УДК 681.322

Ю.А. Брюхомицкий, О.Б. Макаревич

ОБЗОР ИССЛЕДОВАНИЙ И РАЗРАБОТОК ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

по материалам докладов XI Международной научно-практической конференции «Информационная безопасность»

Дается выборочный обзор наиболее интересных и значимых работ российских специалистов, отражающих основные тенденции развития информационной безопасности в России. Обзор выполнен по материалам XI Международной научно-практической конференции «Информационная безопасность», которая состоялась 22-25 июня 2010 года в России, г. Таганроге.

Информационная безопасность; комплексная защита объектов; информационные процессы; защита телекоммуникаций; криптография и стеганография; подготовка специалистов.

Y.A. Bryukhomitsky, O.B. Makarevich

REVIEW OF RESEARCH AND DEVELOPMENT INFORMATION SECURITY

based on reports XI International Scientific and Practical Conference "Information Security"

We give a selective overview of the most interesting and significant works of Russian-ray specialists, reflecting the main trends in information security in Russia. Survey carried out on materials of the XI International Scientific and Practical Conference "Information Security", which states 22-25 June 2010 in Russia, Taganrog.

Information security; comprehensive protection facilities; informational processes, the protection of telecommunications, cryptography and steganography; training.

XI Международная научно-практическая конференция «Информационная безопасность» состоялась 22-25 июня 2010 года в России, в г. Таганроге. В конференции приняли участие 320 отечественных и зарубежных специалистов, которые представляли 5 стран, 32 города, 75 организаций. В составе участников 34 доктора наук, 88 кандидатов наук, 30 аспирантов, 25 студентов. Материалы конференции представлены в 195 докладах, опубликованных в трех книгах [1-3].

Исследования по информационной безопасности, представленные на конференции российскими специалистами, сгруппированы в шесть направлений, соответствующих названиям секций:

1. Комплексная защита объектов информатизации.
2. Защита информационных процессов в компьютерных системах.
3. Защита телекоммуникаций.
4. Методы и средства криптографии и стеганографии.
5. Концептуальные, организационно-технические, правовые, экономические, гуманитарные аспекты информационной безопасности.
6. Подготовка специалистов по информационной безопасности.

* Работа выполнена при поддержке гранта РФФИ № 08-07-00117-а.

Данный обзор является выборочным и охватывает наиболее интересные и значимые работы российских специалистов, отражающие основные тенденции развития информационной безопасности в России.

1. Комплексная защита объектов информатизации. В рамках этой секции на конференции было представлено 36 докладов. Тематика докладов включает информационные, технические и организационные методы, способы и средства защиты как взаимосвязанную совокупность мер, направленных на комплексную защиту объектов информатизации. На секции широко представлен опыт разработки и практического применения средств защиты для различных категорий объектов информатизации.

В докладе А.А. Бурушкин, С.В. Соловьев, А.В. Ступников (ГНИИИ ПТЗИ ФСТЭК России, г. Воронеж) «Об актуальности разработки методического обеспечения построения комплексных систем защиты информации в системах электронного документооборота при интеграции разноплатформенных программно-технических средств» рассматриваются методические аспекты обеспечения безопасности информации в системах электронного документооборота и отмечаются сложности создания эффективной защиты при интеграции таких систем. Дается обоснование необходимости разработки методического обеспечения построения систем защиты информации в системах электронного документооборота органов государственной власти и рассматриваются возможные пути решения этой задачи.

Актуальные вопросы защиты персональных данных в медицинских учреждениях рассмотрены в докладе А.А. Захаров, Е.А. Оленников, И.А. Куриленко, Д.В. Сериков (ТГУ, г. Тюмень) «Модернизация информационных систем медицинских учреждений в соответствии с требованиями законодательства по защите врачебной тайны и персональных данных». Рассмотрены возможные подходы к оптимизации затрат, необходимых для приведения медицинских информационных систем (МИС) в соответствие требованиям законодательства по защите врачебной тайны и персональных данных. Предлагается использовать методы расчленения МИС на отдельные подсистемы, обезличивания и создания дополнительных компонентов, отвечающих за информационную безопасность.

Ряд докладов секции посвящен решению проблем побочных электромагнитных излучений и наводок средств вычислительной техники (ПЭМИН СВТ). В частности, в двух докладах В.П. Иванова (ФГУП СКБ ИРЭ РАН, г. Фрязино) «Информационная безопасность, проблема ПЭМИН, генераторы радиошума» и «Оценка возможности маскировки информативных наводок в отходящих цепях и инженерных коммуникациях с помощью генераторов шума» приведены результаты экспериментальных исследований ПЭМИН СВТ. Показана возможность приема ПЭМИН и восстановления информации. Предложен способ активной маскировки ПЭМИН СВТ с помощью широкополосных генераторов радиошума.

Проблемы ПЭМИН подняты также в докладе И.С. Петров (ЮУрГУ, г. Челябинск) «Оценка энергетической эффективности метода формирования маскирующих помех путем записи/воспроизведения сигналов ПЭМИ от СВТ». Автор приводит оценку эффективности метода формирования сигналоподобной маскирующей помехи с помощью цифровых технологий записи/воспроизведения радиосигналов.

Новый подход к описанию и моделированию разнородных систем безопасности на основе применения среды радикалов представлен в трех докладах специалистов из Ставропольского государственного университета и военного института связи. Это доклады: В.В. Копытов, В.В. Науменко (СГУ, г. Ставрополь) «Применение среды радикалов как подхода по описанию административных регламентов органов государственного управления»; В.В. Копытов, И.И. Яковлев (СГУ, г. Ставрополь) «Использование среды радикалов в моделировании сценариев раз-

вития ситуации в системах видеонаблюдения»; О.М. Лепешкин, С.А. Романов, Ю.П. Стоянов (СВИС, г. Ставрополь) «Разработка интеллектуальной надстройки над методами обнаружения и сопровождения объектов в видеопотоке на основе среды радикалов». Предлагаемый подход к описанию и моделированию разнородных систем безопасности реализуется с использованием среды радикалов, которая предполагает использование метода проб и ошибок, а именно: оснащение системы некоторым набором свободных элементов, предназначенных для конструирования таких проб. Под радикалом при этом понимается любая функциональная система, имеющая два доступных извне состояния: активное и пассивное.

Два доклада специалистов ЗАО ««Амулет»», г. Москва: Е.А. Миронов, А.С. Мосолов «Верификация систем видеонаблюдения»; А.С.Мосолов, О.В. Графова «Сравнение технологий проектирования» были посвящены вопросам моделирования, проектирования, настройки и эксплуатации современных систем охраны. В первом докладе рассматривается проблема настройки и проверки работы камер видеонаблюдения при их установке или обслуживании. Приводится краткое описание программного функционального модуля верификации (модуль инструментария САПР СКБ «Амулет»), его задач и результатов, которые получает эксперт при использовании модуля. Обозначено направление дальнейшего развития модуля. Во втором докладе рассмотрены существующие методы автоматизированного проектирования систем безопасности: запатентованные методики, их достоинства и недостатки. В задачи рассматриваемых методов входит автоматизация проектирования, анализ и оценка эффективности различных систем безопасности.

Системам охраны был также посвящен доклад В.Т. Корниенко, Л.П. Гиниятуллин (ТТИ ЮФУ, г. Таганрог) «Использование акустической голографии в системах видеонаблюдения оптически непрозрачных контролируемых объемов», в котором предлагается использование методов акустической голографии в системах видеонаблюдения охраняемых помещений при отсутствии оптической видимости. В работе также решаются задачи: учета качества акустического контакта с объектом, в том числе влияния реверберации звука; повышения разрешающей способности системы; выявления и выделения в изображении объектов иной природы, связанных с акустическими шумами; преобразования акустических волн и др.

В докладе В.Н. Скакунов*, А.В. Скакунов** (ВолГТУ, г. Волгоград*, ЗАО «ЕВРААС», г. Москва **) «Анализ интеграционного подхода к информационной безопасности» рассматривается современный подход к построению интегрированных систем обеспечения информационной безопасности. Определяется целесообразность интеграционного подхода к различным классам информационных систем, отмечаются сильные и слабые стороны такого решения.

Доклад Ю.А.Уварова (ООО «КиберПро», г. Курган) «Поддержка принятия решений в аудите информационной безопасности информационных систем персональных данных» посвящен актуальной проблеме поддержки принятия решений при аудите информационной безопасности автоматизированных систем обработки персональных данных. Показано, что автоматизация отдельных компонентов поддержки принятия решений при аудите информационной безопасности позволяет значительно повысить качество аудита и его эффективность.

Другой доклад по проблеме защиты персональных данных Г.Е. Шепитько, Е.С. Васильев (МФЮА, г. Москва) «Категорирование объектов информатизации, содержащих персональные данные» декларирует необходимость дробного категорирования объектов информатизации, содержащих персональные данные. Авторами найдены эмпирические зависимости для признаков такого категорирования. Показано, что большинство исследованных объектов имеют недостаточный уровень защиты персональных данных.

В докладе В.Л. Цирлов, О.В. Райков, (ЗАО «НПО ”Эшелон”», г. Москва) «Методика количественной оценки уязвимостей программного обеспечения объектов информатизации» предложен подход к количественной оценке уязвимостей и угроз информационной безопасности, основанный на теории нечетких множеств. Предложены показатели оценки уязвимостей.

В докладе М.И. Тенетко, О.Ю. Пескова (ТТИ ЮФУ, г. Таганрог) «Качественный анализ рисков информационной безопасности» рассмотрены особенности такого анализа, описан алгоритм анализа с помощью нечёткого логического вывода, представлены примеры работы алгоритма с категориями естественного языка.

2. Защита информационных процессов в компьютерных системах. В рамках этой секции на конференции было представлено наибольшее число докладов – 68. Тематика докладов весьма разнообразна и включает, в частности: методы и средства защиты локальных компьютеров и рабочих станций, функционирующих в составе корпоративных и глобальных сетей; вопросы обеспечения защиты от сетевых атак; методы и средства выявления аномалий в сетевой активности; методы и средства выявления злоупотреблений полномочиями со стороны легальных пользователей (инсайдеров); вопросы защиты программного обеспечения от недекларированных возможностей, несанкционированного изменения и управления; вопросы построения и использования персональных и биометрических средств идентификации личности и средств контроля доступа и др.

В докладе А.В. Барабанов, А.С. Марков, А.А. Фадин (ЗАО «НПО ”Эшелон”», г. Москва) «Оценка возможности выявления уязвимостей программного кода при отсутствии исходных текстов программ» исследованы особенности современных систем программирования для проведения аудита безопасности и сертификационных испытаний программ без наличия исходных текстов. Показана возможность выявления уязвимостей, закладок и ошибок, а также подготовки отчетов сертификационных испытаний.

В докладе А.Г. Ломако, М.А. Еремеев, В.А. Новиков (ВКА им. А.Ф. Можайского, г. Санкт-Петербург) «Метод выявления дефектов и недокументированных возможностей программ» представлены результаты разработки метода, позволяющего осуществлять восстановительную коррекцию программы после дизассемблирования ее исполняемого кода. Выполнен анализ существующих структурированных моделей формального описания семантики вычислений и методов исследования программ, позволивших представить модель восстановления функциональных спецификаций программ как систему взаимосвязанного доказательного, верификационного и тестового программирования, на основе которой предложен публикуемый метод.

В докладе В.И. Воробьев, Р.Р. Фаткиева, С.В. Перминов (СПИИ РАН, г. Санкт-Петербург) «Применение онтологического моделирования для поиска информационных аномалий» рассматривается технология построения системы оценки информационных рисков, проводимой в условиях дефицита исходных данных. Описывается алгоритм, позволяющий работать с неполной, неточной и нечисловой информацией и его параллельная организация на вычислительном кластере. Отмечается необходимость перехода от локального продукта и индивидуального использования к клиент-серверной технологии.

В докладе С.Д. Жилкин (НИЯУ «МИФИ», г. Москва) «Результаты применения алгоритмов моделирования программного обеспечения с целью выявления аномалий поведения» для решения задач обнаружения недекларированных возможностей программного обеспечения и прочих аномалий поведения предлагается использование подхода, основанного на построении модели поведения программного обеспечения.

В докладе В.В. Игнатов (ОАО «Инфотекс», г. Москва) «Безопасность в распределенных компьютерных сетях на основе адаптивных P2P систем VPN» обсуждается построение виртуальных защищенных сетей (VPN) с использованием Peer to Peer (P2P) технологий. Предлагается наиболее надежное решение задачи безопасного взаимодействия двух компьютеров в распределенной сети, которое заключается в шифровании (расшифровании) трафика непосредственно источником (получателем) сообщения. Рассматриваемая технология организации виртуальной сети по сравнению со стандартными схемами VPN обеспечивает защиту от доступа злоумышленников любого типа IP-трафика на всех участках сети, включая локальную сеть.

В докладе Г.В. Карайчев, В.А. Нестеренко (ЮФУ, г. Ростов-на-Дону) «Применение весовых функций к методу адаптивных сеток при совместном использовании с методом распределения по IP-адресам» рассматривается метод выявления аномальной активности «без учителя» (адаптивное построение системы). При этом первичные данные о соединениях преобразуются методом главных компонент, а затем анализируются с использованием адаптивных сеток. Цель работы – повышение эффективности и снижение числа ложных тревог – достигается за счет использования метода весовых функций при совместном использовании с методом распределения по IP-адресам.

Три взаимосвязанных доклада авторов из ТТИ ЮФУ, г. Таганрог посвящены методике автоматизированного построения правил фильтрации сетевого трафика.

В первом докладе Д.В. Мордвин, Е.С. Абрамов, А.В. Андреев и И.Д. Сидоров «Методы автоматизации построения правил фильтрации сетевого трафика» рассмотрены основные проблемы построения правил фильтрации и предложена методика автоматизированного построения правил. В представленной методике определены модель сети, метод разработки правил разграничения доступа между узлами в модели, методы и алгоритмы расчета и оптимизации правил фильтрации для заданного разграничения доступа.

Во втором докладе тех же авторов «Метод и алгоритмы построения правил разграничения доступа между узлами сети» представлен основополагающий (в разработках авторов) метод для решения задачи – автоматизации процесса построения правил фильтрации сетевого трафика. Основная идея метода – расчет множества правил фильтрации на основе заданного множества правил разграничения доступа. Метод определяет принципы формирования множества правил разграничения доступа и принципы минимизации их количества.

В третьем докладе Д.В. Мордвин, Е.С. Абрамов, И.Д. Сидоров «Метод расчета субоптимального распределения правил фильтрации по сети для заданного разграничения доступа в сети» представлен ключевой метод решения задачи автоматизации процесса построения правил фильтрации сетевого трафика, призванный решать проблему распределения правил фильтрации между имеющимися межсетевыми экранами за приемлемое время. Метод гарантирует корректность конфигурации правил. В основу метода положено использование генетического алгоритма.

В докладе Е.П. Тумоян, Г.А. Евстафьев (ТТИ ЮФУ, г. Таганрог) «Метод идентификации по клавиатурному почерку для систем мобильного банковского обслуживания» предлагается архитектура системы аутентификации пользователей в системах мобильного банковского обслуживания, а также метод биометрической идентификации мобильных пользователей по клавиатурному почерку. Двухфакторная аутентификация, основанная на поведенческом биометрическом параметре, позволяет повысить безопасность доступа к счетам по сравнению с существующими системами.

Три взаимосвязанных доклада авторов Ю.А. Брюхомицкого и М.Н. Казарина (ТТИ ЮФУ, г. Таганрог) посвящены разработке: метода предварительного анализа исходных данных в биометрических системах клавиатурного мониторинга с целью выделения и учета наиболее информативных клавиатурных параметров; метода многосвязного представления биометрических параметров клавиатурного набора, который позволяет учитывать взаимное влияние событий клавиатуры; метода распознавания клавиатурного почерка на основе использования статистических оценок плотности распределения, сочетающего простоту и точность распознавания. Сбалансированное применение предложенных методов для определенных приложений и категорий пользователей позволяет снизить уровень шума во входных данных и повысить качество систем клавиатурного мониторинга.

В докладе С.Г. Данилюк*, В.Г. Маслов*, А.Б. Катаранов*, А.В. Ефимова**, (МОУ «Институт инженерной физики», г. Серпухов*, ЗАО «НПЦ ”ИРС”», г. Москва** «Выявление недекларированных возможностей программных средств на базе нечеткого ситуационного подхода» рассматривается принцип разработки анализатора исходных текстов программ на основе нечеткого ситуационного подхода. Подход реализуется путем введения набора параметрических показателей, которые описывают преднамеренные и непреднамеренные недекларированные возможности сертифицируемых программных средств.

В докладе А.Ф. Белый, С.М. Климов (ОАО «ЭКА», г. Юбилейный Московской области) «Алгоритм принятия решений по оценке функциональной устойчивости средств автоматизации в условиях компьютерных атак» рассмотрен способ оценки функциональной устойчивости средств автоматизации (СА) в условиях компьютерных атак, основанный на расчёте рисков обеспечения устойчивости функционирования СА по матрице рисков. Разработан алгоритм принятия решений по оценке функциональной устойчивости СА, позволяющий сделать выбор наилучших мер противодействия компьютерным атакам.

Доклад С.Н. Смирнов (ФГУП «СКЦ Росатома», г. Москва) «Анализ средств защиты данных от инсайдерских угроз в СУБД Oracle» посвящен решению задачи защиты данных автоматизированных информационных систем, построенных на основе СУБД промышленного уровня, от деструктивной деятельности инсайдеров. Возможность построения эффективных механизмов защиты показана на примере СУБД Oracle 11g.

В докладе А.А. Талалаев, И.П. Тищенко, В.П. Фраленко, В.М. Хачумов (РАН ИПС им. А.К. Айламазяна, г. Переславль-Залесский) «Эксперименты по нейросетевому мониторингу и распознаванию сетевых атак» рассматривается нейросетевой подход к выявлению сетевых атак, сочетающий достаточно высокую скорость обработки сетевого трафика и результативность в определении сетевых атак. Приведены результаты проведенных авторами экспериментальных исследований.

В докладе О.Н. Федорец (ФГУ «3 ЦНИИ Минобороны России», г. Москва) «Комбинированная система защиты программного обеспечения от несанкционированного использования» предложена система, реализующая как проверку подлинности, так и проверку целостности программного обеспечения и позволяющая перекрыть большинство угроз от несанкционированного использования программного обеспечения.

В докладе В.М. Федоров, Д.П. Рублев, Е.М. Панченко, О.Б. Макаревич (ТТИ ЮФУ, г. Таганрог) «Методы идентификации устройств записи CD/DVD-дисков» приведены результаты исследования возможности идентификации устройств записи CD/DVD по виброакустическим шумам, возникающим при считывании дисков на одном и том же устройстве считывания. Анализ записанных виброакустических шумов производился с помощью вейвлет-преобразования. На основании

проведенного исследования делается заключение, что при записи дисковых носителей CD/DVD возникают неоднородности в записанных данных из-за особенностей движения записывающей головки устройства. Такая неоднородная запись проявляется в шуме считывающей головки, причем имеет место смесь как шума от считывающей головки, так и от неоднородности записанных данных. В работе осуществлено разделение этих двух видов виброакустических шумов с помощью вейвлет-преобразования и проведена последующая идентификация с применением аппарата искусственных нейронных сетей.

В докладе Е.С. Степанова, И.В. Машкина, В.И. Васильев (УГАТУ, г. Уфа) «Разработка модели угроз на основе построения нечеткой когнитивной карты в проекции на топологию сети» на основе теоретико-множественно подхода предложено формализованное описание информационной системы, созданной в соответствии с основными принципами архитектуры безопасности, указанными ГОСТ. Предложен также подход к разработке модели угроз на основе построения нечеткой когнитивной карты в проекции на топологию сети. Проведенный авторами вычислительный эксперимент показал адекватность предложенного метода моделирования угроз для оценки риска нарушения информационной безопасности.

3. Защита телекоммуникаций. В рамках этой секции на конференции был представлен 21 доклад. Доклады охватывают проблематику защиты проводных, радио- и волоконно-оптических линий связи.

В докладе А.П. Жук, С.В. Баркетов, В.В.Сазонов (СВИС РВ, г. Ставрополь) «Вариант помехоустойчивой хаотической системы передачи информации» на основании общеизвестных подходов к повышению помехоустойчивости классических систем передачи информации, разработаны рекомендации по повышению помехоустойчивости хаотических систем передачи информации и вариант такой помехоустойчивой системы передачи информации.

Целью доклада А.П. Жук, Ю.С. Голубь, А.С. Иванов (СВИС РВ, г. Ставрополь) представлена «Методика стохастического формирования ансамблей дискретных ортогональных многоуровневых сигналов» является увеличение количества структур формируемых ансамблей дискретных ортогональных многоуровневых сигналов (АДОМС), обеспечивающих повышение структурной скрытности систем передачи информации с кодовым разделением каналов. Полученная методика позволяет повысить количество структур АДОМС по сравнению с известными методиками формирования АДОМС.

В докладе В.В. Котенко (ТТИ ЮФУ, г. Таганрог) «Решение задачи защиты телекоммуникаций при полной априорной неопределенности источника информации» предлагается подход к решению задачи защиты информации в каналах связи, основанный на применении теории виртуализации. Приведена теоретическая основа нового метода, отличительными особенностями которого являются возможность реализации двух каналов дешифрования и отсутствие ограничений на вид источника информации. На этой основе осуществлен синтез алгоритмов виртуального шифрования и дешифрования.

Доклад Е.И. Кротова (ЯГУ им. П.Г. Демидова, г. Ярославль) «Исследование влияния негауссовских помех на систему передачи информации с кодированием» посвящен решению задачи защиты кодированной информации от влияния негауссовских помех. Целью работы является исследование влияния негауссовских помех на систему связи с частотной манипуляцией при использовании различных кодов. Для этого решается задача выбора кодов, обеспечивающих наименьшую вероятность ошибки в условиях влияния негаусовских помех.

В докладе А.А.Кускова, А.А. Шелупанов, Р.В. Мещеряков, С.С. Ерохин (ТУСУР, г. Томск) «Оценка рисков информационной безопасности телекоммуни-

кационной системы» приведено описание метода оценки рисков на основе марковских случайных процессов. Определяются исходные данные, необходимые для процедур оценки. Прогнозирование состояний информационной системы помогает своевременно предпринимать необходимые меры по предотвращению угроз информационной безопасности и увеличению уровня защищенности тех или иных объектов защиты.

В докладе В.В. Гришачев, О.А. Косенко (РГГУ, г. Москва) «Мониторинг акустооптоволоконных каналов утечки для обеспечения безопасности информационных систем» обсуждается возможность обнаружения канала утечки акустической (речевой) информации в штатных волоконно-оптических коммуникациях путем контроля оптических излучений. Представленные модельные исследования подтверждают возможность реализации подобных схем выявления атаки даже с помощью непрофильного оборудования. Производство специализированного оборудования может более надежно решить проблему выявления подслушивания и помочь службам безопасности защищать речевую информацию в современных условиях быстрого распространения волоконно-оптических технологий связи.

В другом докладе тех же авторов «Оценка степени защищенности объекта информатизации по физическим параметрам каналов утечки» представлен сравнительный анализ методов практической оценки эффективности каналов утечки речевой информации на основе распознания речи и физических параметров прошедшего сигнала. Показано, что методы взаимно дополняют друг друга, повышают объективность оценки опасности канала утечки и выбора технических средств защиты.

В докладе А.Н. Кулаков, Е.Б. Маховенко (СПГПУ, г. Санкт-Петербург) «Криптографические методы обеспечения информационной безопасности на основе идентификаторов в широковещательных системах» предлагается разработка и аппаратная реализация на ПЛИС прототипа системы, обеспечивающей широковещательную передачу данных в условиях незащищенного канала. Для достижения высоких системных показателей эффективности предполагается использовать криптосистемы с открытым ключом на основе идентификаторов. Для эффективной реализации таких криптосистем отмечается необходимость оптимизации процедуры вычисления билинейного отображения.

В докладе А.Э. Маевский (ЮФУ, г. Ростов-на-Дону) «Аналог алгоритма Гурусвами–Судана для списочного декодирования специального класса алгебро-геометрических кодов» на основе метода Гурусвами–Судана списочного декодирования кодов Рида–Соломона построен алгоритм списочного декодирования произвольного кода из класса алгебро-геометрических кодов типа кодов Рида–Соломона. Алгоритм может быть использован для построения систем защиты информации от непреднамеренных помех, несанкционированного доступа, копирования, тиражирования.

В докладе В.Н. Максименко (МТУСИ, г. Москва) «Интеграция методов защиты информации и оценки качества услуг в сетях сотовой подвижной связи» обсуждаются вопросы взаимосвязи использования дополнительной услуги в сетях сотовой подвижной связи по определению местоположения терминала пользователя с необходимостью внедрения соответствующих методов защиты информации. В частности, информация о местоположении терминала должна быть защищена от неутвержденного раскрытия или использования. Таким образом, идентификация текущего местоположения терминала пользователя с заданными показателями качества (горизонтальная и вертикальная точность, время ответа) позволяет оператору сети использовать ее также для разработки инновационных методов защиты информации.

4. Методы и средства криптографии и стеганографии. В рамках этой секции на конференции был представлен 41 доклад по актуальным проблемам криптографии, криптоанализа, стеганографии, стегоанализа, включая методы, алгоритмы, методики, способы реализации.

Первая группа докладов секции относилась к области криптографии.

Доклад А.Т. Алиев, В.В. Асанов (ДГТУ, г. Ростов-на-Дону) «Схема разделения секрета на основе кодов Боуза–Чоудхури–Хоквингхема» посвящен разработке способа построения системы разделения секрета на основе использования кодов, исправляющих ошибки. Идея предложенного способа заключается в том, что сообщение кодируется кодом, способным исправить t ошибок. После чего закодированное сообщение разделяется между K пользователями с внесением в каждую из копий сообщения $t + x$ ошибок. В результате пользователи не имеют возможности самостоятельно восстановить сообщение, так как применение декодера к слову, содержащему более чем $t + \varepsilon$ ($\varepsilon < x$) ошибок, приведет к однозначно ложному декодированию. В качестве кодов, исправляющих ошибки, были выбраны коды семейства кодов Боуза–Чоудхури–Хоквингхема (БЧХ).

В докладе Ю.И. Бутов, О.П. Малофей, О.М. Лепешкин, В.В. Радионов, С.А. Романов (СВИС РВ, г. Ставрополь) рассматривается модель обмена данными для формирования общего ключа между корреспондентами в присутствии активного нарушителя, когда у корреспондентов отсутствуют какие-либо ключи для аутентификации переданных данных. Задача решается с помощью зашумляющих открытых каналов между корреспондентами и третьей стороной, тогда у активного пользователя каналы перехвата хуже, чем основные каналы между корреспондентами.

В другом докладе тех же авторов «Применение модели инициализации по открытым каналам связи в условиях имитовоздействия с обеспечением контролируемой зоны» рассматривается модель для решения задачи распределения последовательностей между корреспондентами с обеспечением меньшего различия между ними по сравнению с различием последовательностей между одним из корреспондентов и нарушителем. Данная задача решается применением зашумленного канала между корреспондентом и центром распределения случайной последовательности, а также обеспечением контролируемой зоны.

В докладе И.А. Калмыков, О.А. Кихтенко, А.В. Барильская (СевКавГТУ, г. Ставрополь) «Алгоритм нелинейного шифрования потока данных с операцией возведения в степень элементов расширенных полей Галуа» рассмотрен алгоритм и представлена структура устройства для вычисления индекса элемента поля Галуа на основе применения полиномиальной системы классов вычетов (ПСКВ). По мнению авторов, использование ПСКВ позволяет разрабатывать криптографические процедуры защиты информации, обладающие всеми достоинствами систем нелинейного шифрования, обеспечивающие реальный масштаб времени закрытия информации и операций, связанных со сложением, умножением, возведением в степень элементов расширенных полей Галуа, а также их различных комбинаций.

В докладе Ю.В. Косолапов, Е.С. Чекунов (ЮФУ, г. Ростов-на-Дону) «Симметричные кодовые криптосистемы на основе кодов в **Ф**-метриках» с целью повышения стойкости симметричных кодовых криптосистем рассматриваются помехоустойчивые коды в **Ф**-метриках и строится кодовая криптосистема на кодах в **Ф**-метрике Вандермонда. Вопрос о применении криптосистемы в **Ф**-метрике Вандермонда для одновременной борьбы с помехами и технической утечкой в настоящее находится пока в стадии исследования.

Доклад В.В. Мкртичян (ФГНУ «НИИ» Спецвузавтоматика»», г. Ростов-на-Дону) «Математическая модель схемы специального широковещательного шифрования, основанная на некоторых конкатенированных кодах» посвящен защите

легально тиражируемой цифровой продукции от несанкционированного распространения. Автором построена математическая модель схемы специального широковещательного шифрования на основе обобщенных кодов Рида–Соломона, специальным образом конкатенированных с кодами Адамара, и декодера Гурусвами–Судана. Построена программная реализация математической модели. Проведено исследование возможности ее применения в случае превышения допустимого числа членов коалиции злоумышленников.

Целью работы В.М. Деундяк, Ю.П. Кириллова (ЮФУ, г. Ростов-на-Дону) «Модификация криптоалгоритма Шамира для одного обобщения рюкзачной криптосистемы Меркля–Хеллмана» является криптоанализ некоторого обобщения классической рюкзачной криптосистемы Меркля–Хеллмана, полученного расширением алфавита. На основе модификации криптоалгоритма Шамира построен алгоритм, позволяющий по открытому ключу найти отмычку, с помощью которой удается во многих случаях расшифровывать криптограммы.

В докладе Л.К. Бабенко, И.Д. Сидоров, А.С. Кириллов (ТТИ ЮФУ, г. Таганрог) «Ускорение вычислений дискретного логарифма с помощью технологии CUDA» рассматриваются возможности дальнейшего ускорения реализации дискретного логарифмирования. Анализируется возможность применения технологии CUDA для ускорения вычислений на различных этапах. Рассматривается эффективная реализация необходимых арифметических операций. Приведены графики, построенные по результатам проведенных экспериментов.

В докладе Л.К. Бабенко, Е.А. Маро (ТТИ ЮФУ, г. Таганрог) «Алгебраический криптоанализ алгоритма шифрования ГОСТ 28147–89» описываются перспективы реализации алгебраических атак на алгоритм ГОСТ 28147–89, приводятся основные этапы криптоанализа, необходимые начальные данные для взлома, а также производится расчет вычислительной сложности атаки.

В докладе Л.К. Бабенко, Е.А. Ищукова (ТТИ ЮФУ, г. Таганрог) «Дифференциальный криптоанализ алгоритма ГОСТ 28147–89» рассмотрена стойкость отечественного стандарта шифрования данных ГОСТ 28147–89 к атаке на основе дифференциального криптоанализа. Показано, что существует ряд *S*-блоков замены, обладающих слабыми свойствами по отношению к дифференциальному криптоанализу. Использование таких блоков в алгоритме ГОСТ позволяет получать характеристики, обладающие довольно высокими вероятностями, которые можно использовать для проведения атаки. В качестве иллюстрации осуществлена атака на 12 раундов алгоритма ГОСТ, которая за несколько минут позволяет определить первый раундовый подключ шифрования.

Доклад В.А. Монарёв*, А.М. Лубкин** (ИВТ СО РАН*, СУТИ**, г. Новосибирск) «Эффективная атака на блочный шифр RC6» посвящен криптоанализу блокового шифра RC6. Предложенная атака основана на результатах Л. Кнудсена и В. Мейера и использует тест хи-квадрат. Схема атаки позволяет значительно уменьшить трудоемкость нахождения секретного ключа. Ранее известные варианты атак, основанные на тесте хи-квадрат, имеют значительно большую сложность.

В докладе В.А. Монарёв (ИВТ СО РАН, г. Новосибирск) «Новый статистический тест для проверки криптостойких генераторов случайных чисел» приведены результаты сравнения нового теста с тестами, предложенными Национальным институтом стандартов и технологий США. Показана его эффективность. Приведены результаты тестирования известных генераторов случайных чисел с помощью нового теста.

В докладе Д.В. Самойленко, О.А. Финько (КВВУ им. С.М. Штеменко, г. Краснодар) «Оценка помехоустойчивости криптосистемы, основанной на китайской теореме об остатках, для *n* каналов с шумом и имитирующим злоумыш-

ленником» представлена сравнительная оценка достоверности криптографической системы с индивидуальным (традиционным) методом контроля и криптографической системы, основанной на избыточном модулярном коде. Показано, что последняя имеет преимущество по имитирующим действиям криптоаналитика.

Большая группа докладов четвертой секциибыла посвящена вопросам стеганографии и стегоанализа.

В докладе А.Т. Алиев, ДГТУ, г. Ростов-на-Дону «Стеганографический метод синонимичных преобразований для текстов на русском языке» рассматривается метод скрытой передачи информации в осмысленных текстах на основе замены синонимов. Основной задачей является реализация данного метода для текстов на русском языке. Для решения данной задачи проводится анализ особенностей русского языка, строятся специальные словари синонимов для разных частей речи, предлагаются алгоритмы сокрытия и извлечения информации с учетом частотных свойств русского языка.

В докладе А.Т. Алиев, М.В. Киселев (ДГТУ, г. Ростов-на-Дону) «Стеганографический метод сокрытия информации в потоковых аудиоконтейнерах на основе амплитудной модуляции» решается задача повышения уровня скрытности при передаче стеганографических сообщений посредством аудиоканалов. Предлагаемый метод сокрытия информации путем незначительного изменения амплитуды сигнала осуществляет встраивание секретной информации не за счет изменения отдельных отчетов, как в известных методах, а за счет изменения амплитуды наиболее низкочастотной составляющей сигнала.

В докладе Е.Ю. Елтышева, А.Н. Фионов (СГУТИ, г. Новосибирск) «Построение стегосистем для изображений с помощью перестановок» предлагается метод сокрытия информации в растровых изображениях форматов BMP, PNG и др., использующих неискажающие методы сжатия. В отличие от известных аналогов, предлагаемый метод внедряет сообщение в растр путем незначительных перестановок соседних байтов яркостей. Проводится анализ и сравнение разработанного алгоритма с известными аналогами.

В докладе В.А. Михеев, М.М. Репин (ОАО «НИИ ”Кулон”», ОАО «Концерн ”ВЕГА”», г. Москва) «Способ многоконтейнерной стеганографической защиты информации с разделением исходного сообщения на части и множественной инкапсуляцией» проблема неэффективности современных стеганографических систем защиты информации объясняется зависимостью надёжности системы защиты от объёма встраиваемых данных в контейнер. Предложен способ, повышающий степень надёжности сокрытия информации с помощью множественной инкапсуляции и позволяющий расширить объём встраиваемых данных.

В докладе В.А. Монарёв (ИВТ СО РАН, г. Новосибирск) «Стегоанализ на основе методов сжатия» предложен новый метод стегоанализа для обнаружения скрытой информации в изображениях. Стегоанализ проводился для файлов с изображением в неискажающем формате (bmp, png, tiff и другие). Информация внедрялась в последние значащие биты (LSB-внедрение). Новый метод проверен на выборке из 3000 файлов. Показано, что он позволяет обнаруживать внедрение при 0,25 %-ном заполнении. Проведен сравнительный анализ с самыми известными методами.

В докладе И.В. Нечта, А.Н. Фионов (СГУТИ, г. Новосибирск) «Цифровые водяные знаки в программах на C/C++» предлагается внедрять водяные знаки путем небольших эквивалентных изменений исходных текстов программ. Предполагается, что такие знаки будут устойчивы к атакам на двоичные исполняемые файлы, при условии, что противник не будет иметь доступа к исходным текстам. Экс-

периментально получены данные об объеме внедряемой информации для типичных приложений Symbian.

В докладе С.Ю. Очимов (СибГУТИ, г. Новосибирск) «Базирующийся на сжатии данных эффективный метод стегоанализа аудиоданных стандарта WAVE» предлагается новый метод обнаружения скрытых сообщений в WAVE данных. Основная его идея заключается в том, что после внедрения сообщения в контейнер нарушается его статистическая структура, поэтому заполненный контейнер будет «сжиматься» хуже, чем исходный (незаполненный). Метод построен на сравнении коэффициентов сжатия исследуемого контейнера и его полностью заполненной копии. При сжатии контейнера использовались общедоступные программы для сжатия данных. Были введены несколько параметров, которые позволили регулировать значения ошибок на пустых и заполненных контейнерах. Метод может быть применён и к любым другим форматам, которые используют для уменьшения занимаемого объёма неискажающее сжатие. Приведены результаты работы метода на большой серии файлов, доказывающие его эффективность.

В докладе А.Н. Савченко (СГУ, г. Ставрополь) «Цифровые водяные знаки и стандарт кодирования JPEG 2000» обсуждаются проблемы внедрения цифровых водяных знаков. Предлагается алгоритм их внедрения, объединяющий операции кодирования и внедрения значащей информации в изображения. Процесс внедрения и извлечения проходит на лету во время сжатия и декомпрессии. Техника внедрения интегрирована в стандарт JPEG2000.

Один доклад этой секции С.Э. Бардаев, О.А. Финько (КВВУ им. С.М. Штеменко, г. Краснодар) «Многофакторная биометрическая криптография на основе пороговых систем» посвящен проблемам построения биометрических криптосистем. В работе предлагается принцип построения многофакторных биометрических криптосистем на основе пороговых (k, n)-схем разделения секрета по n биометрическим данным пользователей и один из возможных вариантов её реализации. Преимущества такого подхода заключается в существенном уменьшении вероятностей ошибок как 1-го, так и 2-го рода, за счет применения многофакторной биометрии. Отказ от необходимости хранения ключей между сеансами позволяет пользоваться такой системой неквалифицированному персоналу.

5. Концептуальные, организационно-технические, правовые, экономические, гуманитарные аспекты информационной безопасности. В рамках этой секции на Конференции был представлен 21 доклад.

В докладе В.П. Иванов (ВПО «ИСТЭК», г. Краснодар) «К вопросу о создании основания теории защиты информации как внутренне совершенной и внешне оправданной научной теории» в опоре на современные достижения философии, концепции современного естествознания, современного видения научной картины мира предложены основания теории защиты информации.

В другом докладе того же автора «Злоумышленник как целостное физическое Я» представлена система аксиом теории защиты информации, опора на которую позволяет выявить следствия и выводы теории защиты информации, а на практике – определить количественные характеристики злоумышленника.

В докладе И.В. Бондарь, В.В. Золотарев (СГАУ им. М.Ф. Решетнева, г. Красноярск) «Формирование метрик процесса защиты информации» предложена модель и методика представления системы защиты, используемая в качестве инструмента оценки защищенности информационной системы. Формирование метрик процесса защиты информации и методика расчета этих метрик, предложенные в работе, позволяют частично решить задачу поддержки принятия решений при анализе и синтезе систем защиты информации.

В докладе Н.В. Гришина (РГГУ, г. Москва) «Безопасность информации как источник эффективных управленческих решений» рассмотрено влияние качества информации на процесс управления принятием управленческих решений и качество таких решений. Автором делается вывод, что залогом принятия эффективного управленческого решения, которое лежит в основе успешной коммерческой деятельности, является обеспечение безопасности информации.

Доклад Г.А. Шевцова (РГГУ, г. Москва) «Современные технологии документооборота как инструмент системы управления и средство защиты циркулирующей в ней информации» был посвящен рассмотрению современных систем документооборота с точки зрения общего жизненного цикла сообщения (документа), который протекает в трех средах существования: социальной, аналоговой и электронной. Подчеркивается, что основной функциональной целью документа является его общественное использование. Именно социальная среда имеет дело со «знаниями» и «сведениями». Остальные две среды только с отображением информации в том или ином виде. Автор отмечает, что в настоящее время происходит значительный отрыв технологических процессов от потребности сообщения (документа) в управленческой среде.

В докладе В.Б. Авдеев, Д.В. Авдеева, А.В. Бердышев (ГНИИИ ПТЗИ ФСТЭК России, г. Воронеж) «Обоснование требований к средствам защиты электронной аппаратуры от террористических электромагнитных атак» предложен новый подход к обоснованию таких требований. Предложенный подход, в отличие от традиционного, в котором определяются критериальные уровни гарантированного деструктивного воздействия, основан на определении противоположных параметров – критериальных уровней отсутствия каких-либо существенных реакций на внешние воздействия, имеющих нелинейный катастрофический характер. Благодаря этому снижаются требования не только к генераторам-излучателям, но и к информационно-регистрирующей системе тест-объектов, которая должна достоверно фиксировать отсутствие сбоев в штатной работе объектов.

В докладе В.Б. Авдеев, Н.Г. Денисенко, С.А. Пырочкин (ГНИИИ ПТЗИ ФСТЭК России, г. Воронеж) «Использование импульсных и постоянных магнитных полей для уничтожения информации на магнитных носителях» приведены результаты исследования воздействий магнитных полей на магнитные носители информации. Результаты исследований, направленных на определение параметров магнитного поля и условий его воздействия на магнитные носители, позволяют сделать вывод о возможности высоконадежного уничтожения информации методом силового импульсно-магнитного воздействия, а также методом воздействия постоянным магнитным полем. Кроме того, полученные результаты позволяют перейти непосредственно к реализации устройств, обеспечивающих безопасное для оператора экстренное высоконадежное стирание информации, записанной на магнитных носителях различных типов.

В докладе М.А. Егоров, А.С. Марков ЗАО «НПО ”Эшелон”», г. Москва) «Актуальные вопросы защиты персональных данных» рассмотрены проблемные вопросы защиты персональных данных и предложены организационно-технические способы их решения. Отмечается, что предъявляемые требования к защите персональных данных не всегда просто реализовать и интегрировать в существующую систему оператора. Необдуманный подход к защите может привести к необоснованным затратам, нарушению бизнес-процессов, потере управляемости, отказу пользователей от применения механизмов защиты.

В докладе С.В. Зданович, А.П. Росенко (СГУ, г. Ставрополь) «Математическое моделирование процесса влияния факторов эмоционального состояния сотрудника на вероятность разглашения конфиденциальной информации» выявлены

зависимости показателя вероятности разглашения тайны от показателя степени важности каждого из рассматриваемых параметров эмоционального состояния. На основании проведенных исследований делается вывод о том, что в целом показатель эмоционального состояния оказывает значительное воздействие на вероятность разглашения конфиденциальной информации. Немаловажную роль играет также показатель коэффициента эмоциональной устойчивости сотрудника. В рамках рассматриваемой модели механизм формирования эмоциональной устойчивости сотрудника может рассматриваться в качестве средства противодействия воздействию дестабилизирующих факторов и в конечном итоге – способствовать повышению общего уровня защищенности информации.

Доклад Е.А. Папкова (ТТИ ЮФУ, г. Таганрог) «Информационное воздействие и информационная безопасность» ставит своей целью рассмотреть виды информационного воздействия на человека и способы уменьшения их влияния. Задачи проведенного исследования: сделать теоретический анализ источников информационного воздействия и описать способы уменьшения их влияния. Рассмотрены различные виды информационного воздействия, описаны объекты и субъекты воздействия, приведены способы уменьшения негативного влияния описанных видов воздействий.

В докладе Ю.А. Колесник, В.С. Компаниец (ТТИ ЮФУ, г. Таганрог) «Практические аспекты задачи обеспечения информационной безопасности средствами современных психотехнологий» обсуждается возможность использования психотехнологий при исследовании гуманитарных аспектов информационной безопасности: метода психозондирования и метода видеокомпьютерной диагностики. Описывается суть обсуждаемых методов, выделяются их достоинства и недостатки. Приводятся ссылки на результаты завершенного исследования.

6. Подготовка специалистов по информационной безопасности. В рамках этой секции на конференции было представлено 9 докладов, посвященных различным аспектам подготовки специалистов в области защиты информации.

Доклад Л.Е. Адамова, О.О. Варламов, Р.А. Санду, О.И. Огородников (УЦ МИВАР, МАДИ (ГТУ), ФГУП НИИР, г. Москва) «Системы защиты персональных данных: подготовка специалистов, практический опыт преподавания и проведения мероприятий по защите персональных данных и рекомендации по снижению рисков» посвящен проблемам обучения, консалтинга и выполнения работ по защите персональных данных. Имеющийся у авторов опыт обучения и оказания услуг по защите персональных данных показывает целесообразность выделения общих моментов в виде «Порядка организации обеспечения безопасности персональных данных». Этот Порядок применяют и в учебных программах, и при обучении, и при защите персональных данных. Качественное обучение студентов и работников уменьшает риски, позволяет выгодно обучать слушателей и повышает эффективность систем защиты персональных данных.

Другой доклад от той же группы организаций Р.А. Санду, О.О. Варламов, М.Л. Оверчук, А.Н. Владимиров «Подготовка специалистов по информационной безопасности и создание многомерной эволюционной прикладной автоматизированной информационной системы поддержки принятия решений для управления инновационными ресурсами в образовании» посвящен описанию экспертной системы управления инновационной деятельностью образования. Авторы отмечают, что, с одной стороны, подготовка специалистов по информационной безопасности должна быть актуальной во времени, так как объективно постоянно происходят изменения как в законодательстве, так и в возможностях программных и технических средств. С другой стороны, информационная безопасность является наукоемкой областью и обладает большим инновационным потенциалом. Поэтому все эти

сложные, часто противоречивые показатели и требования предлагается хранить и обрабатывать в рамках единого формализма с помощью экспертной системы "Многомерная эволюционная прикладная автоматизированная информационная система поддержки принятия решений для управления инновационными ресурсами" (МЭПАИС УИР) учреждений образования России. В работе проведен системный анализ проблем управления инновационными ресурсами с точки зрения технологий, моделей и методов организации баз данных и систем поддержки принятия решений.

В докладе В.С. Галяев (ДГИНХ, г. Махачкала) «О некоторых региональных особенностях подготовки специалистов в области информационной безопасности» обсуждаются наиболее опасные угрозы информационной безопасности в условиях региональных особенностей Республики Дагестан. В качестве основного класса таких угроз выделены внутренние инсайдерские угрозы. Предлагаются рекомендации по построению учебных планов подготовки специалистов по защите информации для наиболее эффективного противодействия данному типу угроз. В частности, в рамках вариативной части для вузов, реализующих подготовку специалистов в области информационной безопасности, рекомендуется ввести предметы «Психология» и «Социология». Это позволит выпускникам по месту работы более успешно противодействовать угрозам социальной инженерии, выявлять манипулируемых и обиженных сотрудников. Также в качестве отдельного курса предлагается введение дисциплины, посвященной методике разработки и реализации политики безопасности, что позволит существенно уменьшить риски, связанные с халатными инсайдерами, а также существенно снизить угрозы, исходящие от других типов инсайдеров.

В докладе А.К. Чернышов, Н.А. Чернышова, А.А. Бондарев (АГУ, г. Астрахань) «Современные особенности подготовки специалистов в области инженерно-технической защиты информации» рассматривается современный подход к обучению на основе виртуальных моделей обучения. Рассматривается применение виртуальных лабораторий как средств формирования у учащихся первичных тактико-технических навыков. На сегодняшний день на базе лаборатории по защите информации Астраханского государственного университета создан ряд виртуальных тренажеров для обучения студентов. Использование этих тренажеров успешно протестировано на студентах специальности 090103 «Организация и технология защиты информации» АГУ. Выборка ответов из государственного экзамена, проводимого в виде тестирования, по дисциплине, где использовались виртуальные модели обучения, показала, что данный метод позволил повысить количество правильных ответов по сравнению с предыдущими выпусками.

В докладе А.В. Рожков, В.Ю. Бердюгин (ЮУрГУ, УФБ по Челябинской области, г. Челябинск) «Преподавание дисциплин блока организационно-правовая защита информации для специальностей блока «Информационная безопасность» на примере Южно-Уральского государственного университета. Отмечается, что универсальность нынешнего образования влечет оторванность от потребностей конкретного предприятия и конкретного производства и от особенностей и направлений развития законодательства в области информационного права. Данный недостаток предлагается компенсировать грамотно проведенной подстройкой будущего специалиста под нужды конкретного заказчика, снабдив его актуальной информацией правового и организационно-правового характера. Отмечается, что Южно-Уральский государственный университет, НИИ цифровых систем обработки и защиты информации имеют богатый опыт воспитания специалистов, сочетающих высокие профессиональные знания со знаниями в области гражданско-правового направления.

В докладе А.В.Рожков, М.В. Алчебаева (ЮУрГУ, ЧГАА, г. Челябинск) «Особенности преподавания криптографии» обозначены научно-методические проблемы, неизбежно встающие перед профессиональными математиками при преподавании криптографии. Универсального и методически безупречного решения этих проблем, видимо, не существует, но авторы предлагают два способа улучшения качества преподавания в рамках классического математического подхода. Первый способ связан с использованием аппарата дискретной математики и алгебры. В силу чего можно рассматривать криптографию, а шире – криптологию, как специализированный раздел на стыке алгебры, математической логики и дискретной математики. Второй способ – это привлечение к преподаванию криптографии теории вероятностей с упором на анализ потоковых шифров, теорию информации, статистический анализ текстов и т.п.

В разрезе тематики представленных на конференции докладов можно отметить наличие определенного научно-технического потенциала России по ряду направлений обеспечения информационной безопасности, в частности, в таких областях, как:

- методология и организационно-технические способы организация комплексной защиты объектов информатизации;
- методология тестирования ПО на обнаружение недекларированных возможностей;
- разработка «быстрых» алгоритмов криптоанализа;
- разработка эффективных методов стеганографии;
- методология обнаружения вторжений;
- технология построения и эксплуатации защищенных виртуальных сетей;
- методология и технология эффективной защиты телекоммуникаций;
- методология обеспечения информационно-психологической безопасности личности.

Анализ проблематики докладов позволяет также выделить как наиболее актуальные, с точки зрения науки, дальнейшие направления развития информационной безопасности:

- теория, методология и технология обнаружения и предотвращения вторжений в компьютерные системы и сети;
- компьютерная инсайдерология;
- метрология методов и средств информационной защиты;
- практическая криптография и стеганография;
- методология и технология защиты программного обеспечения от недекларированных возможностей, несанкционированного изменения и управления;
- технология защиты персональных данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. I. Комплексная защита объектов информатизации. Защита телекоммуникаций. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – 256 с.
2. Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. II. Защита информационных процессов в компьютерных системах. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – 272 с.
3. Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. III. Методы и средства криптографии и стеганографии. Концептуальные, организационно-технические, гуманитарные, правовые, экономические аспекты информационной безопасности. Подготовка специалистов по информационной безопасности. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – 300 с.

Брюхомицкий Юрий Анатольевич
Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: bya@tsure.ru.
347928, г. Таганрог, ул. Чехова, 2.
Тел.: 88634371905.

Макаревич Олег Борисович
E-mail: mak@tsure.ru.
Тел.: 88634312018.

Bryukhomitsky Yuri Anatol'evich
Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: bya@tsure.ru.
2, Chekhova street, Taganrog, 347928, Russia.
Phone: +78634371905.

Makarevich Oleg Borisovich
E-mail: mak@tsure.ru.
Phone: +78634312018.