Раздел I. Общие вопросы информационной безопасности

УДК 004.056:061.68

Ю.А. Брюхомицкий, О.Б. Макаревич

ОБЗОР ИССЛЕДОВАНИЙ И РАЗРАБОТОК ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*
по материалам докладов XII Международной научно-практической конференции «Информационная безопасность-2012»

Дается выборочный обзор наиболее интересных и значимых работ российских специалистов, отражающих основные тенденции развития информационной безопасности в России. Обзор выполнен по материалам XII Международной научно-практической конференции «Информационная безопасность-2012», которая состоялась 25–29 июня 2012 г. в России, г. Таганроге.

Информационная безопасность; концептуальные вопросы информационной безопасности; безопасность информационно-телекоммуникационных систем; защита объектов информатизации; методы и средства криптографии и стеганографии; безопасность программного обеспечения.

Y.A. Bryukhomitsky, O.B. Makarevich

REVIEW OF RESEARCH AND DEVELOPMENT INFORMATION SECURITY
based on reports XII 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 XII International Scientific and Practical Conference "Information Security", which states 25–29 June 2012 in Russia, Taganrog.

Information security; conceptual issues of information security; security of information and telecommunications systems; protection of information; methods and means of cryptography and steganography; security software.

XII международная научно-практическая конференция «Информационная безопасность» состоялась 25–29 июня 2012 года в России, в г. Таганроге. В Конференции приняли участие 197 отечественных и зарубежных специалистов, которые представляли 5 стран, 20 городов, 57 организаций. В составе участников 26 доктора наук, 42 кандидатов наук, 18 аспирантов, 12 магистрантов и студентов. Материалы Конференции представлены в 85 докладах, опубликованных в двух книгах [1, 2].

* Работа выполнена при поддержке грантов РФФИ: №12-07-00081-а, №12-07-06022-г.

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

1. Концептуальные вопросы информационной безопасности.
2. Безопасность информационно-телекоммуникационных систем.
3. Защита объектов информатизации.
4. Методы и средства криптографии и стеганографии.
5. Безопасность программного обеспечения.
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 2011–2012 гг.

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

В докладе В.В. Котенко, Таганрогский технологический институт Южного федерального университета (ТТИ ЮФУ), г. Таганрог «Стратегия обеспечения безопасности функциональной устойчивости систем государственного управления» с позиций теории виртуализации» приводятся результаты исследования проблем обеспечения безопасности функциональной устойчивости систем государственного управления. Определяются модели критических функциональных состояний системы государственного управления. Теоретически обосновывается стратегия обеспечения безопасности функциональной устойчивости систем государственного управления, которая, наряду с открытыми закономерностями, составляет фундаментальный теоретический базис, определяющий стратегическую необходимость деятельности руководства Российской Федерации, направленной на создание государственно определяемых правящей партии и Общероссийского народного фронта. Полученные модели критических состояний системы государственного управления позволяют прогнозировать различные продуктивные варианты реализаций угроз безопасности функциональной устойчивости систем государственного управления и определять эффективные стратеги противодействия. В соответствии с выявленными закономерностями основу этих стратегий составляет создание и развитие системы государственно определяемых органов общественного влияния включающих созданные на государственной основе народные и общественные движения, объединения, форумы, блоки, организации и т.п. с управляемой неопределенностью функционирования.

В докладе С.Г. Данилюк, В.Г. Маслов, А.И. Попов, Межрегиональное общественное учреждение «Институт инженерной физики», г. Серпухов, «Порядок обработки нечеткой информации при оценке состояний информационных систем» предложена процедура обработки нечеткой информации с учетом априорных вероятностей состояний как основы принятия решений по оценке качества информационных систем. Разработанная процедура базируется на основе положений теории нечетких множеств и вероятностно-лингвистической модели. Снятие ограничения о равновозможности состояний объекта повышает степень адекватности модели и априори создает условия для повышения эффективности процесса определения этих состояний. Однако при этом изменение характера модели требует разработки новых по своей сути процедур обработки модели. Рассмотрены вопросы реализуемости и эффективности разработанных алгоритмов формализации и обработки информации, включающей экспертные оценки и, в том числе, информацию об априорных вероятностях состояний объекта. В ходе моделирования бы-

ли проверены и практически подтверждены: функциональность и результативность алгоритма, т.е. способность получать результат при заданных исходных данных, удовлетворяющих установленным ограничениям и допущениям; диагностическая корректность процедуры, т.е. способность получить в качестве результата как «наиболее подозреваемого» того состояния, которое было получено уже апробированной аналогичной по назначению процедурой при идентичных исходных данных; чувствительность процедуры, т.е. способность «реагировать» на изменение исходных данных об априорных вероятностях состояний информационного объекта; «мягкость» процедуры по отношению к исходной информации, как способность сохранения при формализации и обработке как можно большего объема полезной исходной информации вплоть до выработки окончательного решения; эффективность процедуры, как способность идентифицировать нерегламентированное состояние объекта при определенных ресурсных затратах на процесс диагностирования.

В докладе А.П. Стефаров, В.Г. Жуков, М.Н. Жукова, Сибирский государственный аэрокосмический университет (СГАУ) имени академика М.Ф. Решетнева, г. Красноярск, «О решении задачи классификации нарушителей информационной безопасности в автоматизированной системе» рассмотрена проблема построения модели нарушителя. Проведенные авторами исследования показали, что на сегодняшний день нет единого подхода к построению модели нарушителя. Существующие подходы, несмотря на то, что имеют ряд общих классификационных признаков, неполно описывают нарушителей, а категории нарушителей, описанные в различных источниках, не являются коррелированными. Для построения модели нарушителя предлагается использовать оригинальную методику, использующую классификационные признаки и категории нарушителей, соответствующие государственным стандартам, нормативно-методическим документам ФСТЭК России и ФСБ России. В результате проведенных исследований создана модель нарушителя в соответствии с указанными требованиями, что позволяет применять данную модель при защите государственных информационных ресурсов, для защиты которых требования государственных стандартов, нормативно-методических документов ФСТЭК России и ФСБ России являются обязательными для исполнения. Предложенная классификация нарушителей позволяет однозначно классифицировать нарушителей в соответствии с уровнями их воздействия, чего не было представлено ранее в существующих моделях.

Два доклада Ю.А. Брюхомицкого, ТТИ ЮФУ, г. Таганрог посвящены вопросам защиты информации с применением нового перспективного направления искусственного интеллекта – искусственных иммунных систем.

Первый доклад «Использование принципов построения и функционирования иммунных систем в компьютерной безопасности» носит концептуальный, постановочный характер. С позиции иммунологических принципов обеспечения безопасности живых организмов делается анализ предпосылок и возможности создания адаптивных моделей систем компьютерной безопасности, способных отличать «своего от «чужого». При этом система компьютерной безопасности рассматривается как надстройка к компьютерной системе, и в целом они образуют защищенную компьютерную систему, которая функционирует в потенциально враждебной внешней среде. Регулирование взаимоотношений защищенной компьютерной системы с внешней средой определяется принятой политикой безопасности. В случаях выявления нарушений информационной безопасности защищенная компьютерная система предпринимает определенные меры реагирования. Для эффективного решения задач компьютерной безопасности предлагается расширить применяемую для этих целей иммунологическую модель, основанную на алгоритме отрица-

тельного отбора, путем введения в нее свойств двойной пластичности – параметрической и структурной. Система компьютерной безопасности, созданная по такой схеме, будет представлять собой адаптивную самоорганизующуюся структуру, ориентированную на поддержание эффективного уровня обнаружения нарушений компьютерной безопасности, в условиях произвольно изменяющихся внутренних состояний информационной системы и внешних воздействий.

Второй доклад «Иммунологические принципы организации клавиатурного мониторинга пользователей компьютерных систем» конкретизирует предложенный иммунологический подход к моделированию систем скрытного клавиатурного мониторинга пользователей автоматизированных информационных систем. При этом решается задача верификации фактически работающего пользователя на основе применения уникального свойства иммунной системы по выявлению чужеродных для организма клеток – антигенов. Задача выявления «чужого» пользователя формализуется и решается с помощью алгоритма отрицательного отбора. Показаны иммунологические принципы представления и кодирования клавиатурных биометрических данных, построения процедуры обучения, которая сводится к созданию набора детекторов для обнаружения «чужих» пользователей. Рассмотрена схема функционирования системы, в которой статистическая вероятность клавиатурного присутствия в системе «чужого» определяется частотой срабатывания детекторов. Приведены основные особенности, отличающие данный подход от других известных подходов.

2. Безопасность информационно-телекоммуникационных систем. В рамках этого направления на Конференции было представлено 22 доклада отечественных специалистов. Тематика докладов весьма разнообразна и, в частности, включает в себя: методы и средства защиты компьютерных систем от сетевых атак; методы моделирования уязвимостей сетевых систем; методы и средства выявления аномалий в сетевой активности; совершенствование протоколов аутентификации; биометрические технологии идентификации пользователей; способы и механизмы защиты компьютерных систем связи; повышение качества межсетевых экранов; безопасное использование персональных средств идентификации; защиту систем электронного документооборота и др.

В докладе Е.В. Лапина, В.В. Золотарев, А.Е. Заболотникова, СГАУ им. академика М.Ф. Решетнева, г. Красноярск «О подходе к автоматизации анализа информационного риска систем электронного документооборота» представлен программный комплекс, автоматизирующий процедуру анализа оценки параметров документооборота. Основой подхода является выделение критериев эффективности, основанных на формальной модели композитного документооборота. Новизна данной работы заключается в разработке нового способа моделирования систем электронного документооборота (СЭД), позволяющего производить количественную оценку информационных рисков подобных систем. Результатом является повышение эффективности работы СЭД за счет использования автоматизированной системы, позволяющей анализировать информационные риски и получать адекватные оценки защищенности СЭД. Главными преимуществами данной модели являются: простота реализации, возможность адаптации к любому типу организации и возможность модификации в процессе построения. Разработанный программный комплекс может использоваться в организациях различного типа, таких как образовательные и медицинские учреждения, малый и средний бизнес, производственные предприятия. Использование программного комплекса позволит отследить и сбалансировать загруженность участников документооборота, получить рекомендации по улучшению работы СЭД, что в итоге позволит повысить эффективность СЭД. Главными преимуществами программного комплекса являются:

обширная база данных для оценки рисков и выбора контрмер с возможностью ее пополнения, что усиливает эффективность работы данной системы; использование метода не требует специальной подготовки и высокой квалификации аудитора; метод в одинаковой степени подходит как для аудита уже существующих информационных систем, так и для вновь проектируемых.

Доклад А.С. Коноплев, М.О. Калинин, Санкт-Петербургский государственный политехнический университет (СПбГПУ), г. Санкт-Петербург «Способ модельного представления механизмов защиты грид-систем» посвящен проблеме обеспечения безопасности ресурсов в грид-системах. В работе проанализированы особенности архитектуры грид-систем, построена модель угроз. Рассмотрены существующие меры по обеспечению безопасности грид-систем, указаны их недостатки. Авторами предложен подход, позволяющий обеспечить защиту от несанкционированного доступа (НСД) к ресурсам грид-систем на основе безопасного распределения запросов пользователей на выделение ресурсов в соответствии с требованиями политик информационной безопасности. Реализация данного подхода основана на модельном представлении отношений доступа в хостовых средах, учитывающем динамику состояний грид-систем и с этой целью использующем аппарат цветных функциональных сетей Петри. Это позволяет решать в формальном виде комплекс прикладных задач, направленных на обеспечение защиты ресурсов грид-систем от НСД. Предложенный способ модельного представления механизмов защиты грид-систем, реализация указанного программного модуля и его интеграция в состав провайдеров ресурсов позволяют автоматизировать процедуры контроля и анализа безопасности грид-систем, что направлено на обеспечение высокого уровня надежности и защищенности грид-систем используемых, в том числе, государственного, ведомственного и коммерческого применения.

Доклад Д.П. Зегжда, Т.В. Степанова, СПбГПУ, г. Санкт-Петербург посвящен «Оценке эффективности противостояния средств защиты целевым атакам со стороны бот-сетей». На сегодняшний день отсутствуют методы оценки эффективности противостояния средств защиты целевым атакам, направленным на сами средства защиты и организованных с помощью бот-сетей. Авторами предложен набор метрик оценки эффективности, учитывающих сетевую природу современных средств защиты и нападения. Предложенные метрики позволяют численно оценить факторы, влияющие на эффективность защиты или нападения, сделать вывод о результате противостояния сетей агентов защиты и сетей атакующих агентов, а, следовательно, и о защищенности узлов локальной или глобальной сети. Предложенный способ оценки характеристик сетей агентов предусматривает использование метрик, независимых от назначения сети агентов. Описанные характеристики предоставляют полное описание функционирования сети агентов и позволяют сопоставить эффективность функционирования различных бот-сетей и различных средств защиты, а также эффективность средств защиты для нейтрализации и устранения бот-сетей и эффективность противостояния бот-сетей различным средствам защиты.

Два доклада специалистов из Уфимского государственного авиационного технического университета (УГАТУ) были посвящены применению в сфере сетевой безопасности сравнительно нового метода линейной классификации – метода опорных векторов.

В первом докладе В.И. Васильев, И.В. Машкина, К.В. Миронов, И.В. Шарабыров «Разработка модели обнаружения сигнатур атак на основе метода опорных векторов» приводится описание метода опорных векторов (Support Vector Machine, SVM) для построения системы обнаружения вторжений, функционирующей на основе модели обнаружения сигнатур. В работе рассматривается возможность

применения специфического варианта SVM – LMRL (Large Margin Rectangle Learning – обучение на основе прямоугольных кластеров с максимальным зазором), который комбинирует принцип максимизации зазора с представлением каждого класса в виде набора прямоугольных кластеров, для построения классифицирующей модели системы обнаружения вторжений на компьютер, использующей технологию сигнатурного анализа. Задача сводится к созданию модели обнаружения атак, использующих некоторый общий фрагмент кода, уникальный для класса угроз, когда при помощи двух сигнатур с успехом может быть обнаружено все семейство угроз. Для решения этой задачи и строится классифицирующая модель на основе метода опорных векторов. Описаны результаты численного эксперимента, проведенного с помощью разработанного программного обеспечения. Использование метода опорных векторов позволяет в определенной степени нейтрализовать недостатки технологии обнаружения признаков.

Во втором докладе А.Ю. Сенцова, И.В. Машкина «Разработка моделей обнаружения аномалий в сети на основе метода опорных векторов» решается задача создания шаблона нормального состояния трафика сети, состоящего из трех кластеров, каждый из которых позволяет обнаружить определенный класс аномалий. Для этого разработана классифицирующая модель нормального состояния трафика на основе метода опорных векторов, который относится к методам линейной классификации. Использование метода опорных векторов позволяет в определенной степени нейтрализовать недостатки технологии обнаружения признаков и уменьшить требуемый размер оперативной памяти и время, которое затрачивает система обнаружения атак (СОА) на обработку информации.

В докладе А.П. Жук, Е.П. Жук, А.М. Трошков, Ставропольский государственный университет, г. Ставрополь предлагается «Способ передачи информации с псевдослучайной перестройкой формы сигналов для систем связи с кодовым разделением каналов». Способ заключается в том, что в качестве ортогональных расширяющих последовательностей используется система сигналов, описываемая собственными векторами диагональной симметрической матрицы A, коэффициенты которой задаются генератором псевдослучайных чисел. Количество структур ортогональных сигналов при любой размерности ансамбля, получаемых предлагаемым способом, больше, чем при использовании известных способов. Предложенный способ позволяет на основе множества собственных векторов диагональной симметрической матрицы A получить достаточно представительное множество структур дискретных ортогональных сигналов. Сравнительный анализ предложенного способа с наиболее известными способами многоканальной передачи информации, показал преимущество его использования для повышения структурной скрытности передаваемых сообщений. Увеличение числа структур сигналов формируемых предложенным способом и, как следствие, уменьшение вероятности их раскрытия может быть достигнуто за счет расширения диапазона возможных значений диагональных коэффициентов матрицы A.

Два доклада авторов В.М. Федоров, Д.П. Рублев, ТТИ ЮФ, г. Таганрог посвящены вопросам идентификации пользователя по особенностям его работы с клавиатурой и манипулятором «мышь».

В первом докладе «Методы предварительной обработки виброакустических сигналов от клавиатуры возникающих при наборе текста» рассмотрен вопрос об идентификации пользователя по виброакустическому сигналу, возникающему при наборе этим пользователем текста с клавиатуры. Разработан метод выделения моментов начала и окончания информативного сигнала. Исследованы спектры виброакустических сигналов. Для идентификации удерживаемой клавиши предложены признаки, в качестве которых использованы коэффициенты кепстра, вычисленные на основе коэффициентов линейного предсказания.

Во втором докладе представлены разработанные авторами методы «Фильтрации виброакустических сигналов от клавиатуры и манипулятора «мышь», возникающих при работе оператора». В частности, разработан метод фильтрации сигналов на основе спектрального вычитания и фильтра Винера. Отфильтрованные сигналы предполагается использовать для получения информационных признаков в системе идентификация пользователя.

В докладе Е.П. Тумоян, Д.А. Кавчук, ТТИ ЮФУ, г. Таганрог «Оптимизация проверки уязвимостей информационных систем на основе вероятностного нейросетевого моделирования атак» предложен метод, который использует моделирование сетевых атак для оптимизации проверки уязвимостей удаленных информационных систем. Моделирование атак производится на основе вероятностного дерева атак с применением искусственной нейронной сети. Для тестирования и анализа эффективности метода разработана программная система анализа защищенности информационных систем, реализующая предложенный метод. Разработанный метод позволяет провести проверку уязвимостей за меньшее количество попыток эксплуатации при заданной доверительной вероятности обнаружения всех известных уязвимостей. Кроме того, метод также позволяет проводить проверку многостадийных атак.

В докладе В.А. Михеев, А.В. Уткин, «Инженерно-маркетинговый центр Концерна «Вега», г. Москва «К вопросу о защите информации в системах радиочастотной идентификации высокого уровня сложности» обсуждаются вопросы информационной безопасности в условиях применения технологий радиочастотной идентификации (RFID), которые все больше замещают технологии штрихового кодирования. RFID, обладая значительно большими преимуществами по сравнению с традиционными системами штрихового кодирования, имеют свои ограничения, связанные с уязвимостью и несовершенством защиты данных, циркулирующих в радиочастотном интерфейсе между радиочастотной меткой и считывателем. На основании проведенного в работе анализа делается вывод, что вопросы обеспечения защиты информационной среды в RFID-системах требуют: разработки и реализации организационных и технических мероприятий по защите от технических средств на разных стадиях жизненного цикла RFID-систем; разработки и внедрении конструктивных и технических решений по защите RFID-системы от злоумышленника. В свою очередь, защита от злоумышленника может достигаться путем: исключения НСД к обрабатываемой или хранящейся в RFID-системах информации; предотвращения специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе RFID-системы; организации разрешительной системы допуска пользователей и обслуживающего персонала RFID-системы; соблюдения режима конфиденциальности.

Два доклада Конференции были посвящены вопросам качества функционирования межсетевых экранов.

В первом докладе Д.В. Кетов, «Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики», г. Санкт-Петербург рассматривается проблема динамической «Целостности прикладных процессов во встраиваемых операционных системах МСЭ». Предлагаются механизмы и технические средства, основанные на использовании проверок «естественных» правил. По сравнению с известными решениями предлагаемый подход не требует построения управляющего графа программы и имеет явно выраженную прикладную направленность на противодействие наиболее распространенным атакам, эксплуатирующим подмену адреса возврата из функции или адреса вызова (косвенного) функции. Встраиваемые IRM (Inline Reference Monitor) мониторы не требуют знания о структуре программ и графа вызовов и как следствие могут быть легко реализованы на уровне компилятора исходных текстов программ или инструментов постобработки бинарных файлов программ.

Во втором докладе Е.С.Абрамов, Е.С. Баранник, ТТИ ЮФУ, г. Таганрог представлена разработанная авторами «Методика исследования реализации stateful-фильтрации в межсетевых экранах». Разработана программная система, которая обеспечивает возможность проведения тестирования различных моделей МСЭ и позволяет определить, снабжен ли МСЭ функцией stateful-фильтрации. Приводятся результаты исследования нескольких моделей МСЭ. Благодаря тому, что разработанная система тестирования учитывает различные факторы, которые могут нарушить безопасность системы и имеет узкое направление, касающееся исключительно stateful-фильтрации, она может успешно использоваться на практике для выявления уязвимостей МСЭ.

Два доклада специалистов из ТТИ ЮФУ г. Таганрога были посвящены безопасному использованию пластиковых карт.

В первом докладе Л.К. Бабенко, Д.А. Беспалов, Р.Д. Чесноков «Аппаратный модуль регистрации протоколов обмена бесконтактных пластиковых карт» приводится описание завершенного программно-аппаратного комплекса, позволяющего регистрировать протоколы обмена в электромагнитном поле между терминальным устройством и бесконтактной картой, накапливать полезные транзакции, передавать их на ПЭВМ и проводить там первичный анализ с переводом временных дейтаграмм в байтовые последовательности. Для регистрации принимаемых данных авторами был использован подход, используемый в логических анализаторах: детектирование фронта или спада сигнала с измерением их длительности в дискретных отсчетах времени, кратных частоте принимаемого сигнала, до появления следующего перепада логического уровня. Данный подход позволяет избежать пропуска момента смены состояния или регистрации только части принимаемой последовательности. Зарегистрированные таким образом данные подлежат передаче на персональный компьютер, где происходит их дальнейшая обработка и представление в символьном виде. Данный комплекс может быть использован в составе любых инструментальных систем для разработки или анализа комплексов защиты информации с применением бесконтактных пластиковых карт.

Во втором докладе О.Б. Макаревич, Д.А. Беспалов, Р.Д. Чесноков приводится описание «Программного комплекса для анализа протоколов обмена данными в системах бесконтактной идентификации». Комплекс позволяет получить выборку активных сеансов обмена данными между бесконтактными пластиковыми картами и терминальными устройствами для последующего анализа оператором или автоматизированной системой. Полученная информация может существенно повысить эффективность методов анализа защищенности таких систем от угрозы проникновения, взлома, копирования и подмены данных. Полученное авторами решение можно также использовать в системах защиты информации с применением бесконтактных карт для отладки устройств контроля доступа, терминалов, систем считывания данных и т.п.

В докладе М.А. Еремеев, А.Г. Ломако, В.А. Овчаров, С.А. Акулов, В.С. Коротков, Н.В. Свергун, Военная космическая академия им. А.Ф. Можайского, г. Санкт-Петербург представлен разработанный авторами «Метод адаптивного управления активным сетевым оборудованием телекоммуникационной сети в условиях компьютерных атак». Метод обеспечивает: противодействие импульсным и лавинообразным сетевым атакам; получение, хранение и использование базы данных характеристик объекта управления, потоков, соответствующих продукций; расчет характеристик активного сетевого оборудования. Для моделирования архитектуры сети заданного типа, имитации атак, контроля производительности авторами разработан экспериментальный стенд и предложена структура динамически реконфигурируемой технологической сети, позволяющая эффективно осуществлять управление активным сетевым оборудованием.

3. Защита объектов информатизации. В рамках этого направления на Конференции было представлено 7 докладов российских специалистов. Тематика докладов включает информационные, технические и организационные методы, способы и средства защиты, направленные на комплексную защиту объектов информатизации. На секции представлен опыт разработки и практического применения средств защиты для различных категорий объектов информатизации.

Доклад А.Н. Шниперов, К.Н. Захарьин, Сибирский федеральный университет, г. Красноярск «Вопросы разработки комплексной системы защиты информации для распределённой мультиагентной среды электронного обучения» был посвящен проблеме комплексной защиты сложных объектов информатизации, в качестве которых выступают мультиагентные системы электронного обучения (МСЭО). Особенностями проектируемой авторами МСЭО является открытость для подключения из сети интернет, способность функционировать в высоконагруженном режиме. МСЭО характеризуется также разнородностью своих функциональных агентов, их гибкой расширяемостью, а также распределенностью по узлам. Агенты системы защиты информации (СЗИ), представляют собой отдельные программные модули, реализующие решение определенных задач обеспечения информационной безопасности. Архитектура СЗИ предполагает разделение всей МСЭО на периметры безопасности, представляющие собой либо выделенный узел сети, либо группу узлов, выделенную в свое адресное пространство. На каждом периметре безопасности предусмотрено несколько агентов безопасности, каждый из которых отвечает за свой функционал (шифрование, доступ, контроль целостности процессов и т.д.) и взаимодействует с агентом-координатором периметра безопасности. Агенты-координаторы в свою очередь осуществляют взаимодействие друг с другом с целью оценки безопасности всей МСЭО и в случае возникновения угрозы могут предпринять соответствующие меры.

В докладе Степанова, Р.М. Хабибуллин, И.В. Машкина, УГАТУ, г. Уфа описывается «Программная система оценки рисков нарушения информационной безопасности на основе построения нечетких когнитивных карт». В разработанном методе при решении проблемы оценивания рисков нарушения информационной безопасности предложено производить детализацию структуры информационной системы до уровня сегментов сети. В качестве объекта атаки рассматриваются активы, обрабатываемые в сегменте сети. Пользователи рабочих станций другого сегмента сети рассматриваются как потенциальные внутренние нарушители – источники атак. Внешними источниками атак являются удаленные пользователи, обладающие правами доступа к информационной системе, и злоумышленники. Произведена апробация разработанной программной системы для конкретного объекта защиты. Результаты показали работоспособность и устойчивость программной системы к некорректным входным данным.

В докладе Е.А. Максимова, В.А. Корнева, Волгоградский государственный университет, г. Волгоград «Оптимизация технологии безопасного информационного взаимодействия в корпоративных системах» информационное взаимодействия рассматривается на внутри процессорном уровне, в рамках одного автоматизированного рабочего места, на уровне локальной сети и как межсетевое взаимодействие. На каждом уровне исследованы угрозы безопасности и технологии информационной защиты корпоративных систем. В качестве решения вопроса оптимизации технологии безопасного информационного взаимодействия предложен протокол безопасного обмена асинхронными ключами с использованием закрытого алгоритма преобразования ключа, с целью проверки его аутентичности. Применение разработанного протокола позволяет противодействовать угрозам типа «Maninthemiddle». Однако в комплексе необходимо использовать специализированные средства для защиты периметра сети, что позволит защитить систему в обход криптографических средств защиты.

4. Методы и средства криптографии и стеганографии. В рамках этого направления на Конференции был представлен 16 докладов по актуальным проблемам криптографии, криптоанализа, стеганографии и стегоанализа, включая методы, алгоритмы, методики, способы реализации.

В докладе В.Ю. Пластунов, ФГУП «Атомфлот», г. Мурманск «Технология встраивания цифрового водяного знака» представлена обширная информация по определению места использования технологии встраивания цифрового водяного знака (ЦВЗ) среди других направлений защиты мультимедийной информации. Автором проанализированы история появления и актуальность ЦВЗ, определены основные понятия ЦВЗ и критерии эффективности ЦВЗ, рассмотрены схема встраивания и классификация ЦВЗ, выделены особенности ЦВЗ по отношению к криптографическим методам и другим методам стеганографии, сформулированы математические выражения, описывающие в общем виде систему встраивания ЦВЗ. Предложенная математическая запись системы встраивания ЦВЗ, может быть использована для формального описания задач при разработке новых способов встраивания ЦВЗ и их исследований.

Доклад Е.С. Чиркин, Н.Л. Королева, Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, «Защита контента веб-страниц от несанкционированного копирования» посвящен проблеме незаконного заимствования (текстового) контента, имеющего коммерческую ценность. Целью работы является демонстрация возможности технической защиты от несанкционированного воспроизведения контента, ее несостоятельность и ее возможности в качестве вспомогательного инструмента, облегчающего последующую защиту в правовом поле. В рамках данной работы был создан программный комплекс по внесению ЦВЗ в HTML-документы с помощью предложенных подходов.

Два доклада по данному направлению представлены С.А. Диченко и О.А. Финько из Краснодарского филиала Военной академии связи, г. Краснодар.

В первом докладе «Алгоритм контроля ошибок вычисления булевых функций при представлении их линейными числовыми полиномами и устройство для его реализации» представлены алгоритм и устройство его реализации, обеспечивающее параллельное вычисление систем булевых функций при представлении их линейными числовыми полиномами. Параллельная реализация дополнена подсистемой контроля ошибок вычислений, основанной на свойствах избыточных арифметических AN-кодов. Устройство предназначено для построения шифраторов с повышенными требованиями к сбоеустойчивости, а также для любых систем, реализующих логические вычисления.

Во втором докладе описаны разработанные авторами «Параллельные алгоритмы генерации псевдослучайных чисел, основанные на конгруэнтных методах», представленные в алгебраической и матричной формах. Актуальность работы определяется постоянным ужесточением требований к скорости шифрования и увеличению объемов защищаемой информации, что вызывает объективную необходимость построения параллельных алгоритмов генерации псевдослучайных чисел. Приведена сравнительная оценка рассматриваемых и существующих алгоритмов.

В докладе В.М. Шелудько, ТТИ ЮФУ, г. Таганрог «Ускорение шифрования данных по алгоритму ГОСТ 28147-89 в режиме простой замены с помощью технологии CUDA» на примере блочного криптоалгоритма ГОСТ 28147-89 рассматривается практическое применение технологии CUDA (Compute Unified Device Architecture) параллельного программирования для вычислений на GPU (Graphic Processing Unit) производства корпорации NVIDIA. Рассматриваются эффективная программная реализации алгоритма и исследование примененных методов оптимизации программной реализации алгоритма. Автором разработана программа для

операционных систем семейства Windows, которая позволяет зашифровывать и расшифровывать файлы по алгоритму ГОСТ 28147-89 в режиме простой замены с выполнением криптографического преобразования как на CPU (Central Processing Unit), так и на GPU, в зависимости от задаваемых настроек. При разработке и тестировании программы исследованы факторы, влияющие на скорость выполнения криптографического преобразования при программной реализации на CPU и GPU. При реализации шифрования данных на GPU достигается не только значительно более высокая скорость шифрования, но и снижается загрузка центрального процессора ПК, что влечет повышение общей производительности защищенных систем.

В докладе Т.А. Гришечкина, ТТИ ЮФУ, г. Таганрог «Исследование и модификация передачи ключей авторизации в сетях стандарта IEEE 802.16» рассматривается усовершенствование существующей модели сети WiMAX для повышения эффективности использования алгоритма шифрования. В частности, изложен переход от шифрования RSA, который используется при передаче ключа авторизации, к шифрованию NTRU. Из ключа авторизации формируется ключ шифрования трафика TEK (Traffic Encryption Key) и HMAC (Hashed Message Authentication Code). Предлагаемое усовершенствование поможет снизить угрозу возможности повторного использования ключей TEK за счет уменьшения времени шифрования и дешифрования ключей авторизации и, тем самым, позволит сократить их срок действия без ущерба для вычислительных ресурсов базовых приемопередающих станций.

В докладе Л.К. Бабенко, Л.С. Крамаров, ТТИ ЮФУ, г. Таганрог представлены особенности «Реализации коллективной электронной цифровой подписи на основе задачи извлечения корней по модулю», а также результаты проведенных экспериментов, которые показали эффективность реализованного алгоритма коллективной электронной цифровой подписи (КЭЦП). Процедура формирования КЭЦП занимает время, пропорциональное числу пользователей, участвующих в подписании. Алгоритм применим в системах электронного документооборота, для коллегиального подписания документов.

В докладе Л.К. Бабенко, Е.А. Ищукова, Е.А. Щеткина, ТТИ ЮФУ, г. Таганрог «Подходы к анализу новой функции хэширования Skein» представлено новое семейство криптографических хэш-функций Skein, являющихся одним из финалистов конкурса SHA-3, проводимым Национальным институтом стандартов и технологий США (НИСТ). В работе рассматриваются основные особенности построения алгоритма Skein и исследуются некоторые подходы к анализу стойкости данной функции хэширования.

В докладе А.Ф. Чипига, И.А. Калмыков, Е.М. Яковлева, М.И. Калмыков, Северо-Кавказский государственный технический университет, г. Ставрополь «Применение полиномиальной системы классов вычетов в схеме разделения секрета» рассмотрена модификация пороговой схемы разделения секрета, функционирующей в базисе полиномиальной системы классов вычетов. Применение ПСКВ дает возможность реализовать эффективную систему разделения секрета, позволяющей группе авторизованных пользователей восстанавливать общий секретный ключ по его образам.

5. Безопасность программного обеспечения. В рамках этого направления на Конференции было представлено 7 докладов по вопросам поиска и обнаружения уязвимостей программного обеспечения (ПО), построения систем защиты от вредоносных программ, анализа безопасности программного кода, классификации вредоносного ПО и др.

Доклад А.В. Благодаренко, О.Б. Макаревич, ТТИ ЮФУ, г. Таганрог был посвящен «Разработке метода, алгоритмов и программ для автоматического поиска уязвимостей программного обеспечения в условиях отсутствия исходного кода»,

который обладает следующими возможностями: обеспечивает автоматический поиск уязвимостей программного обеспечения в условиях отсутствия исходного кода; позволяет получать оценку покрытия программного обеспечения тестами, отслеживать реакции тестов на исследуемое программное обеспечение и получать количественные характеристики завершения тестовых испытаний; позволяет автоматически выбирать точку внедрения, что сокращает объем входных данных для обеспечения заданного покрытия; позволяет покрывать участки кода, отвечающие за обработку аварийных ситуаций за время, пропорциональное количеству таких участков.

В докладе А.С.Марков, А.А. Фадин, ЗАО «НПО «Эшелон», г. Москва «К вопросу о выявлении дефектов безопасности методом статического сигнатурного анализа» рассмотрен сигнатурный анализ безопасности программного кода. Приведены примеры выявляемых дефектов безопасности. Предложена методика выполнения сигнатурного анализа кода с целью выявления дефектов безопасности. К достоинствам сигнатурного метода статического анализа относятся относительная простота реализации, высокая скорость работы, а также легкость портирования сигнатур на различные платформы и языки программирования. Недостатком сигнатурного подхода является необходимость учитывать различные «вариации» конструкций и блоков кода, которые допускает синтаксис языка программирования и логика выполнения программы. Поэтому наиболее эффективной роль сигнатурного анализа видится авторами в исследовании зависимостей модулей программ и внешних компонент, поиске вызовов функциональных объектов, а также проверке содержимого информационных объектов программы.

Доклад А.Т. Алиев ООО НПО «Редут», г. Ростов-на-Дону, «Построение проактивной системы защиты от вредоносных программ» посвящен анализу и сопоставлению используемых в настоящее время методов выявления вредоносных программ. Показана необходимость разработки антивирусных средств основанных на проактивных методах обнаружения вирусов и вредоносного программного обеспечения. Рассматриваются принципы построения проактивной системы защиты операционных систем семейства Windows, приводится архитектура таких систем, алгоритмы принятия решения и способы снижения вероятности ложных срабатываний. Полученные автором результаты подтвердили

перспективность проактивных методов анализа как направления развития антивирусных средств защиты.

В докладе Тумоян Е.П., Бабенко Л.К., Цыганок К.В., Аникеев М.В., ТТИ ЮФУ, г. Таганрог предложен новый «Метод поведенческого анализа для классификации вредоносного программного обеспечения». Авторами разработаны алгоритмы вычисления меры близости программ, основанные на анализе последовательностей вызовов WinAPI программ и их аргументов, а также файлов создаваемых анализируемым приложением. Для классификации полученных данных используется модифицированный алгоритм нечеткой кластеризации. Метод обеспечивает оценку близости и кластеризацию образцов вредоносного программного обеспечения (ВПО) на основе поведенческих признаков. Полученные кластеры используются для классификации ВПО. Метод обеспечивает не только классификацию образцов ВПО, но и в отличие от других методов предоставляет информацию, которую эксперт может оценить визуально и интерпретировать в терминах предметной области. Метод был экспериментально проверен на реальных образцах вредоносного программного обеспечения.

В докладе А.В. Барабанов, М.И. Гришин, ЗАО «НПО «Эшелон», г. Москва представлены «Предложения по формированию метабазиса оценки соответствия DLP-решений по требованиям безопасности информации». В основу предложений положен подход стандарта «Общие критерии». Представленный метабазис может

применяться при сертификации DLP-решений (data loss prevention) по требованиям безопасности информации для увеличения детерминированности данного процесса. Представленный подход может найти практическое применение в процессе проведения сертификационных испытаний в системе сертификации средств защиты информации ФСТЭК России.

В докладе Е.А. Ларионцева, Н.Н. Стельмашук, ЗАО «НПО «Эшелон», г. Москва представлена «Разработка методики испытаний систем обнаружения вторжений в соответствии с положениями новой нормативной базы». Авторами разработана математическая модель оценки соответствия системы обнаружения вторжений 6-го класса уровня узла, рассмотрены особенности и оптимизация сертификационных испытаний на соответствие им. В работе предложены некоторые методические подходы, позволяющие наиболее оптимально проводить трудоемкие испытания и сократить затраты на проведение оценки соответствия СОВ новой нормативной документации ФСТЭК России.

6. Прикладные вопросы информационной безопасности. В рамках этого направления на Конференции было представлено 12 докладов по вопросам применения принципов, подходов, методов, средств информационной безопасности для решения задач в различных прикладных областях. Кроме того, в это направление вошли доклады, проблематика которых выходит за рамки предыдущих пяти тематических направлений работы конференции.

В докладе С.В. Котенко, К.Е. Румянцев, ТТИ ЮФУ, г. Таганрог «Комплексная аутентификация банковских систем» представлены результаты исследования эффективности аутентификации банковских систем на основе комплексного определения разборчивости и избыточности виртуальных идентификаторов. Приводится система функций разработанного на этой основе комплекса аутентификации банковских систем. Определяются модели формирования идентификаторов и аутентификации. Основные отличительные особенности разработанного комплекса обозначают впервые открывающуюся возможность управления аутентификацией на пользовательском уровне.

Доклад М.Н. Осипов, И.Н. Фалилеев, А.Н. Чекменев, Ю.Д. Щеглов, СГУ, г. Самара посвящен «Особенностям регистрации акустического сигнала на основе анализа спекл-структур». Одними из перспективных направлений регистрации акустического сигнала являются лазерные методы съема информации. В данной работе рассматривается применение спекл-интерферометрии для регистрации акустического сигнала. Предложена оптическая схема с использованием волоконно-оптических элементов для регистрации спекл-структур, модулированных акустическим сигналом. Приведена оценка диапазона применимости предлагаемой лазерной оптоэлектронной системы регистрации акустического сигнала на основе спеклинтерфереметрии.

В докладе Э.Э. Яндыбаева, УГАТУ, г. Уфа проводится «Анализ угроз информационной безопасности при использовании электронной подписи». Данный вопрос является актуальным в связи с массовым переходом на электронный документооборот и применением технологии электронной подписи в государственных учреждениях и коммерческих организациях на территории Российской Федерации. В результате исследования была разработана и составлена классификационная схема угроз безопасности. Наиболее опасной угрозой, по мнению автора, является подмена документа при передаче его на подпись. Данный вид угрозы требует создания принципиально новых схем защиты.

В докладе В.В. Копытов, В.И. Петренко, Д.Н. Суховей, СГУ, г. Ставрополь «Методика расчета затрат от нарушений защищаемой медицинской информации» приводится методика расчета затрат для медицинских учреждений от невыполне-

ния требований по безопасности защищаемой медицинской информации. Цель предлагаемой методики: снижение затрат от нарушений защищаемой медицинской информации. Использование предложенной методики позволит медицинским учреждениям определять величину инвестиций в повышение уровня конфиденциальности и безопасности.

В докладе А.М. Трошков, М.А. Трошков, А.П. Жук, Е.П. Жук, СГУ, г. Ставрополь «Исследование применения мульти-многофакторных биометрических характеристик аутентификации личности и криптографическая защита» предлагаются и описываются усовершенствованные системы биометрической защиты: мультибиометрия и многофакторная аутентификация. Предлагаемые системы биометрической защиты позволяют повысить защищенность биометрических характеристик и параметров. Для повышения защищенности биометрических характеристик в мультибиометрии и многофакторной аутентификации предложена и описана процедура кодирования биометрических параметров с последующей криптографией.

В докладе А.Ф. Чипига, И.А. Калмыков, Р.А. Воронкин, В.Ю. Бабкин, СевКавГТУ, г. Ставрополь представлен «Объектно-ориентированный подход к разработке системы для безопасного хранения конфиденциальной информации на устройствах под управлением ОС Android». Устройства под управлением ОС Android получили большое распространение в последнее время. К таким устройствам можно отнести ноутбуки, планшеты, КПК, электронные книги, смартфоны (коммуникаторы). Подавляющее число пользователей хранит на своих устройствах конфиденциальную информацию как личную, так и служебную. Но она никак не защищена и при утере устройства, что является основной угрозой конфиденциальной информации на мобильных устройствах, возможен беспрепятственный доступ злоумышленника к защищаемой информации. В работе описана программа для безопасного хранения конфиденциальной информации на устройствах под управлением ОС Android. Программа решает проблему утечки конфиденциальной информации при утере, краже или несанкционированном доступе к устройству.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Материалы XII Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2012. – 346 с.
2. Материалы XII Международной научно-практической конференции «Информационная безопасность». Ч. II. Материалы II Всероссийской молодежной конференции «Перспектива-2012. – Таганрог: Изд-во ТТИ ЮФУ, 2012. – 222 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@tsure.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; профессор.

Bryukhomitsky Yuri Anatol'evich – 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; 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 department; professor.