Раздел I. Концептуальные вопросы информационной безопасности

УДК 004.056:061.68

Ю.А. Брюхомицкий, О.Б. Макаревич

ОБЗОР ИССЛЕДОВАНИЙ И РАЗРАБОТОК ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

по материалам докладов XIII Международной научно-практической конференции «Информационная безопасность-2013»

Дается выборочный обзор наиболее интересных и значимых работ российских специалистов, отражающих основные тенденции развития информационной безопасности в России. Обзор выполнен по материалам XIII Международной научно-практической конференции «Информационная безопасность-2013», которая состоялась 9–12 июля 2013 г. в России, г. Таганроге.

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

1. *Концептуальные вопросы информационной безопасности.*
2. *Защита объектов информатизации.*
3. *Безопасность информационных систем и сетей.*
4. *Методы и средства криптографии и стеганографии.*
5. *Информационная безопасность телекоммуникационных систем.*
6. *Прикладные вопросы информационной безопасности.*

Информационная безопасность; концептуальные вопросы; защита объектов информатизации; безопасность информационных систем и сетей; методы и средства криптографии и стеганографии; безопасность телекоммуникационных систем; прикладные вопросы информационной безопасности.

Yu.A. Bryukhomitsky, O.B. Makarevich

OVERVIEW OF RESEARCH AND DEVELOPMENT FOR INFORMATION SECURITY

on the reports XIII International Scientific Conference "Information Security 2013"

Presents a selective overview of the most interesting and significant works of Russian specialists, reflecting the main trends in the development of information security in Russia. The review is based on the XIII International Scientific- Practical Conference "Information Security 2013", held 9–12 July 2013 in Russia, Taganrog.

Research on Information Security, presented at the Conference by Russian specialists are grouped into six areas corresponding to the names of the sections:

1. The conceptual issues of information security.
2. Protection of objects of information.
3. Security of information systems and networks.

* Работа выполнена при поддержке грантов РФФИ: 12-07-00081-а, № 13-07-06033-г.

4. Methods and means of cryptography and steganography.
5. Information security of telecommunication systems.
6. Applied to information security.
Information security; conceptual issues; protection of objects of information; the security of information systems and networks; methods and means of cryptography and steganography; the security of tele-communications systems; applied to information security.

XIII Международная научно-практическая конференция «Информационная безопасность» состоялась 9–12 июля 2013 г. в России, в г. Таганроге. В Конференции приняли участие 147 отечественных и зарубежных специалистов, которые представляли 4 страны, 25 городов, 52 организации. В составе участников: 1 академик, 2 члена-корреспондента РАН, 18 докторов наук, 27 кандидатов наук, 22 аспиранта, 32 магистранта и студента. Материалы Конференции представлены в 65 докладах, опубликованных в двух книгах [1, 2].

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

1. Концептуальные вопросы информационной безопасности.
2. Защита объектов информатизации.
3. Безопасность информационных систем и сетей.
4. Методы и средства криптографии и стеганографии.
5. Информационная безопасность телекоммуникационных систем.
6. Прикладные вопросы информационной безопасности.

Данный обзор является выборочным и охватывает наиболее интересные и значимые работы, российских специалистов, отражающие основные тенденции развития информационной безопасности в России в 2012–2013 гг.

1. Концептуальные вопросы информационной безопасности. В рамках этого направления на Конференции было представлено 5 докладов российских специалистов, посвященных концептуальным и перспективным направлениям в теории защиты информации и информационной безопасности.

Поводом для выступления с докладом авторам Р.М. Юсупову и В.М. Шишкину, СПИИРАН, г. Санкт-Петербург, «Информационная безопасность, кибербезопасность и смежные понятия: Cyber Security VS информационной безопасности» послужила информационная и организационная активность последних месяцев, связанная с разработкой и планами принятия в кратчайшие сроки так называемой «Стратегии кибербезопасности Российской Федерации», инициируемых на уровне Федерального Собрания, а также впечатления от непосредственного участия представителей СПИИРАН в обсуждении её проекта в составе экспертных групп. В докладе представлен краткий обзор принятых за последние годы в ряде стран рамочных документов, направленных на обеспечение безопасности сетевого взаимодействия. Отмечается потребность, и указываются направления актуализации положений действующих доктринальных документов Российской Федерации в сфере информационной безопасности. Утверждается необходимость сохранения независимости её смыслового пространства в интересах национальной безопасности.

Авторы считают, что терминологические дискуссии неконструктивны. Актуальным является не дефиниции понятий, а осмысление новой и перспективной реальности, выработка адекватных ей мер обеспечения безопасности в конкретной практике, в первую очередь касающейся новых и многочисленных проблем безопасности сетевого информационного взаимодействия. По их мнению назрела необходимость развития и актуализации системы документов и, не исключено, понятийного аппарата, отражающих новые реалии и определяющих политику и практику государства, общественные интересы в области информационной безопасно-

сти, в первую очередь, для публичного применения, в расчёте на обозримую перспективу. Для этого нет нужды в терминологическом перевороте. Речь должна идти о системе и преемственности без подражательства и неофитского стремления к альтернативности, как иллюзии новизны. Никто не может запретить употребление любых терминов, в том числе, профессионального жаргона, но следование в русле чужого понятийного аппарата, каким бы универсальным и интернациональным он не казался, замена не столько терминов, сколько смыслов, по сути, есть акт разоружения в информационном противоборстве. Можно отказаться от своих научных традиций, но тогда придётся отказаться от независимости, не только научно-технической, но, рано или поздно, и политической.

Авторам представляется важным – разработка не декларативных стратегических документов, а программ конкретных действий, направленных на противодействие наиболее актуальным угрозам, связанных, прежде всего, с сетевым взаимодействием, с конечными сроками, индикаторами выполнения, финансированием, ответственностью и отчетностью за результаты. Становится необходимым организованное развитие нового направления обеспечения информационной безопасности по выявлению угроз и уязвимостей, организации сбора информации о них, хранению и обеспечению доступа к ней. В этих вопросах имеет место отставание и, как следствие, зависимость от внешних ресурсов. Кроме того нужны программы развития научно-методологического обеспечения решения проблем информационной безопасности. Как показывает жизнь, феноменологический и реактивный подходы, преобладающие в настоящее время, не дают должного эффекта.

Три больших доклада были посвящены вопросам практического применения ранее разработанных О.О. Варламым (МАДГТУ (МАДИ), г. Москва), миварным технологиям.

Коллектив авторов: О.О. Варламов (МАДГТУ (МАДИ), г. Москва), Л.Е. Адамова (ДонГАУ, пос. Персиановский Октябрьского района Ростовской области), Д.В. Елисеев (МГТУ им. Н.Э. Баумана, г. Москва), Ю.И. Майборода (МФТИ, г. Москва), П.Д. Антонов и Г.С. Сергушин (МАДГТУ (МАДИ), г. Москва), М.О. Чибирова (НИЯУ (МИФИ), г. Москва) в своем докладе «Расширение границ автоматизации умственной деятельности человека и миварный подход к моделированию процессов понимания компьютерами смысла текстов, речи и образов» представил результаты обширных исследований по повышению степени автоматизации человеческой деятельности в различных предметных областях, включая и информационную безопасность. Авторы считают, что расширение границ автоматизации умственной деятельности человека является чрезвычайно актуальной задачей, имеющей важное экономическое и стратегическое значение для страны.

Как известно, в области искусственного интеллекта выделяют 3 уровня исследований: рефлексный (нейронные сети и генетические алгоритмы), логический (системы логического вывода) и социальный (моделирования мышления). Для достижения поставленных целей исследования – повышения степени автоматизации человеческой деятельности – наибольший интерес представляет логический уровень. При этом они считают необходимым привлечение гносеологии с переводом ее на математический язык логики, вычислений и баз данных. Это позволяет строить более сложные инструменты познания и перейти на новый уровень расширения границ автоматизации умственной деятельности человека.

В ранних работах О.О. Варламова и его коллег описаны достижения и предложены новые математические формализмы для создания миварных технологий. Миварный подход может применяться в самых разных областях, включая и информационную безопасность. Область информационной безопасности использует все достижения современных наук, а в первую очередь – достижения математики,

кибернетики и информатики. Поэтому расширение границ автоматизации умственной деятельности человека и проблема понимания смысла текстов, речи и образов компьютерами важны, прежде всего, для информационной безопасности. В работе обозначены две основные технологии накопления и обработки информации: многомерные эволюционные базы данных и правил, которые накапливают любую информацию в формализме «вещь, свойство, отношение»; миварные сети, которые позволяют выполнять конструирование алгоритмов решения задач и логический вывод с линейной вычислительной сложностью.

Самое важное, по мнению авторов, состоит в том, что миварные технологии позволили снять существовавшие ограничения и предоставить единые системы с логико-вычислительной обработкой и базами данных. При этом базы данных стали эволюционными и более адекватными, а логический вывод на причинно-следственных связях стал очень быстрым и его вычислительная сложность теперь не *NP*-полная, а линейная относительно количества правил. Более того, теперь логический вывод можно выполнять параллельно, используя все ядра процессоров современных компьютеров. В работах авторов приведены примеры обработки более трех миллионов продукционных правил на обычных ноутбуках, что является революционным прорывом в логической обработке. Как следствие, миварный подход позволил создать более сложные инструменты познания мира.

Исследования авторов показывают возможность описания в одном формализме процессов понимания смысла текстов, речи и образов. Все эти процессы основаны на накоплении и создании многомерной информационной модели мира – «картины мира», где и правила, и факты хранятся и обрабатываются в единой активной базе данных и правил. Миварные технологии позволили смоделировать эти процессы одновременного накопления и логической обработки на основе миварного информационного пространства и миварных логико-вычислительных сетей. Это позволяет создать более сложные научные инструменты познания и существенно расширить границы автоматизации умственной деятельности человека.

Второй доклад в области миварных технологий: Г.С. Сергушин и О.О. Варламов (МАДГТУ (МАДИ), г. Москва), М.О. Чибирова (НИЯУ (МИФИ), г. Москва), Д.В. Елисеев, (МГТУ им. Н.Э. Баумана, г. Москва), Е.А. Муравьева (Филиал УГНТУ в г. Стерлитамаке) «Информационное моделирование сложных систем управления технологическими процессами на основе миварных АСУТП» посвящен созданию интеллектуальных автоматизированных систем управления технологическими процессами (АСУТП).

С точки зрения информационной безопасности АСУТП могут рассматриваться как системы диагностики и автоматизированного управления процессами. Поэтому они могут применяться и в области информационной безопасности для решения аналогичных, по существу, задач сбора, накопления и обработки информации на основе компьютеров.

В работе представлены результаты создания универсального программного комплекса УДАВ и его использования для математического моделирования различных АСУТП в процессе обучения студентов технических вузов. УДАВ создан на основе миварных технологий, которые позволили моделировать сложные технологические процессы в реальном времени. УДАВ, выполняет логический вывод с линейной вычислительной сложностью. Студенты с его помощью успешно создают логические модели систем управления сложными технологическими установками в промышленности. В настоящее время, проводится работа по упорядочению и выкладыванию миварных моделей АСУТП на компьютерные ресурсы вузов. Комплекс УДАВ в настоящее время реализован на основе облачных технологий и доступен на сайте проекта МИВАР www.mivar.org. В перспективе планируется создание муль-

типредметной информационной системы по типу Википедии, когда пользователи смогут самостоятельно создавать описания различных предметных областей и предоставлять к ним открытый доступ для других пользователей.

Третий доклад в области миварных технологий: М.О. Чибирова (НИЯУ (МИФИ), г. Москва), Г.С. Сергушин и О.О. Варламов (МАДГТУ (МАДИ), г. Москва), Д.В. Елисеев (МГТУ им. Н.Э. Баумана, г. Москва) «Миварные и облачные технологии: «он-лайн» реализация универсального решателя задач на основе адаптивного активного логического вывода с линейной вычислительной сложностью относительно правил в виде причинно-следственных связей «если – то» посвящен созданию аппарата логического искусственного интеллекта и его применению в различных предметных областях, включая и информационную безопасность. В работе представлены результаты создания новой версии миварного универсального решателя задач УДАВ, реализованного на основе облачных технологий и способного выполнять адаптивный активный логический вывод. Экспериментально подтверждена теоретическая линейная вычислительная сложность логического вывода и автоматического конструирования алгоритмов решения различных задач на основе миварных сетей и продукций вида «если – то». По мнению авторов, в перспективе УДАВ может практически полностью заменить человека-оператора в информационной безопасности.

Преимуществами миварного подхода к реализации универсального решателя задач являются: линейная вычислительная сложность и реальное время работы; решение логических и вычислительных (и других) задач; управление потоком входных данных и оперативная диагностика; адаптивное описание и непрерывное решение задач; активная работа с запросами или уточнениями входных данных на эволюционной сети правил и объектов (самообучение).

Авторы утверждают, что использование миварных технологий позволило создать теоретические основы логического искусственного интеллекта. По их мнению, представленные ими результаты значительно превышают «мировой уровень» научных исследований, поскольку впервые предложено важнейшее решение по логической обработке продукционных правил с линейной вычислительной сложностью.

Доклад М.А. Стюгин, А.В. Погребной, СФУ, г. Красноярск, посвящен «Проблеме защиты от исследования в системах информационной безопасности». При проектировании систем информационной безопасности очень часто рассматриваются риски, основанные на незащищенности или ненадежности конкретных технических решений, но крайне редко учитывается тот факт, что значительного снижения рисков можно добиться, если сделать защищаемую систему «непонятной» для стороннего наблюдателя. Технологии создания таких «непонятных» систем можно обозначить единым термином защиты систем от исследования.

В работе проанализирован неиспользованный на сегодняшний день ресурс в системах безопасности – защита от исследования систем, под которым подразумевается преднамеренное запутывание злоумышленника при попытке построить адекватный образ атакуемой системы. Для этого проанализированы информационные ограничения, с которыми он сталкивается в процессе исследования. Сформулированы методы защиты систем от исследования. Описаны практические применения и результаты внедрения технологии в области защиты интернет-ресурсов и локальных сетей.

В качестве практических реализаций данного подхода к построению систем безопасности авторами разработана программа ReflexionWeb по защите интернет-ресурсов и ExLook для защиты локальных сетей. Подчеркивается, что перечень возможных внедрений технологий защиты от исследования не ограничен только сетями передачи данных и только техническими направлениями.

Результаты исследования позволяют сформулировать область для дополнительной защиты информационных систем, не исключая применения любых других средств защиты, то есть определяют новый ресурс для снижения рисков. Технические системы, построенные по этим принципам, показали положительные результаты. Программные продукты, реализующие технологию защиты от исследования, прошли успешное внедрение на коммерческих предприятиях.

Проект разработки технических систем в области защиты от исследования за последние три года был поддержан Инновационным центром Сколково, Фондом инноваций, Красноярским фондом поддержки научной и научно-технической деятельности, грантом Президента Российской Федерации МК-1039.2013.9.

2. Защита объектов информатизации. Это направление на Конференции было представлено только одним докладом отечественных специалистов О.Т. Даниловой, Е.Н. и Толстых, ОмГТУ, г. Омск «Анализ комплексной системы информационной безопасности с применением инструментов качества и метода динамического программирования». В работе рассматривается практическое применение некоторых инструментов качества для анализа состояния комплексной системы защиты информации организации, с целью выявления причинно-следственных связей, получения качественных и количественных характеристик уровней защищенности для принятия решений по их эффективной модернизации. Авторы считают, что практическое применение инструментов качества при проведении анализа состояния информационной безопасности организации позволяет выявить причинно-следственные связи показателей информационной безопасности, получить их качественные и количественные характеристики, которые играют важную роль при дальнейшем принятия эффективных решений о повышении уровня информационной безопасности организации. На основании результатов сравнения с законами распределения можно определить основные экономически выгодные направления для повышения уровня комплексных систем защиты информации в целом.

3. Безопасность информационных систем и сетей. В рамках этого направления на Конференции было представлено 17 докладов российских специалистов. Тематика докладов весьма разнообразна и, в частности, включает в себя: методы и средства защиты от атак на беспроводные сенсорные сети; аудит безопасности вычислительных сетей; мониторинг и аудит операционных систем; анализ инцидентов информационной безопасности; анализ профилей злоумышленников в компьютерных системах; защиту информации от НСД для операционных систем; тестирование средств защиты информации; проблемы хранения чувствительных данных средств криптографической защиты; безопасность использования однонаправленных сетей передачи данных; вопросы построения безопасности компьютерных систем на основе использования искусственных иммунных систем; безопасность облачных вычислений; модели вредоносного программного обеспечения и др.

Два доклада Е.С. Абрамова и Е.С. Басан, ЮФУ, г. Таганрог были посвящены безопасности беспроводных сенсорных сетей.

В первом докладе авторами проведен «Анализ сценариев атак на беспроводные сенсорные сети», выявлены угрозы, характерные для каждой атаки, предложены методы для обнаружения и предотвращения атаки. Все рассмотренные ими атаки разделены на два общих класса: активные и пассивные, а также выделен класс атак на средства защиты сети. Существующих механизмов защиты от этих атак недостаточно, и необходимо разрабатывать новые способы защиты характерные для беспроводных сенсорных сетей. Список атак, рассмотренный в докладе, хотя и представлен широко, но не является исчерпывающим. Многие атаки включают в себя несколько стадий. Для большинства атак представлены методы предотвращения атаки. Особый интерес представляет класс атак на средства защиты информации, так как данные атаки еще недостаточно изучены.

Во втором докладе тех же авторов «Разработка архитектуры системы обнаружения вторжений для беспроводных сенсорных сетей» представлен обзор методов и систем обнаружения атак, существующих на сегодняшний день, проведена их классификация, а также выделены достоинства и недостатки. Выделены общие недостатки всех методов и предложены основы будущей разработки защищенной беспроводной сенсорной сети, а также системы обнаружения вторжений.

Доклад М.Е. Бурлаков, М.Н. Осипов, СамГУ, г. Самара был посвящен «Аудиту безопасности локальной вычислительной сети с помощью динамической системы на нейронах с реакцией на последовательности». В работе описываются общие принципы обучения динамической системы на нейронах, а также поясняется механизм создания базы данных оптимальных и дефектных шаблонов. Кроме того рассмотрены вопросы теоретического обоснования и практического применения предложенной реализации системы аудита безопасности локальной вычислительной сети. Определяются основные аспекты применимости системы аудита в рамках выбранной модели информационной системы. Результатом исследования является подтверждение актуальности применения выбранной модели с дальнейшим определением ее сферы применения.

Доклад Д.А. Стеценко, ВолГУ, Волгоград был посвящен «Разработке типовой архитектуры подсистемы мониторинга и аудита ОС на базе Linux». Рассматривая Распоряжение правительства РФ от 17 декабря 2010 г. № 2299-р о переходе с ПО Microsoft на аналоги Open Source автор делает вывод, что только при условии использования такого ПО совместно с системами мониторинга и аудита, можно добиться должного уровня защищенности информационных систем государственных органов.

Информационная система, функционирующая под управлением ОС с открытыми исходными кодами и оснащенная средствами мониторинга и аудита, позволяет квалифицированному специалисту провести своевременный анализ событий, повлекших нарушение безопасности, выработать решение и внедрить его в рабочую систему, тем самым, раз и навсегда перекрыть возможность злоумышленнику реализовать подобную атаку снова. Свойство наблюдаемости автоматизированной системы мониторинга и аудита событий информационной безопасности в зависимости от качества его реализации позволяет в той или иной мере следить за соблюдением сотрудниками организации ее политики безопасности и установленных правил безопасной работы на компьютерах, а, следовательно, контролировать большую часть из всех возможных каналов утечки информации. Средства мониторинга и аудита позволяют своевременно идентифицировать и предотвратить утечку информации в результате проведения атак, типичных для компьютеров под управлением ОС GNU\Linux, подключенных к локальной сети и обрабатывающих конфиденциальную информацию.

В докладе также уделяется внимание вопросам повышения эффективности процесса своевременного реагирования на события информационной безопасности организаций частного сектора. Делается вывод об актуальности задачи – разработки модели подсистемы мониторинга и аудита, функционирующей на любой платформе ОС семейства Linux.

Тема аудита информационной безопасности была также представлена в докладе С.Н. Смирнов (СКЦ Росатома), С.А. Киреев, (Концерн «Системпром»), г. Москва, «Анализ средств аудита информационной безопасности в СУБД Oracle». В работе рассмотрена задача автоматизированного аудита информационной безопасности информационных систем, построенных на базе СУБД промышленного уровня. На примере средств СУБД Oracle 11g авторами показана возможность – построения эффективных механизмов контроля действий пользователя баз данных на

основе штатных средств аудита системы. Рассмотрены возможности и области применения дополнительного средства избирательного аудита. Выбор более совершенного механизма аудита уменьшает потенциальные потери, связанные с деструктивными действиями нарушителя, но сбор и обработка данных аудита требуют дополнительных затрат ресурсов системы. Выбор конкретного решения, в конечном счете, определяет значения элементов матрицы платежей, которые в соответствии с предложенной постановкой задачи определяют цену игры, рассматриваемую как характеристику качества обеспечения информационной безопасности системы.

В докладе В.Г. Жуков, А.А. Шаляпин, СГАУ им. М.Ф. Решетнева, г. Красноярск «Алгоритм прецедентного анализа инцидентов информационной безопасности» рассматривается решение задачи совершенствования процесса управления инцидентами информационной безопасности путем автоматизации процедуры идентификации стратегии реагирования с помощью аппарата прецедентного анализа. Предлагаемый авторами подход основан на поиске решения по аналогии «от частного к частному», применение которого позволит повысить оперативность реагирования и многократно использовать ранее накопленный опыт разрешения инцидентов. Приводится описание алгоритма прецедентного анализа инцидентов информационной безопасности, а также результаты численных экспериментов, которые на множестве тестовых данных демонстрируют работоспособность аппарата прецедентного анализа при автоматизации процедуры идентификации стратегии реагирования. Преимущества применения прецедентного анализа заключаются в возможности повторно применять накопленный опыт и в сокращении времени поиска сценариев реагирования для аналогичных инцидентов. Предложенный подход также позволяет решить задачу обнаружения аномальных инцидентов в классе, наличие которых сигнализирует эксперту о необходимости детального изучения сложившейся ситуации.

В докладе А.П. Стефаров, М.Н. Жукова, СГАУ им. М.Ф. Решетнева, г. Красноярск «Сравнительный анализ профилей злоумышленников в компьютерных системах на основе международных стандартов» рассмотрены профили злоумышленников в компьютерных системах, которые отражены в национальных стандартах, являющихся ратифицированными Российской Федерацией международными стандартами ISO. Проведен сравнительный анализ профилей злоумышленников, отраженных в стандартах, с профилями злоумышленников, разработанными авторами.

Сравнительный анализ проводился по наиболее распространенным классификационным признакам, применяемым при построении профилей злоумышленников: место воздействия злоумышленников, мотивы их действия, каналы атак, средства атак, возможность сговора различных категорий злоумышленников, наличие доступа к штатным средствам, уровень знаний об объектах атак, уровень квалификации, уровни воздействия злоумышленников и стадии жизненного цикла компьютерной системы. Для формирования сравнительных признаков определялось количество возможных значений каждого классификационного признака, далее сравнительные признаки представлялись в виде нормированных коэффициентов.

Два доклада А.М. Каннера, ОКБ САПР, г. Москва были посвящены операционной системе Linux.

В первом докладе «Linux: объекты контроля целостности» автором обосновывается необходимость расширения устоявшегося списка контроля целостности компонентов ОС Linux до ее загрузки модулями ядра ОС. В качестве доказательства положения о необходимости данных мер приводится описание атаки «Инъекция кода» в модули ядра Linux. Предложены меры противодействия таким атакам, которые должны приниматься на этапе проектирования системы защиты информации от НСД.

Во втором докладе «Linux: К вопросу о построении системы защиты на основе абсолютных путей к объектам доступа» рассматриваются способы идентификации объектов доступа в ОС Linux, как одни из ключевых вопросов, стоящих перед разработчиком системы защиты информации для таких ОС, анализируются их преимущества и недостатки. Целью исследования является формулирование посылок, на которые необходимо опираться при выборе метода идентификации объектов доступа, в отличие от второстепенных посылок, опираться на которые ошибочно.

В докладе Т.М. Борисова, А.В. Кузнецов, А.И. Обломова, ОКБ САПР, г. Москва «Тестирование средств защиты информации» рассмотрены особенности тестирования программно-аппаратных средств защиты информации от НСД различных типов (функционирующих в ОС, функционирующих до загрузки ОС, включающих в свой конструктив флешь-память). Цель проведенного исследования заключается в оценке соответствия принятых принципов тестирования указанным задачам, а также в формировании корпуса требований к полноценному тестированию программно-аппаратных средств защиты информации от НСД. Рассмотренные аспекты тестирования программно-аппаратных средств защиты информации показывают, что для них нельзя применять напрямую перенесенные принципы тестирования программных продуктов. Разработчики адаптируют эти принципы в соответствии с собственными представлениями о целесообразности, однако актуальной перспективной задачей авторам видится формирование корпуса специальных принципов, учитывающих все особенности продуктов данного типа.

В докладе Ю.П. Ладынская, А.Ю. Батраков, ОКБ САПР, г. Москва «Хранение данных средств криптографической защиты информации: выбор носителя» рассматриваются требования к хранилищам данных средств криптографической защиты с точки зрения информационной безопасности, соответствие устройств, традиционно применяемых в этом качестве, данным требованиям, а также ряд обстоятельств, которые могут существенно влиять на выбор устройств при прочих равных условиях. Цель исследования – формирование корпуса критериев, позволяющих отдавать предпочтение тому или иному устройству на основании фиксируемых и однозначных показателей.

Доклад С.С. Лыдин, ОКБ САПР, г. Пенза «Организация однонаправленного канала передачи данных на базе защищенного служебного носителя информации» посвящен исследованию проблемы построения одностороннего канала передачи данных между сегментами информационной системы с различными уровнями обеспечения защищенности информации. Для решения данной проблемы на практике обычно применяются однонаправленные сети передачи данных, эксплуатация которых сопряжена с рядом трудностей, связанных с потребностью в верификации данных и, как следствие, невозможностью использования в информационных системах большинства традиционных сетевых протоколов. В работе предложено альтернативное решение по организации канала односторонней передачи данных на базе защищенного служебного носителя информации. Автор описывает обобщенную архитектуру защищенного служебного носителя, на базе которого может быть организован односторонний канал передачи данных, и минимальный набор реализуемых механизмов, достаточный для выполнения основных требований, предъявляемых к такому каналу. Автор полагает, что предлагаемое решение может быть востребовано в качестве средства противодействия скрытым каналам утечки информации, в частности, при построении системы защиты персональных данных в коммерческих и государственных организациях.

Два доклада Ю.А. Брюхомицкого, ЮФУ, г. Таганрог были посвящены перспективным вопросам обеспечения безопасности компьютерных систем на основе использования искусственных иммунных систем.

В первом докладе «Модель искусственной иммунной системы с двойной пластичностью» предлагается формальная модель мониторинга информационных процессов в компьютерной системе на основе парадигмы искусственной иммунной системы с двойной пластичностью. Задачей мониторинга является своевременное выявление нелегитимных информационных процессов. Модель мониторинга основана на модифицированном алгоритме отрицательного отбора, в котором в формализованном виде используется свойство двойной пластичности иммунной системы, позволяющее за счет регулирования типа и числа детекторов поддерживать более высокое качество распознавания нелегитимных информационных процессов.

Во втором докладе «Регулирование распознающих свойств искусственных иммунных систем с двойной пластичностью» рассматриваются подходы и методы регулирования распознающих свойств искусственных иммунных систем с двойной пластичностью, обеспечивающие необходимый баланс первичных и вторичных детекторов, участвующих в выявлении «чужих» информационных процессов. В числе предложенных автором – бионический подход и метод контролируемого уничтожения вторичных детекторов. По аналогии с живой иммунной системой определен эффект «старения» искусственной иммунной системы и предложены методы его нейтрализации.

В докладе О.Ю. Песковой, ЮФУ, г. Таганрог «Облачные сервисы и безопасность: подходы и проблемы» приведены: классификация облачных сервисов, моделей сервиса и моделей развертывания; набор требований к облачным службам; результаты технологических прогнозов ПО для облачных вычислений. Выделены наиболее интересные и критичные с точки зрения обеспечения безопасности облачные технологии. Рассмотрены основные проблемы обеспечения безопасности в облачных сервисах. Предложена классификация проблем информационной безопасности облачных технологий по трем категориям: технологические и организационные проблемы, юридические проблемы, антропогенные проблемы. Рассмотрены вопросы стандартизации и документирования облачных вычислений, а также их применения в системах обеспечения безопасности.

В докладе Л.К. Бабенко, А.С. Кириллов, ЮФУ, г. Таганрог, «Модели образцов вредоносного программного обеспечения на основе используемых системных функций и способов получения их адресов» рассматриваются вопросы построения модели вредоносного программного обеспечения (ВПО), ориентированной на включение в структуру образцов информации не только о конкретных системных функциях, но и способах получения их адресов. По мнению авторов, такая модель может быть использована для эффективного обнаружения и классификации неизвестных ранее экземпляров ВПО и, в отличие от более традиционных моделей, будет более гибкой, устойчивой к изменениям и не зависимой от упакованности и зашифрованности образца ВПО.

4. Методы и средства криптографии и стеганографии. В рамках этого направления на Конференции было представлено 13 докладов по актуальным проблемам криптографии и криптоанализа. Тематика докладов, в частности, включает в себя: способы организации защищенного хранилища информации при облачных вычислениях; разработку и применение протоколов конфиденциальных вычислений; построение новых моделей кодовых криптосистем; повышение стойкости схем специального широковещательного шифрования; исследование стойкости алгоритмов шифрования ГОСТ 28147-89 и RC5 и др.

Доклад Ю.В. Косолапов, В.Э. Никулин, ЮФУ, г. Ростов-на-Дону «Способ организации распределенного хранилища, устойчивого к частичной утечке данных» посвящен способам организации защищенного хранилища информации при облачных вычислениях. Для гарантирования надежности предоставляемого храни-

лища провайдеры часто используют принцип распределения информации между несколькими носителями с добавлением избыточности. Этот принцип может быть использован не только для гарантирования надежности хранения, но и для защиты информации от несанкционированного просмотра. Применение традиционного способа защиты конфиденциальности информации на носителе путем шифрования осложняется необходимостью управления жизненным циклом ключевой информации. При заранее определенном количестве доступных злоумышленнику носителей, имеющих различную вероятность утечки информации, авторы предлагают построить защищенную систему хранения так, чтобы злоумышленник не мог однозначно восстановить секрет, при этом для организации защиты нет необходимости применять секретные ключи. Такую систему хранения предлагается построить на основе концепции канала с наблюдением второго типа со специальным алгоритмом оптимального распределения информации между двумя и тремя носителями.

В докладе В.Г. Жуков, А.В. Вашкевич, СГАУ им. М.Ф. Решетнева, г. Красноярск «Конфиденциальный кластерный анализ при вертикальном секционировании данных» приведено обзорное исследование актуальных проблем в разработке и применении протоколов конфиденциальных вычислений, в частности, конфиденциального кластерного анализа. Представлены недостатки существующих решений конфиденциального кластерного анализа методом K-means при вертикальном секционировании данных, а также предложены пути их устранения с помощью криптографических примитивов и требования, которым они должны соответствовать. С помощью предложенных мер будет гарантироваться обеспечение конфиденциальности данных при кластерном анализе для заданной модели информационного обмена, а именно для указанного общего количества участников и количества сговорившихся из них. В частности, разрешена проблема раскрытия данных при малом количестве участников.

Проделанная авторами работа позволяет в дальнейшем модернизировать существующие протоколы, а также – распространить полученные сведения для последующего применения конфиденциального кластерного анализа в Российской Федерации.

В докладе Е.С. Чекунов, ЮФУ, г. Ростов-на-Дону «Об алгоритмическом проектировании системы Мак-Элиса с использованием списочного декодера Бернштейна» с целью повышения стойкости кодовой криптосистемы к атакам на секретный ключ строится вариант системы Мак-Элиса с использованием списочного декодера Бернштйна.

Стойкость предложенной Мак-Элисом кодовой криптосистемы с открытым ключом на основе бинарных кодов Гоппы основывалась на *NP*-сложности задачи декодирования произвольного линейного кода. Однако с появлением детерминированных алгоритмов атак на шифрограмму стало возможным восстанавливать зашифрованный текст с помощью компьютерных кластеров за приемлемое время. Для противостояния таким атакам криптосистему усилили за счет увеличения параметров кода и количества искусственных ошибок в протоколе, а также применения списочного алгоритма декодирования. Цель настоящей работы заключается в том, чтобы построить модель кодовой криптосистемы Мак-Элиса на бинарных кодах Гоппы с использованием известной математической модели списочного декодера Бернштейна для применения в системах защиты данных от НСД. Данный подход позволяет увеличить уровень защищенности системы в целом, не меняя при этом ее параметры.

Авторы Н.В. Бессуднова (ЮФУ) и В.В. Мкртичян (НИИ «Спецвузавтоматика»), г. Ростов-на-Дону представили доклад «Исследование алгоритма Сантхи списочного декодирования *q*-ичных кодов Рида-Маллера и возможности его применения в схемах специального широковещательного шифрования». Целью проведен-

ного ими исследования является изучение возможности применения эффективного алгоритма списочного декодирования Сантхи для построения схемы защиты тиражируемой цифровой продукции от несанкционированного распространения. Для достижения этой цели исследуется алгоритм Сантхи списочного декодирования q-ичных кодов Рида-Маллера и структура этих кодов. На основе исследований авторами доказывается утверждение о возможности применения алгоритма Сантхи в схемах специального широковещательного шифрования.

Авторы С.А. Евпак (ЮФУ) и В.В. Мкртичян (НИИ «Спецвузавтоматика»), г. Ростов-на-Дону представили доклад «О границах применения специальной схемы защиты информации, основанной на q-ичных кодах Рида-Маллера». Известен перспективный способ защиты легально тиражируемой цифровой продукции от несанкционированного распространения, называемый схемой специального широковещательного шифрования (ССШШ). Известно также, что злоумышленники, являющиеся легальными пользователями ССШШ, могут объединяться в коалиции и пытаться атаковать ССШШ. В более ранних работах С.А. Евпаком и В.В. Мкртичяном было доказано, что для эффективного поиска всей коалиции, или, по крайней мере, ее непустого подмножества, можно применять q-ичные коды Рида-Маллера и представлена соответствующая математическая модель эффективной ССШШ. Целью настоящей работы является исследование математической модели эффективной ССШШ на основе q-ичных кодов Рида-Маллера и списочного декодера Пеликаана для тех же кодов в случае превышения допустимого числа членов коалиции злоумышленников. Настоящее исследование позволило установить новые границы применения схемы защиты легально тиражируемой цифровой продукции от несанкционированного распространения.

Три доклада специалистов ЮФУ, г. Таганрог были посвящены исследованию стойкости алгоритма шифрования ГОСТ 28147-89.

В первом докладе Бабенко, Е.А. Ищукова «Линейный криптоанализ алгоритма ГОСТ 28147-89» авторами представлен универсальный алгоритм поиска слабых блоков замены по отношению к линейному криптоанализу. Данное исследование направлено на предотвращение использования слабых блоков замены для тех алгоритмов шифрования, в которых данные элементы не являются фиксированными. Разработанный алгоритм был опробован на примере анализа блоков замены для алгоритма шифрования ГОСТ 28147-89. Применение алгоритма позволило без труда обнаружить большое число ослабленных блоков замены, использование которых может значительно ослабить стойкость используемого алгоритма шифрования.

Во втором докладе тех же авторов «Различные подходы к оценке стойкости алгоритма шифрования ГОСТ 28147-89» рассмотрены подходы к анализу алгоритма шифрования ГОСТ 28147-89 на основе методов линейного и дифференциального криптоанализа, алгебраической и слайдовой атак. Приведены численные результаты, полученные экспериментально в результате применения рассмотренных методов анализа различными специалистами в области криптографии, включая авторов данного доклада.

В третьем докладе Л.К. Бабенко, Е.А. Маро «Оценка стойкости алгоритма ГОСТ28147-89 к алгебраическим методам криптоанализа» приведено описание принципа оценки стойкости российского стандарта шифрования ГОСТ 28147-89 методом eXtended Linearization (XL) алгебраического анализа. В работе приводятся алгоритмы: генерации системы уравнений для фиксированных блоков замены (S-блоков), решения полученной системы уравнения методами линеаризации и eXtended Linearization. Выполнено моделирование атаки на алгоритм ГОСТ⊕.

В докладе Л.К. Бабенко, С.И. Сохненко, ЮФУ, г. Таганрог «Особенности функции хэширования Keccak» описана криптографическая хэш-функция Keccak, являющаяся победителем конкурса SHA-3 и ставшая новым стандартом, принятым Национальным институтом стандартов и технологий США (НИСТ).

В докладе В.О. Осипян, А.С. Жук, А.Х. Арутюнян, Ю.А. Карпенко, КубГУ, г. Краснодар «Разработка математической модели системы обработки потока данных по заданному набору элементов множества» сформулирована и решена задача построения упорядоченного множества строк на заданном алфавите, допускающего взаимно-однозначное соответствие между его подмножествами и буквами алфавита. Разработан алгоритм для построения такого множества строк и приведены граничные оценки относительно их мощностей. На основе полученных результатов построена математическая модель симметричной криптосистемы с количеством ключей, экспоненциально зависящим от числа исходных параметров, в качестве прикладного приложения.

Авторы отмечают возможность дальнейшего развития данной криптосистемы по параметрам: упрощение алгоритма построения ключа, построение СЗИ с открытым ключом с использованием задачи об суперобобщенном рюкзаке.

Доклад Е.А. Ищуковой, ЮФУ, Таганрог был посвящен «Линейному криптоанализу алгоритма шифрования RC5». В работе рассмотрены подходы к анализу стойкости алгоритма RC5 на основе использования метода линейного криптоанализа. Рассмотрены способы построения линейных аналогов при использовании операции целочисленного сложения по модулю. Рассмотрены алгоритмы построения линейных аналогов и поиска секретного ключа на их основе. Поскольку алгоритм ГОСТ 28147-89 имеет в своей структуре такое же криптографическое преобразование, что и алгоритм RC5, а именно, – операцию целочисленного сложения по модулю, – достигнутые результаты могут быть объединены с полученными ранее результатами в области анализа алгоритма ГОСТ 28147-89 для проведения оценки его стойкости по отношению к линейному криптоанализу.

5. Информационная безопасность телекоммуникационных систем. В рамках этого направления на Конференции было представлено 9 докладов. Тематика докладов включала в себя: разработку математического аппарата для оценки вероятности неприема апериодических псевдослучайных последовательностей в каналах связи различного типа; способ измерения частоты радиосигнала в акустооптическом приёмнике-частотомере; применение алгоритма декодирования БЧХ-кодов для оценки разведзащищенности псевдослучайных последовательностей специальных систем связи; совершенствование способа обмена информацией в высокоскоростных беспроводных информационных сетях; применение производных систем ортогональных сигналов для повышения помехоустойчивости систем радиосвязи с кодовым разделением абонентов; моделирование методов скремблирования цифрового потока данных; безопасность передачи сообщений ключевого управления по каналам связи в системах радиосвязи; анализ проблемы выбора параметров технических средств спутниковой связи.

Доклад Д.М. Собачкин, КВВУ им. С.М. Штеменко, г. Краснодар посвящен «Оценке вероятности неприема апериодической псевдослучайной последовательности в составных и двоичных симметричных каналах связи». Целью работы является разработка математического аппарата для оценки вероятности неприема апериодических псевдослучайных последовательностей (АПСП) в составных рэлеевских каналах с тропосферным рассеиванием и дискретных симметричных каналах. Рассмотрение дискретных каналов как отображение непрерывных линейно-стохастических каналов позволило исследовать влияние ошибок синхронизации в дискретных каналах на основе изучения свойств непрерывных каналов связи. В результате такого подхода получены строгие оценки вероятности неприема АПСП в составных и биномиальных каналах связи и проведен сравнительный анализ синхронизации АПСП в них.

В докладе А.В. Помазанов, С.С. Шибаев, ЮФУ, г. Таганрог «Способ измерения частоты радиосигнала в акустооптическом приёмнике-частотомере» применительно к акустооптическим приёмникам-частотомерам (АОПЧ) и измерителям параметров радиосигналов предложен алгоритм вычисления частоты измеряемого сигнала. Суть алгоритма заключается в том, что кривая настройки реального АОПЧ заменяется непрерывной ломаной линией, при последующем использовании которой обеспечивается возможность повышения точности вычисления искомой частоты.

Авторы рекомендуют предложенный ими алгоритм к практическому использованию. Эффективность использования алгоритма, по их мнению, будет возрастать с увеличением полосы рабочих частот АОПЧ.

В докладе С.А. Расторгуев, КВВУ им. С.М. Штеменко, г. Краснодар рассматривается «Применение алгоритма декодирования БЧХ-кодов для оценки разведзащищенности псевдослучайных последовательностей специальных систем связи». Целью работы является доказательство независимости разведзащищенности псевдослучайной последовательности (ПСП) от длины периода, даже при неограниченном его увеличении. В работе предлагается для вскрытия структуры ПСП специальных систем использовать итеративный алгоритм декодирования БЧХ-кодов Берлекемпа-Месси. Путем имитационного моделирования алгоритма Берлекемпа-Месси доказывается возможность вскрытия структуры ПСП даже при неограниченном увеличении его периода. Строго обоснована зависимость разведзащищенности ПСП в сеансах связи от перехвата чистого отрезка ПСП, равной длине формирующего его линейного рекуррентного регистра. Суть алгоритма вскрытия структуры ПСП основана на том, что на каждом шаге декодирования делается попытка определения полинома обратных связей, формирующего эту последовательность регистра путем формирования порождающего полинома.

По результатам исследования сформулированы необходимые и достаточные условия обеспечения заданной разведзащищенности ПСП в сеансах связи.

Доклад А.П. Жук, В.И. Петренко, Ю.В. Кузьминов, А.А. Лысенко, СКФУ, г. Ставрополь посвящен «Совершенствованию способа обмена информацией в высокоскоростных беспроводных информационных сетях с использованием новых типов ансамблей дискретных последовательностей». Целью работы является анализ известных способов формирования ансамблей ортогональных последовательностей на предмет обеспечения при их использовании максимальной структурной скрытности систем передачи информации с кодовым разделением каналов.

Доклад В.И. Петренко, А.П. Жук, Ю.В. Кузьминов, Д.Н. Суховей, СКФУ, г. Ставрополь посвящен «Применению производных систем ортогональных сигналов для повышения помехоустойчивости систем радиосвязи с кодовым разделением абонентов». В работе рассмотрено влияние параметров адресных и расширяющих спектр дискретных последовательностей на помехоустойчивость широкополосных систем радиосвязи с кодовым разделением абонентов. Рассмотрен способ формирования ансамблей многозначных ортогональных дискретных последовательностей при использовании производящих последовательностей линейной структуры. Разработано правило формирования производных последовательностей, проведен расчет и сравнение их автокорреляционных свойств.

Доклад В.Т. Корниенко, ЮФУ, г. Таганрог «Скремблирование цифрового потока данных: использование виртуальных приборов LabVIEW в учебном процессе» посвящен описанию лабораторного практикума на основе технологии виртуальных приборов LabVIEW, предназначенному для выполнения операций скремблирования цифрового потока данных. В работе рассмотрены приложения операций скремблирования цифрового потока и приведен пример реализации виртуального скремблера в системе передачи видео высокой четкости.

В докладе И.Е. Любушкина, А.В. Шарамок, Фирма «АНКАД», г. Москва «Безопасность передачи сообщений ключевого управления по каналам связи в системах радиосвязи» рассмотрена модель удаленного управления ключевой информацией в радиосетях высокого уровня сложности. Предложена модель транспортного уровня передачи команд ключевого управления на базе протокола SNMPv3. Рассмотрена архитектура протокола. Разработаны методы внедрения подсистемы ключевого управления в архитектуру протокола SNMPv3. Приведен сравнительный анализ разработанных методов.

В докладе А.Ф. Чипиги, СКФУ, г. Ставрополь «Анализ проблемы выбора параметров технических средств спутниковой связи при использовании пониженных частот и сдвоенного приема» приведены результаты разработки методики параметрического синтеза низкочастотных систем спутниковой связи по заданным требованиям к их энергетической скрытности и помехоустойчивости.
Параметрический синтез включает в себя выбор технических характеристик, скорости передачи, системного запаса, несущей частоты.

6. Прикладные вопросы информационной безопасности. В рамках этого направления на Конференции было представлено 16 докладов по вопросам применения принципов, подходов, методов, средств информационной безопасности для решения задач в различных прикладных областях. Кроме того, в это направление вошли доклады, темы которых выходят за рамки предыдущих пяти тематических направлений работы конференции.

Доклад С.Е. Кузнецов, В.А. Клейменов, НТЦ «Атлас», Пенза «Анализ ПО посредством исследования информационных потоков». Целью данного исследования является определение способа анализа ПО посредством исследования информационных потоков. В процессе проведенного исследования наиболее приоритетными были принципы максимально возможного сокращения экспертных трудозатрат при сохранении относительно высокой достоверности результатов анализа ПО. Предлагаемый в итоге способ предусматривает при проведении анализа ПО, как непосредственную работу эксперта, так и применение автоматизированных средств.

Предложенная реализация способа исследования информационных потоков позволяет оптимизировать трудоемкость анализа ПО, разработанного на большинстве современных языков программирования, причем в большинстве случаев основные положения предложенной реализации способа не зависят от назначения и области применения исследуемого ПО.

Данная методика позволяет сократить временные трудозатраты эксперта при относительно хороших показателях достоверности результатов анализа. Одним из проблемных моментов предлагаемой методики является отсутствие функциональной возможности определения наличия защищаемых данных в конкретных областях памяти, что обуславливается изменением состояния системы во времени. Реализация такой функциональной возможности является предметом дальнейшей работы авторов над данной проблемой.

Четыре доклада специалистов ЮФУ, г. Таганрог объединены общим подходом к различным аспектам обеспечения защиты информации с позиции виртуализации.

В первом докладе В.В. Котенко, К.Е. Румянцев, А.И. Поляков, А.И. Ежов «Алгоритмы оптимизации процессов защиты дискретной информации с позиций виртуализации информационных потоков» решается задача синтеза алгоритмов оптимизации процессов шифрования и дешифрования с позиций виртуализации информационных потоков. Виртуализация реализуется включением на выходе преобразования шифрования и на входе преобразования дешифрования модуля

виртуализации информационного потока, осуществляющего дешифрование криптограмм исходного и виртуального информационных потоков, шифрование результатов дешифрования и задержки во времени ключевых последовательностей и сообщений. Авторы утверждают, что программная реализация полученных алгоритмов применительно к известным шифрам DES и AES показала значительное (практически на порядок) увеличение эффективности шифрования.

Во втором докладе С.В. Котенко, К.Е. Румянцев, В.В. Котенко, А.И. Ежов, А.И. Поляков «Защита объектов информатизации на основе информационной виртуализации видеоидентификаторов» предлагается вариант реализации подхода, основанного на информационной виртуализации идентификаторов, применительно к задачам защиты объектов информатизации от НСД.

Традиционное решение задачи повышения эффективности защиты объектов информатизации достигается путем многоуровневого комплексного применения значительного числа обнаружителей НСД различных видов и увеличения количества уровней их комплексного применения. В итоге это приводит к значительным финансовым затратам на фоне – снижения функциональной устойчивости системы защиты объектов информатизации, в целом. Авторы показывают возможность решения этой проблемы на основе информационной виртуализации идентификаторов.

Проведенные авторами экспериментальные исследования варианта реализации этого подхода показали значительное расширение возможностей защиты объектов информатизации при незначительных экономических затратах.

В третьем докладе С.В. Котенко, К.Е. Румянцев, В.В. Котенко «Идентификационный анализ с позиций информационной виртуализации идентификаторов» предлагается новый подход к комплексному идентификационному анализу на основе информационного тестирования параметров психофизиологических и биометрических идентификаторов человека и формирования соответствующего им информационного образа личности.

Теоретическая основа подхода базируется на математическом аппарате и подходах теории информации и теории виртуализации. С этих позиций основу психофизиологического тестирования человека составляет исходная информация о значениях параметров психофизиологических идентификаторов. Тогда отношения объектов исследования (тестируемых) и исследователя представляются в виде схемы коммуникации, где объект исследования выступает в качестве источника информации, а исследователь – в качестве получателя информации. Такая схема коммуникации предполагает переход из материальной (вещественной) области представления параметров психофизиологических идентификаторов в информационную область. Этот переход обеспечивается путем виртуализации материального представления параметров психофизиологических идентификаторов.

По мнению авторов, реализация предложенного подхода открывает новую область методов многофакторного идентификационного анализа личности. Значительное число известных психофизиологических идентификаторов и еще большее число их возможных комбинаций позволяют прогнозировать большой реализационный потенциал подхода в части разработки принципиально новых методов, применимых для решения широкого круга задач психофизиологии и идентификационного анализа личности.

В четвертом докладе В.В. Котенко, А.А. Поляков «Стратегия оптимизации методов защиты непрерывной информации с позиций виртуализации относительно условий теоретической недешифруемости» приводится теоретическое обоснование стратегии оптимизации процесса защиты непрерывной информации с позиций виртуализации относительно условий теоретической недешифруемости. Получена модель виртуализации процесса защиты непрерывной информации с пози-

ций условий теоретической недешифруемости, составляющая фундаментальную основу – стратегии оптимизации процесса защиты непрерывной информации. По мнению авторов, применение предложенной стратегии открывает принципиально новую область возможностей разработки методов скремблирования, обеспечивающих абсолютную недешифруемость.

В докладе А.О. Шумская, Р.В. Мещеряков, ТУСУР, г. Томск «Использование расстояния Махаланобиса в задачах идентификации происхождения текста» рассматривается вопрос применимости статистических методов атрибуции для решения задач выявления искусственной генерации текста. Для определения сходства некоторого текста с характеристиками искусственного текста применяется метрика расстояния Махаланобиса.

В работе представлены результаты экспериментальных вычислений степени схожести случайного входного текста со специально исследуемыми выборками искусственных текстов. Предполагается, что этот и подобные расчеты могут позволить выработать наиболее эффективный способ выявления искусственной генерации текстовых произведений.

В докладе А.Ю. Исхаков, Р.В. Мещеряков, ТУСУР, Томск «Схемы аутентификации пользователя в СКУД с использованием QR кодов и передачи данных по технологии NFC» представлены результаты исследования применимости технологий QR кодов и беспроводной высокочастотной связи малого радиуса в качестве транспорта аутентификационной информации.

В современных системах контроля и управления доступом СКУД процедура аутентификации пользователей обычно реализуется посредством электронных проходных с использованием бесконтактных карт доступа. Они являются классическим примером аутентификации второго типа, наследуя и недостатки любой системы однофакторной аутентификации.

В связи с этим авторами предлагается механизм двухфакторной аутентификации, предполагающий использование мобильного устройства связи в качестве носителя пользовательского идентификатора. При этом в мобильном устройстве реализуется программный генератор одноразовых паролей, который позволит защитить систему аутентификации от компрометации статичного идентификатора. В качестве второго фактора аутентификации предлагается использовать защиту от НСД к приложению-аутентификатору (в случае потери/кражи мобильного устройства).

В докладе Е.В. Лапина, В.В. Золотарев, СГАУ им. М.Ф. Решетнева, г. Красноярск «Автоматизация процесса исследования параметров систем электронного документооборота» приводится решение задачи – анализа оценки параметров документооборота. Основой подхода является отслеживание состояния системы документооборота в динамике.

В докладе В.В. Золотарев, СГАУ им. М.Ф. Решетнева, г. Красноярск «К вопросу моделирования безопасности автоматизированных систем управления технологическими процессами» представлен подход к оценке и моделированию безопасности, в том числе элементов информационной безопасности программных и аппаратных компонентов, для автоматизированных систем управления технологическими процессами различных типов. Предполагается, что в дальнейшем подход будет конкретизирован и привязан к типовым решениям.

Доклад Б.И. Ефимов, Р.Т. Файзуллин, ОмГТУ, г. Омск посвящен «Вопросу устойчивости объективного решения экспертов в системах принятия решений с привлечением экспертов при воздействии угроз информационной безопасности». В работе сформулировано основное требование к системе – обеспечения информационной безопасности системы принятия решений с привлечением экспертов. Предложено решение задачи – вычисления вероятности принятия ложного реше-

ния в системах принятия решения с привлечением экспертов под воздействием угроз информационной безопасности, направленных на изменение ответов экспертов. Получены оценки, показывающие целесообразность или нецелесообразность увеличения количества экспертов для уменьшения влияния действий злоумышленника на принимаемое решение. Рассмотрены типы атак на основе увеличения вероятности неверного решения.

В докладе Н.Д. Абасов, А.М. Абасова (ЮФУ, г. Таганрог), С.В. Савин, О.А. Финько (КВВУ им. С.М. Штеменко, г. Краснодар) «Отказоустойчивый регистратор защищённой информации, функционирующий в избыточном модулярном коде» рассматривается устойчивая к ошибкам система обработки и хранения информации, построенная на основе свойств избыточного модулярного кода и функционирующая в кольце неотрицательных целых чисел по модулю p. Предложены решения, позволяющие обеспечить информацию, хранимую в регистраторах защищённой информации, свойством самовосстановления после различных деструктивных воздействий, являющихся следствиями функционирования в экстремальных условиях. По сравнению с методами резервирования достигается уменьшение избыточности оборудования.

Доклад Е.П. Соколовский, А.К. Малашихин, О.А. Финько, КВВУ им. С.М. Штеменко, г. Краснодар посвящен «Применению числовой нормальной формы представления булевых функций в логико-вероятностном методе И.А. Рябинина». Оценка безопасности структурно-сложных систем, в том числе – систем защиты информации (СЗИ), с использованием логико-вероятностного метода основывается на исследовании сценариев опасных состояний, реализованных монотонными булевыми функциями. Развитие путей практического использования логико-вероятностного метода в СЗИ затруднено сложностью – автоматизации процессов построения сценариев опасных состояний и получения вероятностных функций перехода исследуемой системы в опасное состояние. В работе рассматривается применение фундаментальных положений алгебры логики для построения и реализации вероятностных полиномов в методе И.А. Рябинина. Применение ориентировано на решение задач автоматизации построения и вычисления вероятностных функций перехода СЗИ в опасное состояние.

Доклад Н.И. Елисеев, О.А. Финько, КВВУ им. С.М. Штеменко, г. Краснодар «Подсистема проверки целостности графической информации в системах электронного документооборота». Существующие технологии защиты информации, реализованные в системах электронного документооборота, в ряде случаев не позволяют обеспечить объективность результата проверки целостности графической информации. В работе предлагаются решения, обеспечивающие современные средства электронной подписи свойством «гибкости» при проверке целостности графической информации, представленной как в электронном виде, так и на твердых («бумажных») носителях.

В докладе И.А. Калмыков, Е.М. Яковлева, М.И. Калмыков, А.Б. Саркисов, ИИТТ СКФУ, г. Ставрополь «Разработка алгоритма определения злоумышленника для схемы разделения секрета, функционирующей в модулярном полиномиальном коде» рассмотрены основы построения схемы разделения секрета, которая функционирует в полиномиальной системе классов вычетов (ПСКВ). Приведены требования, предъявляемые к системе оснований ПСКВ. Рассмотрен алгоритм восстановления секрета с помощью китайской теоремы об остатках. Разработан алгоритм определения злоумышленника в группе пользователей, которые восстанавливают секрет. В основу алгоритма положена позиционная характеристика непозиционного модулярного полиномиального кода.

В докладе В.М. Федоров, Д.П. Рублев (ЮФУ, г. Таганрог), Е.М. Панченко (НИИ Физики ЮФУ, г. Ростов-на-Дону) «Сегментация виброакустических сигналов, возникающих при нажатии/отпускании клавиш клавиатуры» рассмотрена проблема сегментации виброакустических сигналов, возникающих при наборе данных на клавиатуре. Предложены алгоритмы сегментации сигналов на основе дискретного вейвлет-преобразования и условия превышения порога пиками сигнала для идентификации принадлежности фрагмента виброакустического сигнала нажатию либо отпусканию клавиши. Точность идентификации, по заявлению авторов, составила более 96 %.

В докладе Т.А. Гришечкина, О.Б. Макаревич, ЮФУ, г. Таганрог «Выявление вредоносных узлов в сетях ad hoc при различных типах атак» показано применение методики выявления вредоносных узлов в сети ad hoc с кластерной архитектурой. Описывается поведение вредоносных узлов со стороны различных типов атак, которые они могут осуществлять. Кроме того, приводятся примеры поведения узлов при межкластерном взаимодействии.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Материалы XIII Международной научно-практической конференции «Информационная безопасность». Ч. I. – Таганрог: Изд-во ЮФУ, 2013. – 276 с.
2. Материалы XIII Международной научно-практической конференции «Информационная безопасность». Ч. II. Материалы III Всероссийской молодежной конференции «Перспектива-2013». – Таганрог: Изд-во ЮФУ, 2013. – 252 с.

Статью рекомендовал к опубликованию к.т.н. М.Ю. Руденко.

Брюхомицкий Юрий Анатольевич – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: bya@tgn.sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; доцент.

Макаревич Олег Борисович – e-mail: mak@tsure.ru; тел.: 88634312018; кафедра безопасности информационных технологий; зав. кафедрой.

Bryukhomitsky Yuriy Anatoly – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University” e-mail: bya@tgn.sfedu.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; associate professor.

Makarevich Oleg Borisovich – e-mail: mak@tsure.ru; phone: +78634312018; the department of security in data processing technologies; head of the department.

УДК 004.056.5, 004.89

А.М. Цыбулин, М.Н. Свищева

СИСТЕМНЫЙ ПОДХОД К ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ БОРЬБЫ С ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТЬЮ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ

Предлагается системный подход к повышению эффективности борьбы с инсайдерской деятельностью пользователей. Контролируется эффективность работы пользователей с любой информацией в течение рабочего времени. Оценка эффективности работы персонала имеет своей целью сопоставить реальное содержание, качество, объемы и интенсивность труда персонала с установленными нормами. Для противодействия утечкам информации по вине внутренних нарушителей разработан программный комплекс, кото-