенствование структуры системы защиты в федеральном округе, развитие ее научно-технического и кадрового потенциала. Южный федеральный университет (ЮФУ), будучи одним из ведущих вузов страны, активно участвует во внедрении концепции в Южном федеральном округе.

По проблемам информационной безопасности (ИБ) в ЮФУ в настоящее время реализованы следующие структуры (рис. 1).

Южно-российский региональный центр по проблемам информационной безопасности в системе высшей школы	Факультет информационной безопасности в ТТИ ЮФУ, г. Таганрог
Лаборатория фундаментальных исследований проблем ИБ ИИРПУ КБНЦ РАН, г. Таганрог	Отдел защиты информации в НИИ физики ЮФУ, г. Ростов-на-Дону

Рис. 1. Структура подразделений по проблемам ИБ в ЮФУ

Основные работы по направлению «Информационная информация» проводятся в Технологическом институте Южного федерального университета в г. Таганроге (бывшем Таганрогском радиотехническом университете) рис. 2.

Работы по ИБ в ЮФУ ведутся в следующих направлениях:

- подготовка, повышение квалификации и переподготовка кадров;
- проведение исследований и разработок, направленных на внедрение в сфере науки и производства безопасных информационных технологий;
- аттестация и лицензирование технических средств защиты информации.

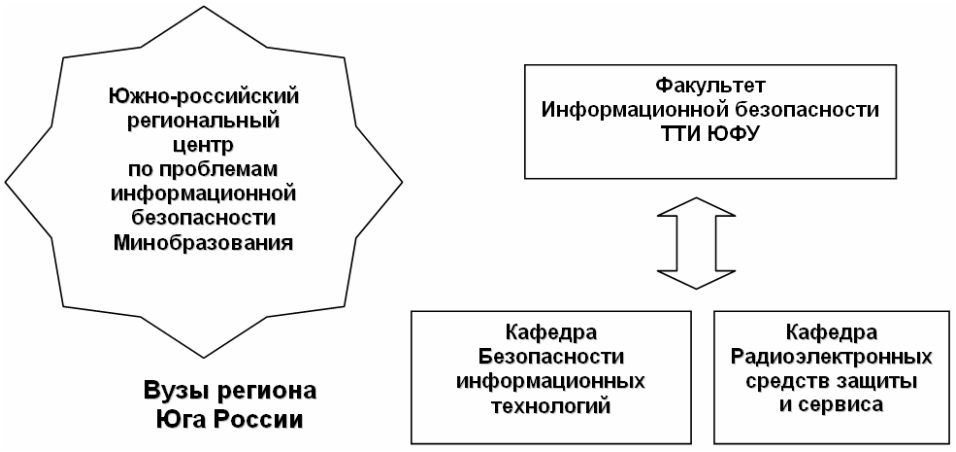

Рис. 2. Структурные подразделения ТТИ ЮФУ по ИБ

Информационная безопасность – это такая область, в которой невозможно обойтись без отечественных разработок. В рамках научных структурных подразделений ЮФУ ведутся фундаментальные и прикладные НИОКР. Ежегодно сотрудниками Южно-российского регионального центра по проблемам информационной безопасности и кафедры БИТ выполняется хоздоговорных и госбюджетных научно-исследовательских и опытно-конструкторских работ на сумму от трех до шести с половиной миллионов рублей.

Проводимые исследования охватывают широкий круг проблем. К ним относятся:

- защита от несанкционированного доступа к информационным ресурсам рабочих станций в локальных и глобальных сетях с использованием современных методов криптографии и разрабатываемых методов биометрической идентификации (аутентификации) пользователя «по голосу», по «отпечатку пальца», по клавиатурному подчерку, а также с использованием «интеллектуальных карт» и электронных брелков типа eToken;
- создание технологических, программных и программно-аппаратных средств выявления и обнаружения информационно-технических атак на объекты информационной сферы;
- повышение уровня защищенности информации при передаче в информационно-телекоммуникационных сетях общего пользования на основе применения средств стеганографии и разработка способов контроля скрытной передачи информации;
- разработка методического обеспечения и средств защиты информации от несанкционированного доступа, обрабатываемой в геоинформационных системах;
- исследование и выбор оптимальных инженерно-технических решений создания перспективного защищенного цифрового абонентского терминального оборудования для использования его в интеллектуальных системах (сетях) связи;
- разработка методов и средств управления доступом к данным, в частности, для геоинформационных систем с использованием сертификатов открытых ключей.

По всем рассматриваемым проблемам широким фронтом ведутся разработки как сотрудниками подразделений, так аспирантами и студентами. Результатами данных исследований являются новые алгоритмы, методы, методики, комплексы программ, а также оптимальные инженерно-технические решения по отдельным аппаратно-программным средствам, использование которых позволит решить многие проблемы в области защиты информации объектов информатизации. Все они опубликованы в статьях, доложены на конференциях и семинарах. Сотрудниками кафедры изданы три монографии: Новые технологии электронного бизнеса и безопасности / 2-е изд., доп. и перер. – М.: Радио и связь, 2002. – 512 с., Защита информации с использованием смарт–карт и электронных брелоков. – М.: Гелиос АРВ, 2003. – 352 с. и Алгоритмы «распределенных согласований» для оценки вычислительной стойкости криптоалгоритмов. – М.: Изд-во ЛКИ, 2008. – 112 с.

Научные исследования проводятся на современной аппаратуре и сертифицированном программном обеспечении.

Следует отметить, что многие сотрудники кафедры являются руководителями грантов Российского фонда фундаментальных исследований (РФФИ), всего же за период 1999 - 2008 гг. кафедра выполнила четырнадцать грантов РФФИ. Среди них: «Разработка системного программного обеспечения параллельных вычислительных систем на основе сетевых Internet/Intranet кластеров для решения задач моделирования», «Разработка и исследование методов и средств защиты информации в геоинформационных системах», «Исследование и разработка моделей, методов и средств обнаружения атак», «Исследование и разработка высокоточных методов и средств стегоанализа», «Организация и проведение научно-практических конференций по информационной безопасности».

Трое молодых сотрудников кафедры выиграли молодежные гранты РФФИ. Каждый год мы имеем от 40 до 50 публикаций по тематике «Защита информации».

Все вышесказанное подтверждает наличие на кафедре научной школы, способной вести подготовку специалистов высшей квалификации. Таким образом, исследовательская, опытно-конструкторская работа и научные публикации являются приоритетными задачами персонала кафедры.

Все результаты научных работ используются в учебном процессе при чтении лекций и проведении лабораторных и практических занятий.

Так, например, создан лабораторный практикум по изучению возможностей и приобретению практических навыков разработки приложений с использованием смарт-карт ASE фирмы Athena Smartcard Solutions Ltd [1]. Интегрированная программная среда ASESoft служит для создания приложений на смарт-карте ASE и состоит из двух уровней.

Первый (нижний) уровень предназначен для обмена данными с картами ASE-card и устройствами считывания карт ASE Drive, передачи потоков данных между программой и устройством ASE Drive, между устройством и картами.

Второй уровень (High Level Api) позволяет разработчику обмениваться данными с картой по протоколу ISO 7816-4, управлять состоянием ридера и карты, позволяет сформировать пакет данных, распознаваемых ридером, проверить ответ на валидность, производить выполнение простейших операций над картой (доступ к данным, выбор идентификатора файла, получение служебной информации о карте), а также высокоуровневых команд (прочитать данные в пользовательский файл, создавать и управлять файлами, производить внутреннюю и внешнюю аутентификацию, операции сравнения и т.д.).

Типичное приложение, работающее со смарт-картами, использует следующую последовательность вызова функций:

1. Получение основной информации об устройстве ASEDrive.
2. Открытие устройства.
3. Вызов функций для проведения необходимых операций с картой.
4. После выполнения всех операций с картой, завершение сеанса работы путем закрытия устройства.

В лабораторном практикуме подробно рассматривается каждый из этапов, приводится подробное описание всех низкоуровневых и высокоуровневых функций, формулируются варианты заданий для выполнения студентами.

Предлагаемые задания связаны с разработкой приложений, которые проводили бы аутентификацию и авторизацию при использовании студентами смарт-карт в научно-технической библиотеке, при получении стипендии, в медицинском пункте.

Благодаря изучению смарт-карт ASE, как одного из современных средств защиты информации студенты приобретают навыки эксплуатации и разработки перспективных систем с использованием других интеллектуальных карт, электронных брелоков, аппартных ключей, которые еще только создаются [2].

Разработан лабораторный практикум по изучению методов и систем биометрической аутентификации [3]. Работа посвящена вопросам практического изучения функционирования, а также методов оценки характеристик биометрических систем. Программный комплекс текстонезависимой голосовой аутентификации (рис. 3) состоит из двух основных частей:

- подсистема регистрации пользователя;
- подсистема аутентификации пользователя.

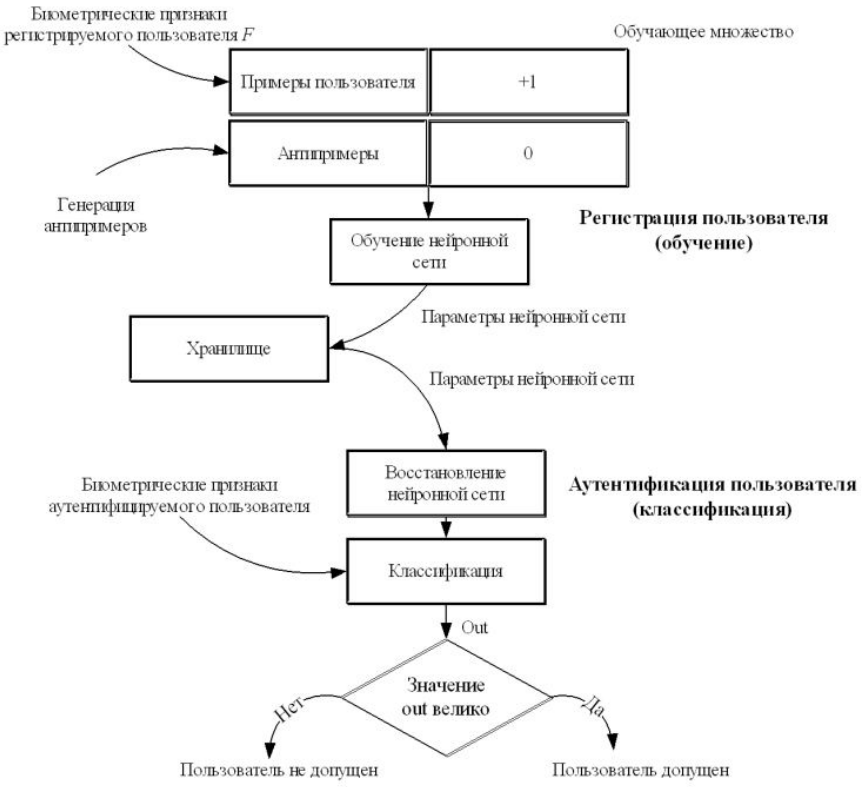

Рис. 3. Структура системы голосовой аутентификации

Для решения задач регистрации и аутентификации пользователя. использованы искусственные нейронные сети. Работа с программным комплексом состоит из следующих основных этапов:

1. Запись голоса регистрируемого пользователя.

2. Создание биометрического шаблона пользователя. Заключается в удалении пауз шумных участков речи, выделении биометрических параметров обучения искусственной нейронной сети с архитектурой многослойный персептрон.

3. Аутентификация пользователя на основе созданного ранее шаблона.

Студенты при выполнении работы практически реализуют все три этапа биометрической голосовой аутентификации, используя в качестве дикторов себя и своих коллег, строят графики распределений вероятностей, определяют ошибки первого и второго рода.

Благодаря проводимым на кафедре БИТ перспективным НИОКР по биометрическим методам аутентификации с использованием нейросетевых технологий студенты, магистранты, аспиранты и сотрудники имеют возможность глубоко изучать не только перспективные средства защиты информации, но и современный уровень теоретических основ информатики.

Разработан лабораторный практикум по изучению системы удостоверяющих центров для обеспечения взаимной аутентификации, для рассылки и проверки сертификатов открытых ключей, организации защищенной сетевой транзакции при регистрации пользователя и получении сертификата [4].

Так выглядит вкладка «Клиенты» в созданной лабораторной работе по системе удостоверяющий центр (рис. 4).

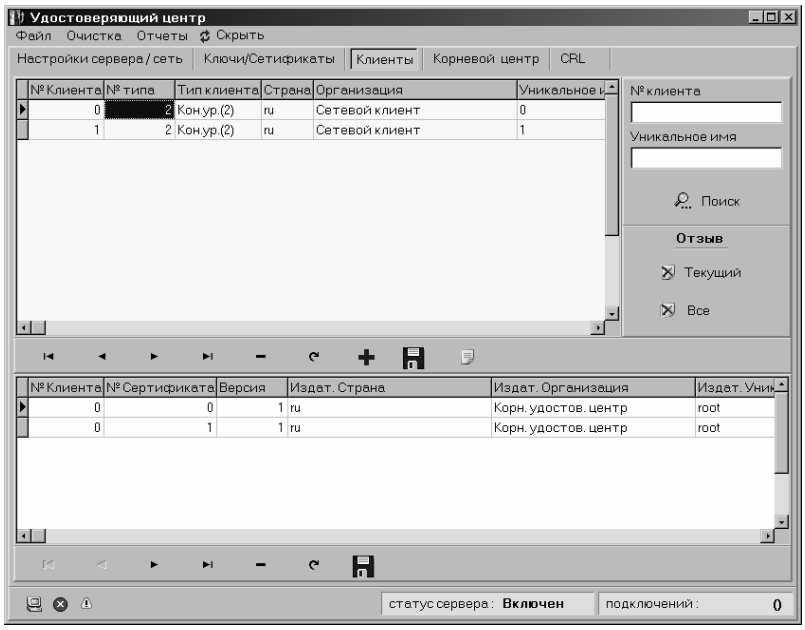

Рис. 4. Меню «Клиенты» в лабораторной работе по удостоверяющим центрам

Разработанный удостоверяющий центр (рис. 5) может выполнять следующие функции:

- ♦ хранение и выдачу сертификатов конечным пользователям и другим удостоверяющим центрам;

- проверку сертификатов по всей иерархии удостоверяющих центров (до корневого включительно);
- отзыв скомпрометированных сертификатов;
- организацию защищенной сетевой регистрации (получение сертификата) для конечных пользователей;
- создание разветвленной иерархии удостоверяющих центров любой конфигурации.

Цифровой сертификат – это набор данных, содержащий значение открытого ключа, информацию, идентифицирующую владельца и издателя сертификата, служебную информацию, а также электронно-цифровую подпись, сгенерированную удостоверяющим центром. Цифровой сертификат является механизмом распространения открытых ключей. Разработанная структура сертификата и методы его проверки отвечают рекомендациям X.509v3 – международнопризнанному формату инфраструктуры открытых ключей.

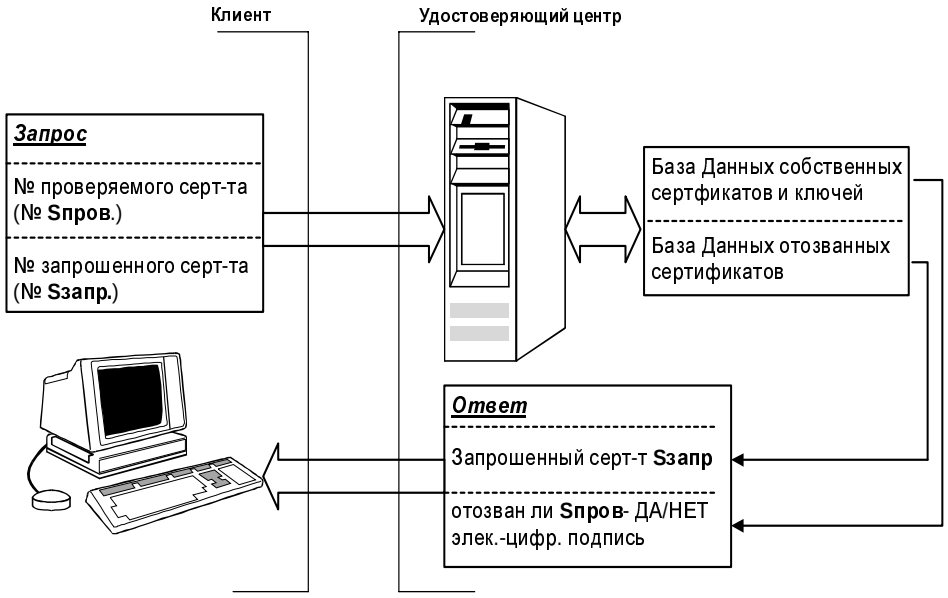

Рис. 5. Структура удостверяющего центра

Лабораторная работа состоит из 4 основных этапов:

1. Установка и настройка корневого удостоверяющего центра на отдельном компьютере в сети (уровень в иерархии = 0).
2. Установка и настройка подчиненного корневому удостоверяющего центра на отдельном компьютере в сети (уровень в иерархии = 0).
3. Установка и настройка клиентского приложения для проведения защищенной сетевой транзакции.
4. Проведение защищенных сетевых транзакций.

На основании знакомства с возможностями удостоверяющих центров, выполнения этапов лабораторной работы, реализуя перечисленные функции, студенты овладевают технологией инфраструктуры открытых ключей, современными протоколами аутентификации.

Разработано пять лабораторных работ, посвященных современным методам криптоанализа [4-8].

1. Изучение метода линейного криптоанализа применительно к алгоритмам шифрования, построенным по схеме Фейстеля.
2. Изучение метода дифференциального криптоанализа применительно к алгоритмам шифрования, построенным по схеме Фейстеля.
3. Изучение метода дифференциального криптоанализа применительно к многораундовым алгоритмам шифрования, построенным на основе сети SPN.
4. Изучение метода линейного криптоанализа применительно к многораундовым алгоритмам шифрования, построенным на основе сети SPN. Изучение метода слайдовой атаки на примере алгоритмов шифрования, построенных по схеме Фейстеля.

Разработанные лабораторные работы отвечают следующим требованиям:

- обладают похожим интуитивно понятным интерфейсом;
- запрашивают все необходимые сведения о студенте содержат не менее 10 вариантов индивидуальных заданий;
- позволяют проверить правильность проведенного анализа..

Для выполнения работ использованы следующие учебные алгоритмы шифрования.

1. Учебный алгоритм шифрования, построенный по схеме Фейстеля.
2. Алгоритм шифрования, построенный по принципу сети SPN.
3. Алгоритм шифрования S_DES.

Первые два алгоритма разработаны авторами специально для проведения лабораторных работ, третий – позаимствован из литературы [10].

Интерфейсы программы для проведения лабораторных работ изображены на рис. 6.

Таким образом, на кафедре созданы предпосылки для изучения стойкости существующих и вновь создаваемых криптоалгоритмов.

Первые три лабораторные работы могут быть использованы для курсов: «Программно-аппаратные средства обеспечения информационной безопасности», «Программно-аппаратная защита информации» при обучении студентов специальностей 090103,090104, 090105.

Последние пять лабораторных работ могут быть использованы для курса «Криптографические методы и средства обеспечения информационной безопасности» при обучении студентов специальностей 090103,090104, 090105.

Благодаря оперативному использованию результатов НИОКР в учебном процессе студенты, магистранты, аспиранты и преподаватели могут легко осваивать современные средства защиты информации и повышать свою квалификацию в области программно-аппаратных средств и методов защиты, изучая на практике основные ее подсистемы: криптографическую, аутентификации, управления доступом, контроль целостности.

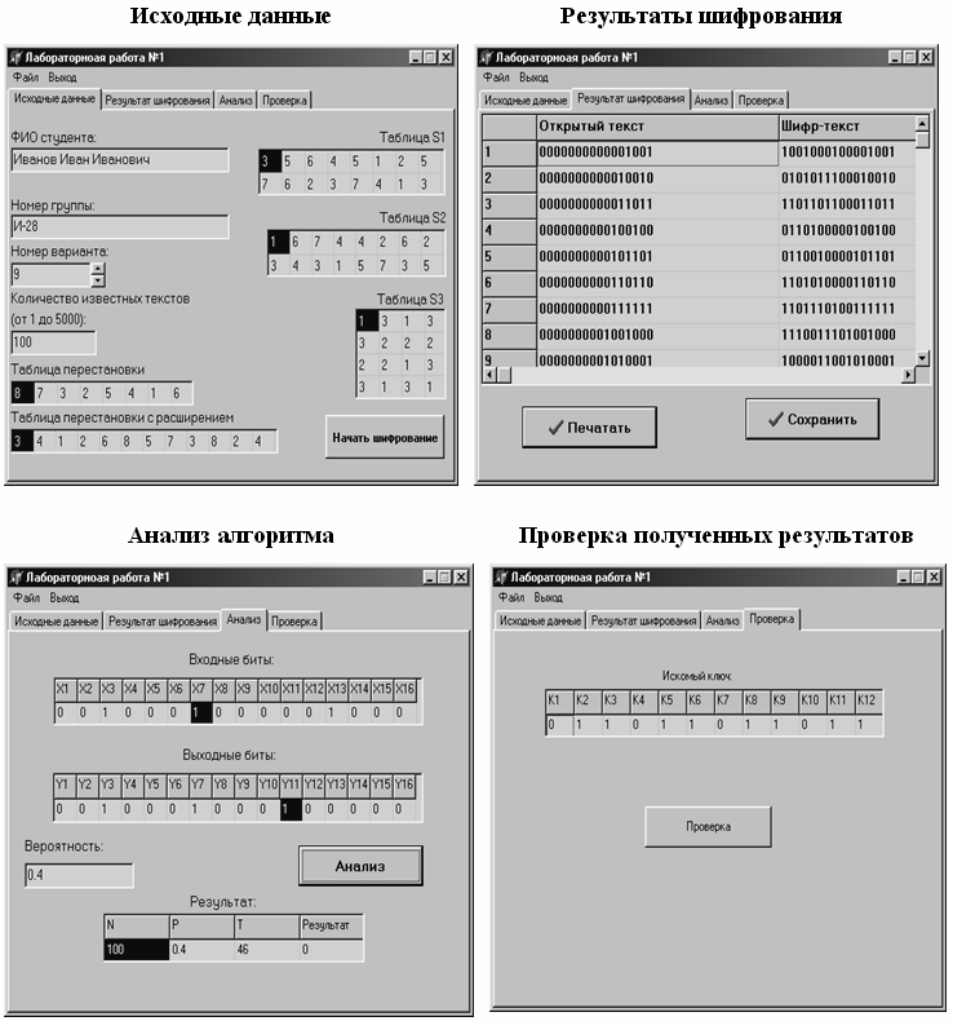

Рис. 6. Интерфейсы программы для проведения лабораторных работ

В первую очередь ЮФУ является кузницей по подготовке и переподготовке кадров, особо следует отметить проблему повышения квалификации. Университет готовит специалистов по трем специальностям направления 090100 Информационная безопасность» [11]. В настоящее время на факультете «Информационной безопасности» ежегодно обучается более 1000 студентов по специальностям:

- 090103 – Организация и технология защиты информации;
- 090104 – Комплексная защита объектов информатизации;
- 090106 – Информационная безопасность телекоммуникационных систем;
- 210403 – Защищённые системы связи.

Страна уже получила около 900 специалистов, из них 140 имеют дипломы с отличием. Наши выпускники работают в государственных организациях и учреждениях, банках, частных фирмах, в силовых структурах. Распределение молодых специалистов пока не вызывает затруднений, 80% их них работают по специальности. Подготовка кадров в субъектах ЮФО приведена в таблице.

Таблица

Подготовка кадров по ИБ в ЮФО

№	Субъект ЮФО	Вуз	Специальность	Кол-во обучающихся студентов	Кол-во выпущенных специалистов
1 2 3 4 5	Ростовская обл. Ставропольский край Краснодарский край Астраханская обл. Волгоградская обл.	12 вузов	Все специальности, кроме 090101 и 090107	3310	1940

Нет специальностей по направлению «Информационная безопасность» в вузах: Кабардино-Балкарии, Северной Осетии, Дагестана, Калмыкии, Чеченской республики, Адыгеи.

Комплексная система подготовки кадров в Технологическом институте ЮФУ (2000-2008 г.г.), в том числе и высшей квалификации, показана на рис. 7.

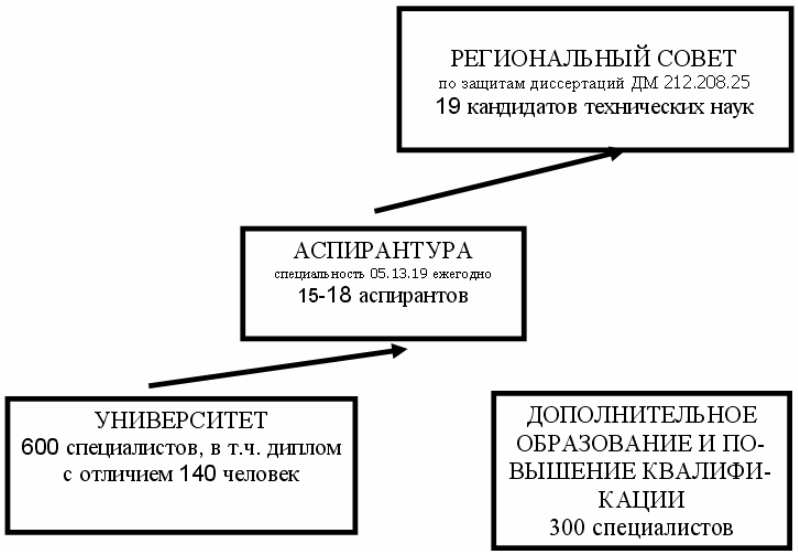

Рис. 7. Комплексная система подготовки кадров в ТТИ ЮФУ

Следует отметить, что в совете по защите диссертаций в 2005-2008 гг. защитились 19 соискателей по специальностям 051319 «Защита информации и информационная безопасность» и 052505 «Информационные системы и процессы». Подготовка кадров напрямую связана с проблемами квалификации «учителей» и наличием современной лабораторной базы. В этом плане в ЮФУ все в порядке: на факультете информационной безопасности работает восемь докторов наук и более 30 кандидатов, за последние два года приобретено оборудования на 40 млн рублей.

Большая роль в организации совместных работ и координации деятельности кафедр, факультетов и структурных подразделений вузов региона Юга России принадлежит Южно-Российскому региональному учебно-научному центру (РУНЦ) ЮФУ по проблемам информационной безопасности в системе высшей школы, созданном приказом по Минвузу от 20.08.97 г. №1781 (рис. 8). Центр участвует в разработке, формировании и реализации научно-технических и учебных программ органов государственной власти и местного самоуправления в области проблемных и прикладных проблем ИБ. Основные задачи РУНЦ по ИБ:

- создание комплексной системы регионального уровня по подготовке, повышению квалификации и аттестации кадров всех уровней квалификации в области информационной безопасности;
- организация, подготовка и проведение методических семинаров, конференций;
- проведение исследований и разработок по ИБ в интересах региональных структур;
- подготовка и издание учебной, научной и методической литературы по ИБ.

Рис. 8. Структура и задачи Южно-Российского регионального учебно-научного центра по проблемам информационной безопасности в системе высшей школы ЮФУ

Решением Совета по безопасности при представителе Президента в Южном федеральном округе на Центр возложены функции окружного Центра по обучению и повышению квалификации. С таким же предложением выступил Совет по безопасности при Губернаторе Ростовской области, при этом Центр ЮФУ должен функционировать как в Таганроге, так и в Ростове. За последние три года курсы повышения квалификации окончили 70 сотрудников Администрации Ростовской области, 30 специалистов Пенсионного фонда РФ, сетевые администраторы Русславбанка и его филиалов, преподаватели вузов Южного региона. Дипломы о дополнительном образовании по специальности «Организация и технология защиты информации» получили более 300 выпускников других кафедр ЮФУ.

Одной из существенных задач в настоящее время является создание **ЦЕНТРА коллективного пользования**, оснащенного современной аппаратурой и программным продуктом, для проведения обучения студентов, преподавателей и специалистов ЮФО.

Взаимодействие РУНЦ ЮФУ с субъектами Южного федерального округа осуществляется через:

- обучение в ТТИ ЮФУ филиалы по направлению ИБ 090100;
- семинары повышения квалификации по ИБ для преподавателей вузов ЮФО (университеты Ставрополя, Нальчика, Ростова, Махачкалы, Элисты, Новочеркасска, Астрахани и др.);
- целевую аспирантуру (из университетов Нальчика, Майкопа, Махачкалы).

В работе регионального диссертационного докторского совета по специальности 051319 участвуют профессора из университетов Ростова, Нальчика, Ставрополя, Краснодара. На научно-практических конференциях по ИБ участвуют практически все университеты ЮФО. Наши профессора участвуют в работе ГЭК университетах Южного региона. (СГУ – Ставрополь, КГУ – Краснодар, ВГУ – Волгоград). Ведутся совместные работы по грантам РФФИ (КБГУ – Нальчик).

Таким образом, Южный федеральный университет своей деятельностью в области информационной безопасности активно содействует выполнению задач, обозначенных в Концепции по защите информации в Южном федеральном округе. Определенный вклад при этом вносит лаборатория фундаментальных проблем информационной безопасности ИИПРУ КБНЦ РАН, функционирующая в составе ТТИ ЮФУ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Бабенко Л.К., Зорина Д.А., Юрков П.Ю.* Лабораторный практикум по изучению возможностей и приобретению практических навыков разработки приложений с использованием смарт-карт ASE фирмы Athena Smartcard Solutions Ltd. . – Таганрог, ТРТУ, 2004. – 53 с.
2. *Бабенко Л.К., Ищуков С.С., Макаревич О.Б.* Защита информации с использованием смарт-карт и электронных брелков. – М.:ГелиосАРВ, 2003. – 352 с.
3. *Бабенко Л.К., Тумоян Е.П., Юрков П.Ю.* Лабораторный практикум по изучению методов и систем биометрической аутентификации. – Таганрог, ТРТУ, 2004. – 14 с.
4. *Бабенко Л.К., Басан А.С.* Лабораторный практикум по изучению системы удостоверяющих центров. . – Таганрог, ТРТУ, 2004. – 30 с.
5. *Бабенко Л.К., Ищукова Е.А.* Изучение метода линейного криптоанализа применительно к алгоритмам шифрования, построенным по схеме Фейстеля. – Таганрог, ТРТУ, 2004. – 21 с.
6. *Бабенко Л.К., Ищукова Е.А.* Изучение метода дифференциального криптоанализа применительно к алгоритмам шифрования, построенным по схеме Фейстеля. – Таганрог, ТРТУ, 2004. – 15 с.
7. *Бабенко Л.К., Ищукова Е.А.* Изучение метода дифференциального криптоанализа применительно к многораундовым алгоритмам шифрования, построенным на основе сети SPN. – Таганрог, ТРТУ, 2004. – 24 с.
8. *Бабенко Л.К., Ищукова Е.А.* Изучение метода линейного криптоанализа применительно к многораундовым алгоритмам шифрования, построенным на основе сети SPN. – Таганрог, ТРТУ, 2004. – 24 с.
9. *Бабенко Л.К., Ищукова Е.А.* Изучение метода слайдовой атаки на примере алгоритмов шифрования, построенных по схеме Фейстеля. – Таганрог, ТРТУ, 2004. – 24 с.
10. *Столлингс В.* Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 670 с.
11. *Захаревич В.Г., Макаревич О.Б.* Реализация в Таганрогском государственном радиотехническом университете концепции «Исследовательский университет» по сквозной подготовке специалистов всех уровней в области информационной безопасности. Проблемы образования в области информационной безопасности. Сборник трудов межвузовской научно-методической конференции. Москва, 17-18 ноября 2004 г. – М.: ИКСИ Академии ФСБ России, 2004. – С.48-56.