УДК 004.056

# СОВРЕМЕННЫЕ МЕТОДЫ МАРКИРОВАНИЯ НЕПОДВИЖНЫХ ИЗОБРАЖЕНИЙ В ЧАСТОТНОЙ ОБЛАСТИ

**В.А. Батура**
**Научный руководитель – д.т.н., профессор А.Ю. Тропченко**

**Краткое введение, постановка проблемы.** С развитием информационных технологий резко возросла угроза нарушения прав интеллектуальной собственности, связанная с потенциальной возможностью ее неограниченного тиражирования через электронные каналы передачи данных. Цифровые водяные знаки (ЦВЗ) на данный момент являются одним из самых эффективных средств защиты мультимедийной информации от незаконного распространения и модификации. Цифровое маркирование – динамично развивающаяся область защиты интеллектуальной собственности. Каждый год ученые разрабатывают новые алгоритмы внедрения ЦВЗ или модификации уже имеющихся.

**Целью работы** является обзор некоторых современных методов цифрового маркирования неподвижных изображений в частотной области, разработанных за последние несколько лет.

**Базовые положения исследования.** Большинство исследований цифрового маркирования посвящено использованию изображений в качестве носителей водяного знака (стегаконтейнеров). Главными причинами этому служит фиксированный размер контейнера, наличие шумовых структур в изображении, а также слабая чувствительность человеческого глаза к незначительным искажениям изображения.

При использовании методов внедрения ЦВЗ в частотную область чаще всего используются дискретные косинусные преобразования (ДКП) и дискретные вейвлет-преобразования (ДВП). Этому есть две причины. Во-первых, соответствующие преобразования эффективно используются при сжатии изображения. Во-вторых, ДКП используется в формате JPEG, а ДВП – в JPEG2000 соответственно. Поэтому использование данных преобразований при встраивании ЦВЗ в изображения вышеперечисленных форматов повышает стойкость ЦВЗ к компрессии изображения.

**Промежуточными результатами работы** является выявление следующих преимуществ рассмотренных методов внедрения ЦВЗ:

- стойкость к атакам подделки и коллажа, а также высокая точность обнаружения места подделки изображения в схеме полу-хрупкого водяного знака автора Radu O. Preda;
- эффективность использования алгоритма на основе сходства самоорганизующихся карт для искусственных нейронных сетей в целях создания ЦВЗ в системе FFDW;
- повышение безопасности встраивания ЦВЗ в алгоритме авторов Qiaolun Gu и Tiegang Gao за счет использования хаотических систем.

**Выводы.** В современных методах цифрового маркирования используются различные вспомогательные методы: от хаотических систем до искусственных нейронных сетей. Нейронные сети являются очень перспективной технологией для создания ЦВЗ на основе контейнера. В работе был проведен краткий обзор некоторых современных эффективных методов цифрового маркирования неподвижных изображений в частотной области, разработанных учеными за последние несколько лет. Было приведено краткое описание методов, выделены их достоинства и недостатки, требующие последующей доработки.

УДК 004.7

# ВЛИЯНИЕ КОДЕКОВ VOIP НА КАЧЕСТВО ПЕРЕДАЧИ ГОЛОСОВОГО ТРАФИКА В СЕТИ WIMAX

**Г.М. Ваттимена**
**Научный руководитель – д.т.н., профессор Т.И. Алиев**

Одним из широко используемых сервисов в IP-сетях является VoIP (Voice over Internet Protocol) – технология передачи голосового трафика по IP-сети. Качество передачи голоса в таких сетях определяется задержками передачи пакетов, которые в свою очередь зависят от пропускной способности среды передачи данных. В последние годы все более широкое применение находят беспроводные технологии передачи данных, в частности технология WiMAX (Worldwide Interoperability for Microwave Access), которая в состоянии предоставить услуги передачи данных со скоростью до 70 Mbps в радиусе до 50 км.

Основной проблемой при реализации VoIP в WiMAX-сети является выполнение требований к качеству передачи голосового трафика, которые сформулированы в рекомендациях RFC в виде ограничений на такие параметры QoS (Quality of Service), как задержка передачи, джиттер и вероятность потери пакетов в сети передачи данных. Значения этих параметров в значительной степени зависят от способа кодирования, реализованного в кодеках.

В сети WiMAX могут использоваться различные кодеки (G.711 G.723 и G.729) для кодирования и декодирования передаваемых данных, рекомендованные международным союзом электросвязи (ITU-T). Кодек используется на стороне абонента для преобразования аналогового сигнала в цифровые импульсы. Среди этих кодеков G.711 и G.729, наиболее часто используемые кодеки в сети WiMAX.

В работе исследуется влияние кодеков G.711, G.723 и G.729 при использовании их в WiMAX-сети на показатели QoS при передаче голосового трафика. Исследования проводятся с использованием симулятора OPNET, с помощью которого определяются и анализируются параметры QoS при передаче пакетов из конца в конец.

В работе рассмотрены три модели WiMAX-сети с одной базовой станцией (БС), различающиеся количеством абонентских станций (АС), а именно: 12 АС, 50 АС и 90 АС. Радиус ячейки – 1 км. Для каждого из трех кодеков (G.711, G.729 и G.723) были проведены имитационные эксперименты в среде OPNET, длительность каждого из которых составляла 30 минут реального времени.

Результаты моделирования демонстрируют различия в характеристиках трех стабильных кодеков. Значение задержки при передаче пакетов из конца в конец в сети с 12-ю АС для кодека G.729 выше, чем для кодеков G.711 и G.723. Для кодеков G.729 и G.723 значение задержки не превышало допустимое стандартом значение 150 мс. Однако в случае 50 АС и 90 АС кодек G.711 имеет значение задержки, превышающее 150 мс.

Наименьшее значение джиттера задержки выявлено для кодека G.729 по сравнению с кодеками G.711 и G.723. Для кодека G.711 с увеличением числа пользователей (АС) джиттер задержки растет значительно быстрее по сравнению с другими кодеками, причем этот рост пропорционален росту числа пользователей. Для чувствительных к задержкам сетей, таких как VoIP, положительные значения джиттера являются нежелательными.

Моделирование и исследование кодеков было проведено для оценки производительности VoIP для WiMAX-сети с использованием среды моделирования OPNET. Проанализированы несколько важных параметров, таких как задержки из конца в конец и джиттер задержки. Голосовые кодеки G.711, G.723 и G.729 были смоделированы так, чтобы найти наиболее подходящие голосовые кодеки для VoIP через сеть WiMAX. Результаты моделирования свидетельствуют о том, что кодек G.729 очень хорошо использовать в сети WiMAX. К тому же G.729 не требует большой пропускной способности и обеспечивает требуемое качество передачи голосового трафика.

УДК 004.272

# СРАВНЕНИЕ ИСПОЛЬЗУЕМЫХ РЕСУРСОВ И ЗАТРАТ ПРИ РЕАЛИЗАЦИИ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ ВОЗМОЖНОСТЯМИ JAVA

**Д.А. Воронина**
**Научный руководитель – к.т.н., ассистент В.В. Соснин**

Параллельные вычисления – способ организации вычислений, при котором независящие друг от друга последовательности операций некоторой программы исполняются в один промежуток времени на разных вычислителях, что существенно снижает общие временные затраты на выполнение всей программы. Хотя термин «Параллельные вычисления» охватывает не только вопросы параллелизма в программировании, но и аппаратные интерфейсы, поддерживающие возможности параллельного выполнения процессов, наибольшую практическую ценность в настоящее время имеют исследования и разработки в области параллельных алгоритмов и внедрения их при разработке программных продуктов.

**Целью работы** является исследование применимости различных возможностей языка Java, предоставляемых в рамках поддержки параллелизма, к ряду разнородных задач. Как и в любой системе, в стеке технологий параллелизма языка Java с повышением уровня абстракции значительно упрощается процесс решения типовых задач, однако за счет потери гибкости и контроля над исполнением решение нетиповых задач становится неэффективным.

Язык Java предоставляет набор полезных низкоуровневых примитивов для синхронизации, но в их использовании много тонкостей, связанных с производительностью, взаимной блокировкой, доступностью, управлением ресурсами и безопасностью потоков. Поэтому разработчиками был создан пакет утилит для реализации параллелизма, включая блокировки, взаимные исключения, очереди, пулы потоков, облегченные задачи, эффективные параллельные коллекции, атомарные арифметические операции и другие базовые строительные блоки параллельных приложений. Этот пакет называется util.concurrent, и он образует основу пакета java.util.concurrent в JDK. Таким образом, в языке Java для каждой задачи необходимо найти некоторый компромисс между применением высокоуровневых абстракций из пакета java.util.concurrent и низкоуровневых инструментов, реализованных непосредственно в самом языке.

В работе анализируются ресурсы и затраты при реализации многопоточности на различных типовых задачах средствами JDK с помощью средства JProfiler, таких как время выполнения, затраты по потребляемой памяти, количество используемых классов и методов. В результате были сформулированы рекомендации по использованию возможностей реализации параллельных вычислений языка Java, позволяющие рационально их использовать в зависимости от решаемой задачи.

УДК 004.6

# ИССЛЕДОВАНИЕ МЕТОДОВ ОПИСАНИЯ ИНФОРМАЦИОННЫХ ПОТОКОВ В СЕТИ ИНТЕРНЕТ

**Н.С. Гордеев**
(Волжский политехнический институт (филиал) «Волгоградский государственный технический университет»)
**Научный руководитель – к.т.н., доцент Д.Н. Лясин**
(Волжский политехнический институт (филиал) «Волгоградский государственный технический университет»)

В настоящее время происходит стремительное развитие информационно-коммуникационной инфраструктуры. С каждым днем размеры информационных потоков становятся все больше и больше, а найти в них необходимую информацию становится все сложнее и сложнее. Наряду с увеличением количества информации увеличивается и количество ее источников. Это породило ряд проблем, связанных с хранением и обработкой больших объемов данных. Существующие программные средства, методики и алгоритмы не всегда справляются с поставленной задачей, поэтому необходимо их совершенствовать, а также разрабатывать новые. Именно поэтому основная **цель исследования** – выявить закономерности в поведении информационных потоков сети интернет и изучить возможности их использования для анализа и прогнозирования.

В исследовании предпринята попытка детально рассмотреть технологии и принципы контент-мониторинга, используемые при решении различных типов задач. В частности, предлагается рассмотрение динамики тематических потоков новостной информации в рамках логистической модели. На основе этих принципов разработана методика сбора информации, которая позволяет проводить систематизацию и анализ полученных данных. Процесс сбора и анализа информации автоматизирован путем создания программного модуля, который позволяет ускорить обработку полученных данных.

Анализ информационных потоков позволяет отследить процесс зарождения новой темы, а методы экстраполяции позволяют прогнозировать дальнейшее ее развитие. Это исследование позволяет следить за процессами развития и старения информации, а также выявить резонанс, созданный данной темой в реальном и виртуальном мире.

Результаты, полученные, при исследовании информационных потоков позволяют:

– проанализировать информационные потоки с целью количественного изучения динамики отдельных тематических направлений;
– установить насколько точно математическая модель описывает наблюдаемые информационные потоки сети интернет;
– сделать выводы о возможных параметрах настройки разработанного программного модуля.

**Литература**

1. Ландэ Д.В. Основы интеграции информационных потоков. – К.: Инжиниринг, 2006. – 240 с.
2. Брайчевский С.М., Ландэ Д.В. Современные информационные потоки: актуальная проблематика // Научно-техническая информация. – 2005. – Сер. 1. – №11. – С. 21–33.
3. Ландэ Д.В., Морозов А.Ю. Новостной Интернет // Телеком. – 2005. – №1–2. – С. 58–62.

УДК 532.783

# МЕТОДЫ ВИЗУАЛИЗАЦИИ СТРУКТУРЫ ПОВЕРХНОСТИ СУХИХ ОСТАТКОВ ЖИДКОСТЕЙ НА ОСНОВЕ ЖК ДЛЯ НУЖД ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**В.И. Данилюк**
**Научный руководитель – д.т.н., профессор М.Г. Томилин**

Визуализации структуры материалов является актуальной задачей для многих областей биологии, химии, материаловедения и информационных технологий. Структура материала определяет многие его свойства, открывая возможности их практического использования. Эта проблема актуальна еще и потому, что многие структуры вообще не наблюдаются в оптический микроскоп.

**Целью работы** является использование метода, основанного на применении тонких слоев нематических жидких кристаллов (НЖК) для визуализации невидимой структуры поверхности различных модификаций осадка пресной воды, подвергнутой электролизу, в поляризованном свете. Эффективность метода иллюстрируется новыми примерами применения, показывающими его перспективы как уникальной регистрирующей среды для решения задач дефектоскопии поверхности материалов. Предпосылкой для визуализации структуры объектов является исходная упорядоченность молекул НЖК. Получение изображения структуры через слой НЖК связанно с нарушением его исходной упорядоченной ориентации и возникновением локальной деформации слоя НЖК в окрестности неоднородности структуры. Невидимые структуры и ее слабые модификации можно непосредственно наблюдать в поляризованном свете на просвет или отражение в интерференционных цветах при достаточной величине фазовой задержки. Объектом исследования явился осадок пресной воды, подвергнутой электрохимической обработке для получения анолита и католита с различными показателями pH. В основе обработки лежит закономерность аномального изменения реакционной и каталитической активности воды, подвергнутой электролизу. Реакционная способность связана с образованием метастабильных частиц и условиями, приводящими к изменению межмолекулярных взаимодействий и физической структуры воды.

После высыхания капли исследовался ее осадок. При испарении капля уменьшается в объеме, но ее граница удерживается на месте. Уходящий от границ объем компенсируется потоками от центра к краям, формирующими характерные кольца. Полученный узор – результат самоорганизации взвешенных частиц в испаряющейся капле, которые стремятся осесть на ее краях. Для объяснения полученных результатов были измерены краевые углы изученных образцов с помощью гониометра. Определение краевого угла было автоматизировано и рассчитано с помощью программы Drop analysis. Было проведено сравнение результатов, полученных методом НЖК и по измерению контактных углов. Данные двух методов совпали: анолит лучше смачивает поверхность и обладает большей гидрофильностью, чем католит. Увеличение значений краевых углов образцов согласуется с увеличением pH и уменьшением условий их смачивания. Также в ходе исследования было выяснено, что метод визуализации с помощью НЖК позволяет выявить и рассмотреть структуру сверхтонких слоев, что невозможно без их применения.

УДК 004.75

# ИССЛЕДОВАНИЕ ИНСТРУМЕНТОВ ДЛЯ СОЗДАНИЯ РАСПРЕДЕЛЕННЫХ ПРИЛОЖЕНИЙ НА ЯЗЫКЕ JAVA

**А.Н. Дмитриев**
**Научный руководитель – ассистент С.В. Клименков**

Сейчас сложно представить себе высоконадежную и производительную клиент-серверную систему, которая в своей работе не использовала бы преимущества кластеризации. Множество современных веб-приложений требует поддержания на высоком уровне показателей доступности и устойчивости к отказам и в то же время на низком уровне – времени обработки запроса. Благодаря кластеризации клиент может взаимодействовать с распределенной системой как с единым сервером, получая при этом лучшие характеристики сервиса. Так как это требует усложнения серверной логики кодом, не имеющим отношения к бизнес-модели, разработчики используют различные библиотеки для построения распределенных приложений. Наиболее распространенными из них для языка Java являются JGroups, используемая в сервере приложений JBoss, и Shoal, используемая в Glassfish.

JGroups предоставляет широкие возможности для написания распределенных приложений различной сложности на базе надежного группового обмена сообщениями (reliable multicast). Shoal – альтернативная библиотека, развивающаяся в рамках проекта Glassfish и базирующаяся на реализации Java NIO Grizzly.

Основная цель использования данных библиотек в веб-приложениях – это репликация данных сессий пользователей на различные машины и поддержание их актуальности. Проблемой здесь является невозможность одновременного обеспечения устойчивости к разделению, высокой доступности и согласованности данных пользователей в соответствии с CAP-теоремой. На практике требования, накладываемые на эти характеристики задаются предметной областью решаемой задачи. К примеру, системе «банк-клиент» необходимы высокие показатели по согласованности данных и устойчивость к разделениям, в то время как пропускной способностью можно пожертвовать, а высоконагруженному поисковому сервису или социальной сети важнее доступность и пропускная способность, а согласованностью данных можно с определенными допущениями пожертвовать. Из этого следует, что используемый инструмент кластеризации должен обеспечивать характеристики, определяемые задачами предметной области.

**Целью работы** является выбор подходящего инструмента для построения распределенных Java приложений с различными бизнес-задачами.

В работе исследованы библиотеки JGroups и Shoal и их роль в Java EE серверах приложений Glassfish и JBoss. В результате исследования было установлено, что Shoal обеспечивает лучшие показатели по производительности за счет использования Java NIO, однако JGroups предоставляет более обширный API, за счет чего позволяет более гибко использовать преимущества кластеризации.

УДК 004.627

# ВЕРИФИКАЦИЯ БЛОКОВ ДАННЫХ В СИСТЕМЕ БЕЗХЕШЕВОЙ ДЕДУПЛИКАЦИИ

**М.А. Жуков, Д.Б. Афанасьев**
**Научный руководитель – ассистент Д.Б. Афанасьев**

Дедупликация – это технология, ориентируемая на исключения избыточности в наборах данных путем замены повторяющихся данных ссылками на уже существующие данные, обеспечивая таким образом сокращение хранимой на носителе информации. Эту технологию используют преимущественно в области резервного копирования, по причине наличия большой избыточности в данных резервных копий. Важной задачей при реализации дедупликации является задача верификации блоков. Исторически сложилось, что большинство реализаций данной технологии имеют в основе хешевую концепцию, подразумевающую верификацию с использованием хеш-суммы блока. Данная концепция предполагает достаточно большие дополнительные расходы на хранении хеш-структур (связка хеш суммы блока с ссылкой на блок), например для хранения только хеш-структур в памяти для 1 терабайта дедуплицированных данных понадобится 40 гигабайт, при использовании алгоритма хеширования MD5, с размером ссылки на блок 8 байт и размером блока в 1 килобайт. Проблема создания менее ресурсозатратной системы дедупликации крайне актуальна ввиду постоянного увеличения объемов хранящихся данных.

**Целью работы** является разработка и исследование модуля верификации блоков в системе безхешевой дедупликации.

Предложен следующий алгоритм функционирования. Модуль верификации основывается на идее использования частей блока данных в качестве адресов структур в памяти и данных на носителе. По мере поступления новых блоков в памяти разрастается древо структур, содержащих в себе ссылки на другие структуры. Адресация внутри структур производится с использованием определенных частей блока данных в зависимости от глубины расположения конкретной структуры. Допускаем, что максимальная глубина дерева ограничена из предположения о больших накладных расходах для хранения структур. Последняя структура хранит информацию о расположении данных на носителе. Информация в такой структуре хранится в виде «ссылка на носитель – количество подозреваемых блоков». На носителе блоки сгруппированы, и внутри группы хранятся в упорядоченном виде, обеспечивая возможность сокращения количества операций чтения с носителя при поиске блока. Сам процесс верификации блока осуществляется с использованием оставшейся части блока, нетронутой при адресациях, сокращая время проверки блока.

В работе описывается и исследуется алгоритм модуля верификации блока в создаваемой системе безхешевой дедупликации, определяются возможные проблемы и предлагаются пути их решения, выявляются накладные расходы на ресурсы вычислительной системы.

УДК 004.75

## ПРОБЛЕМА ОБЪЕКТНО-РЕЛЯЦИОННОГО ОТОБРАЖЕНИЯ В РОЛЬ-ОРИЕНТИРОВАННОМ ПРОГРАММИРОВАНИИ

**И.В. Калинин**
**Научный руководитель – к.т.н., доцент Л.А. Муравьева-Витковская**

Концепция роле-ориентированного программирования является современным развитием объектно-ориентированного программирования. Добавление к объектам новых сущностей, «ролей», позволяет приблизить программные конструкции к сущностям реального мира. Такой подход приближает язык программирования к естественным языкам, позволяя создавать программный код, более понятным человеку, удобным в поддержке и устойчивым к изменениям при развитии вычислительной системы.

При разработке новых информационных продуктов перед производителем стоит задача взаимодействия с хранилищами данных и поддержкой совместимости с существующими протоколами хранения. При взаимодействии с базами данных, основанных на SQL, объектно-ориентированных приложений, для хранения данных используется объектно-реляционное отображение. Для роле-ориентированной модели требуется реализация хранения ролей в реляционной базе данных и интерфейса доступа к ее структуре.

Актуальность данной темы обусловлена возрастающим интересом к вопросу приближения языка программирования к естественному языку, включающему в себя концепцию роле-ориентированного программирования.

**Целью работы** является выбор подходящего решения для сохранения объектов роль-ориентированного программирования в реляционной базе данных.

В работе проанализированы возможности для использования классических подходов к хранению объектов в реляционных базах данных. В результате исследования были выявлены преимущества и недостатки различных способов организации хранения и сформулированы рекомендации по использованию их при решении практических задач.

УДК 004.9

## ПОСТРОЕНИЕ ПЛЕТЕНЫХ КОДОВ С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЕТНОСТЬ

**Н.И. Макаров**
**Научный руководитель – д.т.н., профессор Б.Д. Кудряшов**

Коды с малой плотностью проверок на четность наряду с турбо-кодами характеризуются низкой сложностью декодирования и в то же время обеспечивают помехоустойчивость близкую к теоретическим пределам. Для достижения меньшей вероятности ошибки декодирования желательно иметь как можно большее значение минимального расстояния.

Плетеные коды – это коды с малой плотностью проверок на четность, которые строятся с помощью графов. Благодаря особенностям их структуры для декодирования могут быть использованы итеративные методы. Однако в среднем такие коды имеют меньшее минимальное расстояние Хэмминга, чем лучшие линейные коды с теми же параметрами. Поэтому желательно найти плетеные коды на основе разных графов с наибольшим минимальным расстоянием.

В исследовании рассматривался двудольный граф Хивуда (14 вершин, 21 ребро), с размерами подматриц 4×4. В этом случае получается код с порождающей матрицей 28×84 (скорость 1/3).

При теоретической верхней границе на минимальное расстояние Хэмминга, равной 18, в докладе предлагается алгоритм, позволяющий построить код с минимальным расстоянием 16. Приводятся результаты моделирования, показывающие, что построенные коды имеют вероятность ошибки при декодировании по максимуму правдоподобия меньшую, чем циклически усеченные коды, применяемые в технологии WiMax.

УДК 004

## АСПЕКТЫ ПРИМЕНЕНИЯ DRM-СИСТЕМ В РАМКАХ КОМПЛЕКСНОЙ ЗАЩИТЫ ТЕКСТОВОЙ И ГРАФИЧЕСКОЙ ИНФОРМАЦИИ КОНТЕНТА ПЕРСОНАЛЬНЫХ ЭЛЕКТРОННЫХ УСТРОЙСТВ, ИСПОЛЬЗУЮЩИХСЯ В ОБРАЗОВАТЕЛЬНОЙ СФЕРЕ

**Н.Ф. Насыров**
**Научный руководитель – к.т.н., доцент Н.Н. Горлушкина**

Программно-аппаратные учебные комплексы на базе персональных электронных устройств в настоящее время находятся на стадии становления. Происходит определение их роли и места в современном образовательном процессе, создание нормативно-правовой документации, проводится работа по созданию рекомендаций по максимально эффективному использованию планшетных компьютеров для внедрения элементов электронного обучения и дистанционного обучения в основной образовательный процесс. Несмотря на то что потенциал портативного устройства как инструмента обучения до конца не раскрыт, можно рассматривать вопросы защиты информации в интересах правообладателя.

Современные системы DRM (Digital rights management) в первую очередь применяются для защиты информации от создания копий. Несколько реже подобные программные средства используются для отслеживания и пресечения нелегального копирования. Однако большинство из этих систем ориентировано на работу на персональных компьютерах или работу с цифровым контентом без привязки к конкретной операционной системе, что не всегда применимо к контенту персональных электронных устройств.

Применение только технических средств защиты информации не дает полной гарантии защиты данных от копирования. Защитить права и интересы правообладателей возможно только с использованием комплексного подхода, применяя правовые, организационные и технические меры защиты.

**Целью работы** является создание системы, обеспечивающей эффективную защиту текстовой и графической информации от неправомерного использования. Разработанные методы позволяют идентифицировать пользователя, нелегитимно использующего определенные материалы, в частности, допустившего копирование и распространение информации.

В интересах крупнейших правообладателей на законодательном уровне введена ответственность за обход DRM систем. Так, в IV части Гражданского кодекса РФ предусматривается использование технических средств защиты авторских прав (ст. 1299), а также предусматривается гражданско-правовая (ст. 1301 ГК РФ) и административная ответственность (ст. 7.12 КоАП РФ). Ссылаясь на указанные законодательные акты в рамках организационных мер необходимо определять персональную ответственность пользователя за нелегальное распространение информации.

В настоящее время наиболее распространены следующие технологии защиты текстовой и графической информации:

1. ограничение и/или запрет на выделение и/или копирование фрагментов текста и изображений;
2. кодирование информации о правообладателе контента в графических файлах;

3. использование «водяных знаков» – полупрозрачных изображений, нанесенных на графические файлы;
4. использование невидимых меток в тесте, которые сохраняются при конвертации файла в другие форматы и др.

Данные технологии, как правило, ориентированы на использование только технических средств защиты информации и в большинстве случаев направлены на указание правообладателя. Очевидно, данные решения не позволяют идентифицировать и аутентифицировать пользователей, разграничить доступ, обеспечить контроль легитимности использования информации.

Одной из трудностей защиты текстовой и графической информации является сложность идентификации пользователя, допустившего (умышленно или неумышленно) обнародование данных.

Ниже представлена общая последовательность предлагаемых действий генерации и отображения контента на стороне пользователя:

– генерация персонального контента на сервере с интеграцией элементов идентификации пользователя;
– передача контента пользователю на персональное электронное устройство;
– авторизация пользователя (при необходимости) путем ввода уникального логина и пароля;
– отображение контента на экране устройства.

В ходе исследований были разработаны следующие технологии идентификации пользователя:

1. по идентификатору пользователя определяется уникальный набор шрифтов. Определенные символы текста (буквы алфавита, буквицы и др.) отображаются заранее заданным шрифтом;
2. генерация уникального фона для текстового контента. Был реализован следующий алгоритм. В битовой области размера 3×3 пиксель с координатами (1;1) задается белым цветом. Остальные 8 пикселей используются для кодирования идентификатора пользователя путем задания четырех оттенков одного цвета. Данный подход предоставляет возможность создать 65536 уникальных изображений, что с учетом численности контингента обучающихся позволяет использовать его в электронных пособиях ведущих университетов. Необходимо отметить возможность задания разных оттенков фонового изображения для лучшего восприятия информации пользователем;
3. генерация цветной строки отделения колонтитулов по идентификатору;
4. добавление битовых областей ко всем изображениям документа в виде оформления блока подписи рисунка. Используется алгоритм, аналогичный представленному второму решению. Данный подход практически не ограничен по количеству комбинаций цветов, что теоретически не накладывает ограничений на количество пользователей контента программно-аппаратных учебных комплексов.

Комплексное использование описанных мер совместно с существующими подходами используются в качестве сдерживающего фактора и нормативно-правового контроля для потенциальных нарушителей. Опираясь на правовые и организационные меры возможно повышение эффективности применения технических средств защиты информации учебных комплексов.

Результаты работы будут использованы в процессе создания программно-аппаратных учебных комплексов на базе персональных электронных устройств.

УДК 004.92

# МОДИФИКАЦИЯ АЛГОРИТМА ТЕКСТУРНОЙ КОМПРЕССИИ LSDXT ДЛЯ РАБОТЫ НА ГРАФИЧЕСКОМ ПРОЦЕССОРЕ

**И.В. Перминов**
**Научный руководитель – д.т.н., профессор Т.Т. Палташев**

**Вступление, постановка проблемы.** Текстуры повсеместно применяются в компьютерной трехмерной графике и в простейшем случае представляют собой двухмерное изображение, накладываемое на трехмерную поверхность с целью улучшения визуальной детализации без усложнения геометрии.

Одним из эффективных вариантов повышения производительности и снижения требований к подсистеме памяти является использование предварительно сжатых текстур. Они хранятся в памяти и передаются по шинам в сжатом виде и распаковываются аппаратно внутри графического процессора. С ростом сложности систем визуализации, работающих с текстурами, обновляемыми на каждом кадре, актуальной также стала задача быстрого сжатия текстур силами самого графического процессора. Основная сложность тут заключается в том, что кодеки, обладающие высоким качеством результирующего изображения, очень требовательны к вычислительным ресурсам [1] и по большей части рассчитаны на выполнение на центральном процессоре.

Однако для эффективного исполнения алгоритма на графическом процессоре необходимо обеспечить высокий уровень внутреннего параллелизма. При сжатии текстур это условие выполняется естественным образом, так как каждый блок изображения может обрабатываться независимо. Для достижения высокой скорости сжатия, алгоритм обработки отдельного блока также должен быть модифицирован, в том числе для параллельной обработки.

Автором данной работы ранее был предложен метод [2] сжатия текстур в темпе генерации кадров, являющийся переработкой алгоритма L.Spiro [3]. Однако сам исходный алгоритм и представленный позднее кодек LSDxt [4] рассчитаны на высококачественное сжатие на CPU.

**Целью работы** является реализация всех этапов сжатия, используемых в LSDxt, с целью расширения возможностей GPU варианта online-кодека для обеспечения поддержки качественного сжатия в режиме offline.

Основным результатом является прототип кодека, позволяющий при сопоставимом качестве получить десятикратный прирост быстродействия по сравнению с LSDxt. Кроме модификации алгоритма для исполнения на графическом процессоре, в работе также рассмотрена проблема сторожевого таймера, перезагружающего GPU в случае слишком длительной обработки одного задания.

**Литература**

1. Brown S. DXT Compression Techniques. 2006. [Электронный ресурс] – Режим доступа: http://www.sjbrown.co.uk/2006/01/19/dxt-compression-techniques/, своб.
2. Перминов И.В. Динамическая компрессия визуальных данных в графических процессорах // Труды конференции РАСО-2012: Параллельные вычисления и задачи управления. – Секция В. – М., 2012. – С. 31–41.
3. DXT Compression Revisited. 2012. [Электронный ресурс] – Режим доступа: http://lspiroengine.com/?p=312, своб.
4. Release. LSDxt DXT Compressor. 2012. [Электронный ресурс] – Режим доступа: http://lspiroengine.com/?p=516, своб.
5. OpenCL Programming Guide for the CUDA Architecture, v4.2 // NVidia Corporation. – 2012.

УДК 004.4

# БЕСКОНТАКТНОЕ ИЗМЕРЕНИЕ БИОЛОГИЧЕСКИХ ПАРАМЕТРОВ ЖИЗНЕДЕЯТЕЛЬНОСТИ ЧЕЛОВЕКА

**А.И. Россомахина, Н.М. Лукьянов, А.А. Дергачев, Т.А. Полякова**
**Научный руководитель – к.т.н., доцент Н.М. Лукьянов**

Техника стала неотделимой частью современной медицины. Зачастую ни одна диагностическая процедура не обходится без применения какого-либо электронного инструмента или датчика. Более того, сейчас датчики одевают на себя даже здоровые люди для того, чтобы самостоятельно следить за самочувствием и, исходя из получаемых данных о своем состоянии, выполнять те или иные действия для улучшения своего здоровья, такие как диеты, физические упражнения, изменение распорядка дня. Персональная медицина позволяет человеку следить за своим здоровьем, не посещая кабинеты врача.

Одной из быстро развивающейся в плане применяемых технических средств областью персональной медицины и здорового образа жизни являются системы оценки качества сна. Существуют два традиционных подхода к исследованиям сна: полисомнография и актиграфия.

В качестве альтернативного метода мы предлагаем использовать технологию анализа изображения с возможностью определения характера и направления движения человека, а также обнаружение и измерение дыхания. Анализируя изображения, возможно, определить количество исследуемых объектов и характер их движения в отдельности, что позволит решить проблему невозможности применения акселерометров для анализа сна двух и более лиц.

Изучаемый нами раздел технического зрения рассматривает такие задачи, в которых при помощи видеокамеры и нескольких алгоритмов можно обнаружить и исследовать изменения, происходящие в теле человека, незаметные обычному глазу.

**Целью работы** является изучение алгоритмов для измерения глубины дыхания, пульса человека и количества его движений во сне и написание проекта на языке Си. Исследования проводятся на основе Visual Studio с применением библиотеки OpenCV.

В результате реализации проекта работы с видео изображением были выбраны следующие методы:

1. для размытия изображения – фильтр Kuwahara;
2. для выделения контуров – алгоритм Канни;
3. для выявления векторов движения – метод иерархического поиска.

Предлагаемый метод лишен недостатков имеющихся у контактных проводных и беспроводных датчиков, его преимуществом является нетребовательность к техническому оснащению аппаратного комплекса и отсутствие необходимости одевать на человека датчики. На момент исследований данный метод в зависимости от технических параметров изображения или условий его получения дает от 60 до 78 процентов точности измерений.

УДК 004.6

# ПРОБЛЕМА ИДЕНТИФИКАЦИИ МОДЕЛЕЙ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ WEB-РЕСУРСОВ

**П.Н. Рудакова**
(Волжский политехнический институт (филиал) «Волгоградский государственный технический университет»)
**Научный руководитель – к.т.н., доцент Д.Н. Лясин**
(Волжский политехнический институт (филиал) «Волгоградский государственный технический университет»)

С увеличением числа пользователей интернета и с бесконечным ростом web-ресурсов разработчикам сайтов становится труднее заинтересовать посетителей. Для оценки востребованности сайта разработчиками и определения места в рейтинге выдачи поисковыми системами необходимо определить категории посетителей ресурса. Один из способов разделения посетителей – это идентификация моделей поведения. Модель поведения пользователя – совокупность действий, совершаемых пользователем при посещении сайта.

Для того чтобы выполнить идентификацию, необходимо собрать пользовательские данные для последующего анализа. Для сбора статистики данных существуют различные инструменты web-аналитики, но, ни одна из таких систем не предоставляет возможности классификации пользователей по моделям поведения. Отсутствие таких систем обуславливает актуальность данной проблемы.

Задачей исследования является идентификация моделей пользователей по их поведению на сайте. Это поможет оптимизировать web-ресурса, оценить эффективность рекламной кампании, а также предоставить персонализированный контент.

Данная тема уже неоднократно поднималась в веб-аналитике, причем рассматривалась она с различных сторон [2]. Наиболее известным исследованием моделей поведения пользователей является работа Booz – Allen & Hamilton & Nielsen//NetRatings. Были определены следующие модели поведения:

- искатели фактов;
- повторные посетители;
- бесцельный серфинг;
- любители информации;
- серфинг;
- торопливые;
- выполнение одной миссии.

В своих трудах такие авторы, как Андреа Бьянко, Брайан Клифтон [3] и другие, рассматривают различные подходы к анализу и идентификации моделей.

В ходе работы были рассмотрены технологии сбора данных о работе пользователя с web-ресурсом, а также методы их анализа. Опираясь на рассмотренные методы и исследования, разработан способ сбора данных о пользователе и методика параметрического синтеза. Для анализа собираемых данных был разработан алгоритм разбиения пользователей по типу поведения на основе методологии и математического аппарата кластерного анализа. Разработана математическая модель поведения пользователя.

Научная новизна состоит в том, что на данный момент не существует инструментов для идентификации моделей пользователей по их поведению.

В дальнейшем необходимо реализовать такой инструмент с использованием разработанной математической модели.

**Литература**
1. Bindu Madhuri. Ch, Dr. Anand Chandulal. J, Ramya. K and Phanidra. M. Analysis of Users' Web Navigation Behavior using GRPA with Variable Length Markov Chains // International Journal of Data Mining & Knowledge Management Process (IJDKP). – 2011. – V. 1. – № 2.
2. Javadi Alimohammad, Zanjanizadeh Homa, and Javadi Maryam. On the Quality of Internet Users' Behavioral Patterns in Using Different Sites and its Impact on Taboos of Marriage: A Survey among Undergraduate Students in Mashhad City in Iran // World Academy of Science, Engineering and Technology. – 2008. – № 22.
3. Brian Clifton. How Google Analytics Works – Advanced Web Metrics with Google Analytics. – New York: Wiley Publishing, Inc., 2008. – 40 p.

УДК 625.1:004.94

## ОЦЕНКА ПЕРСПЕКТИВНОЙ ПРОПУСКНОЙ СПОСОБНОСТИ ЖЕЛЕЗНОДОРОЖНЫХ УЧАСТКОВ С УЧЕТОМ ПРЕДОСТАВЛЕНИЯ «ОКОН», НА ОСНОВЕ ПРИМЕНЕНИЯ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРОЦЕССОВ ПЕРЕВОЗОК

**В.С. Тимченко**
(Петербургский государственный университет путей сообщения)
**Научный руководитель – д.т.н., профессор И.М. Кокурин**
(Петербургский государственный университет путей сообщения)

**Введение.** Освоение перспективных возрастающих объемов перевозок требует своевременного обеспечения соответствующей пропускной и провозной способности железнодорожных дорог.

Проводимые с этой целью реконструкции и ремонты инфраструктуры сопровождаются предоставлением большого количества «окон», что влечет закрытие движения, ограничения скоростей и пропуск рабочих поездов. Действующая инструкция по расчету наличной пропускной способности железных дорог учитывает перерывы в движении не более 2,5 часов. Для определения перспективной пропускной способности железнодорожного участка в периоды предоставления более длительных «окон» необходимо учитывать множество сложно взаимодействующих факторов, обусловленных количеством, длительностью, расположением и временем выполнения реконструктивных и ремонтных работ.

**Целью работы** является изложение уникального метода определения пропускной способности железнодорожных участков, необходимой для освоения перспективных объемов перевозок, с учетом предоставления «окон» на задаваемый период прогнозирования.

**Базовые положения исследования.** Учет предоставления «окон» на длительную перспективу при оценке пропускной способности может быть обеспечен только методом имитационного моделирования процессов железнодорожных перевозок. Данный метод, в отличие от применяемых аналитических и графических методов, определяющих пропускную способность в одинаковых расчетных грузовых поездах, оценивает ее в реальных поездах, обращающихся на рассматриваемых железнодорожных участках.

Имитационная модель определяет ежегодный суммарный вес брутто поездов всех категорий, которые планируется пропускать за период прогнозирования по обследуемой линии. По этим данным в соответствии с классом, группой и категорией железнодорожного пути, а также сроками предыдущих ремонтов, технологией и нормами затрат на выполнение предстоящих работ, определяются места, количества и длительности «окон» для

предстоящих ежегодных ремонтов. На основе этой информации имитационная модель процессов перевозок определяет наличную пропускную способность и сравнивает ее с потребной. Если наличная пропускная способность меньше потребной, модель рассчитывает количество поездов, которое должно быть перенаправлено на параллельные железнодорожные направления для обеспечения заданных размеров движения при рассматриваемом варианте развития инфраструктуры в течение ежегодных периодов проведения ремонтных работ.

Модель оценивает стоимости потерь от простоев и дополнительных пробегов поездов и суммирует их со стоимостями ремонтных работ при различной продолжительности «окон». Оптимальной продолжительности «окна» соответствует наименьшая из указанных сумм. Сравнение количественных и качественных показателей рассматриваемых экспертами вариантов организации работ с предоставлением «окон» и пропуска поездов служит информационной поддержкой выбора наилучшего варианта.

Промежуточным результатом выполненной работы является развитие имитационной модели процессов железнодорожных перевозок, с целью расширения круга решаемых задач.

Основным результатом работы является создание уникального метода оценки пропускной способности железнодорожных участков, обеспечивающей освоение прогнозируемых объемов перевозок, с учетом предоставления ежегодных «окон» на рассматриваемый период и определения числа поездов, которые должны быть перенаправлены на параллельные железнодорожные участки.

Практическим результатом является применение предлагаемого метода по заказу ОАО «РЖД» для оценки пропускной способности железнодорожной линии Мга-Лужская, которая обслуживает морской торговый порт Усть-Луга, в условиях ее реконструкции с предоставлением большого количества «окон» в период с 2010 по 2015 годы.

УДК 004.047

## ГЕНЕРАЦИЯ ЕСТЕСТВЕННО-ЯЗЫКОВЫХ КОНСТРУКЦИЙ НА ОСНОВЕ ФОРМАЛИЗОВАННЫХ ЗНАНИЙ

**Ю.А. Туча**
**Научный руководитель – к.т.н., профессор Т.А. Павловская**

**Вступление, постановка проблемы.** В настоящее время в современных информационно-компьютерных системах текст на естественном языке наиболее широко распространен как средство коммуникации с пользователем.

Для эффективного освоения такой информации зачастую возникает необходимость в ее автоматическом анализе и смысловой обработке. Решение многих прикладных задач автоматического анализа текста на естественном языке, таких как аннотирование, реферирование, а также извлечение знаний, требует учета множества различных особенностей естественно-языковых текстов: лексико-фразеологических, синтаксических, а также семантических. Извлечение знаний наиболее эффективно при использовании методов, основанных на семантических законах естественного языка.

В последнее время наиболее перспективными считаются приемы, основанные на попытках формализации методов работы с семантикой. У такого логического подхода, несмотря на возникающие, на первый взгляд противоречия, есть достаточно весомые плюсы, такие как простое распараллеливание единой задачи и множественность решаемых задач на едином наборе знаний.

Формализованные знания имеют определенные и вполне очевидные преимущества. Также на их основе можно создавать новые знания в форме умозаключений и утверждений. Зачастую существует необходимость и в обратной задаче, а именно генерации естественно-

языковых конструкций текста из его семантического или формального представления.

Автором данной работы предложен метод генерации конструкций естественного (русского) языка на основе ранее созданного, его формализованного представления, использующего извлеченные знания для задачи генерации тестовых заданий на основе учебных материалов.

Таким образом, предложенный метод генерации рассчитан на создание определенного типа языковых конструкций и использует определенный тип входных данных. В процессе генерации создается промежуточное семантическое представление.

Так как генерация происходит из формализованного представления текста на естественном языке, у нас имеется необходимая лингвистическая и семантическая информация, что упрощает создание грамматической структуры некоторых типов тестовых заданий.

**Целью работы** является реализация всех этапов обработки текста, используемых как при формализации языковых конструкций, так и при обратной генерации из них текста с целью получения на его основе учебных тестовых заданий.

Основным результатом является разработка структуры программной системы и методов автоматизированной обработки учебных текстов на естественном языке, для выделения смысловых понятий и генерации примеров тестовых вопросов для дальнейшего редактирования преподавателем.

УДК 004.056.53

## АРХИТЕКТУРА БЕЗОПАСНОСТИ ОС ANDROID

**А.И. Гуркин, О.К. Тампер**
**Научный руководитель – д.т.н., профессор А.Ю. Щеглов**

**Введение.** На последний квартал 2012 года ОС Android заняла более 70% рынка смартфонов. Такая популярность этой ОС привлекла внимание злоумышленников. Таким образом, понимание архитектуры безопасности ОС Android необходимо для создания качественных приложений.

**Постановка задачи.** Необходимо рассмотреть основные составляющие архитектуры безопасности операционной системы Android. Определить, как осуществляется защита данных пользователя и защита системных ресурсов.

**Промежуточные результаты.** Основой платформы Android является Linux ядро. Оно обеспечивает систему несколькими ключевыми функциями безопасности: моделью разрешений, изолированием процессов, механизмом межпроцессного взаимодействия. В многопользовательской операционной системе одной из основных целей безопасности Linux ядра было изолировать пользователей друг от друга. Android не многопользовательская операционная система и механизмы изоляции пользователей друг от друга в ней используются для изоляции приложений. Система присваивает уникальный идентификатор пользователя (UID) для каждого приложения Android. Таким образом, Android изолирует приложения друг от друга на уровне ядра и обеспечивает безопасность между приложениями и системой на уровне процесса через стандартные средства Linux, такие как идентификаторы пользователя и группы, которые назначены приложениям. По умолчанию приложения не могут взаимодействовать друг с другом и имеют ограниченный доступ к ОС. Доступ к ОС необходим приложениям для использования ресурсов устройства (камеры, GPS, Bluetooth, доступ к сети и т.д.). Изолированность приложений на

уровне ядра, является основой в архитектуре безопасности системы, используя уязвимости ядра, злоумышленник может получить права другого пользователя для своего приложения, тем самым выйдя из песочницы. Также многие пользователи для увеличения функционала устройства сами получают права пользователя root, тем самым подвергая себя риску.

Приложения чаще всего написаны на языке Java и выполняются в виртуальной машине Dalvik. Также существуют приложения написанные на C/C++ (нативные), или Java приложения, использующие нативные библиотеки. Все приложения выполняются в изолированной программной среде, получая набор разрешений, задекларированных разработчиком в файле AndroidManifest.xml. При установке приложения пользователь должен принять набор разрешений из манифеста, иначе приложение не будет установлено. Получив разрешение на использование какого-либо ресурса системы, приложение может использовать его злонамеренно, нанося вред пользователю или устройству. Злоумышленники пользуются этим и вносят недокументированные возможности в свои приложения, например, право на полный доступ к интернету дает возможность приложению участвовать в DDoS атаках.

**Основной результат.** В работе рассмотрены основные составляющие архитектуры безопасности операционной системы Android. Выявлены ее сильные и слабые стороны и даны рекомендации по использованию механизмов защиты в приложениях. Показаны пути для обхода защитных механизмов на разных уровнях операционной системы.

УДК 004.75

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ СПОСОБОВ ОБНАРУЖЕНИЯ РАСПРЕДЕЛЕННОЙ АТАКИ

**С.А. Жмылёв, Д.Б. Афанасьев**
**Научный руководитель – ассистент Д.Б. Афанасьев**

Для современной вычислительной системы угроза подвергнуться распределенной атаке довольно высока. Такого рода атакам зачастую подвергаются системы, ориентированные преимущественно на обслуживание большого числа клиентов. В связи с этим перед специалистами, занимающимися обслуживанием таких систем, возникает ряд задач по обнаружению распределенных атак и сведению их последствий к минимуму. Диагностика таких систем – сложная и объемная задача, так как в системе может присутствовать большое количество направлений атаки. Причем, чем больше сервисов предоставляет система клиентам со своей стороны, тем шире спектр возможностей атакующего, а значит, сложнее становится обнаружить в такой системе атакуемый элемент и сохранить работоспособность системы. Существует довольно много способов обнаружения распределенных атак: от анализа внешней активности сервиса до проведения его профилирования.

**Целью работы** является определение критериев эффективности и сравнительный анализ способов обнаружения распределенных атак.

В статье рассматривается поведение систем под воздействием различных распределенных атак, исследуются способы их обнаружения, выбираются и обосновываются критерии оценки эффективности предложенных способов.

УДК 006.88

# АНАЛИЗ НОРМАТИВНОЙ БАЗЫ ТРЕБОВАНИЙ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА И ОРГАНИЗАЦИИ ЕЕ САМООЦЕНКИ

**Е.А. Карпова**
**Научный руководитель – к.п.н., доцент А.В. Маятин**

Неотъемлемой задачей банковской деятельности является обеспечение информационной безопасности и ее аудит с целью выявления слабых мест и повышения безопасности предоставляемых услуг.

**Целью исследования** является анализ нормативной базы и стандартов обеспечения информационной безопасности банковской деятельности и проведения ее самооценки. Актуальность темы обусловлена тем, что не существует единого документа, определяющего требования к процедуре самооценки и обеспечению информационной безопасности.

Основная цель проведения самооценки – это оценка соответствия информационных систем банка стандартам и нормативным актам в банковской сфере, а также анализ качества используемых защитных мер, которые строго регулируются ФСТЭК, ФСБ, ЦБ и СТО.

Стандарт Организации Банка России Информационной Безопасности Банковской Системы (СТО БР ИББС) является основным нормативным актом в банковской сфере, предъявляющим требования к информационной безопасности, но далеко неединственным. Аудит и самооценка по СТО БР ИББС отличается от аудита по другим нормативным актам за счет выделения нового руководства по проведению самооценки. Однако СТО БР ИББС затрагивает глубоко не все аспекты обеспечения информационной безопасности и организации ее самооценки. В частности, основным регулятором требований по работе с персональными данными являются ФСТЭК и ФСБ.

Стоит отметить, что в СТО БР ИББС не бывает несоответствия требованиям, просто уровень соответствия может быть разный: от нуля до пяти. И только уровни выше 4-го считаются положительными.

Вопрос аудита соответствия требованиям СТО БР ИББС актуален еще и ввиду того, что методика оценки соответствия, предложенная в рамках законодательства о национальной платежной системе, и методика оценки соответствия СТО БР ИББС могут очень сильно расходиться в итоговых значениях. При этом оценка по первой методике стала обязательной, в то время как оценка по СТО БР ИББС до сих пор носит рекомендательный характер.

Акцент на том, как правильно управлять информационной безопасностью и проводить ее аудит делается в таких стандартах, как Cobit и ГОСТ Р ИСО 17799. Установлена связь этих стандартов, которую можно просмотреть на следующих примерах:

1. DS 5.3 Управление идентификацией явно соотносится с требованиями ГОСТ Р ИСО\МЭК 17799 4.2.1.1 о физическом и логическом контроле доступа и 9.6 о контроле доступа к приложениям;
2. DS 5.6 Определение инцидентов в сфере безопасности пересекаются с требованиями 9.3 обязанности пользователей и 9.5.2 процедуры регистрации с терминала;
3. AI 4.2 Передача знаний бизнес-менеджерам равнозначны требованиям 8.1.1 документальное оформление операционных процедур.

Основной отраслевой стандарт СТО БР ИББС вобрал в себя множество требований группы стандартов 270xx. Основные пересечения требований наблюдаются в областях обеспечения и управления информационной безопасностью, организации аудита, оценке рисков нарушения информационной безопасности и защиты персональных данных.

Четкие требования к самооценке предъявляет к тому же негосударственный стандарт PCI DSS, обязательный для исполнения всеми банками, которые обрабатывают, передают и хранят данные владельцев карт. Платежные системы накладывают жесткие штрафы за отсутствие ежегодных отчетов по самооценке, ежеквартального сканирования сетей с

помощью уполномоченных организаций и ежегодных аудиторских проверок аккредитованными компаниями.

Многообразие правовых актов и стандартов по обеспечению информационной безопасности и проведению аудита накладывают множество правил на банк, выполнение которых может привести к серьезным санкциям и потери клиентов.

Были рассмотрены основные взаимосвязи нормативных актов по обеспечению информационной безопасности, выделены регуляторы этих требований и составлена таблица, в которой проанализированы основные требования по информационной безопасности.

Следует отметить, что между нормативными актами существуют противоречия (в частности, ФЗ 152 «О персональных данных» запрещает построение модели угроз самостоятельно, что в свою очередь разрешается ФСТЭК – основной орган контроля) и неопределенность в плане требований аттестации. Такая ситуация в первую очередь вызвана большим количеством регуляторов.

Требования СТО Банка России подразумевают непрерывный характер, направленный на постепенное и поэтапное наращивание уровня защиты информационной безопасности, в отличие от требований ФСТЭК и ФСБ, носящих скорее разовый характер. Таким образом, банку следует в первую очередь начать с реализации требований СТО Банка России, которые в большинстве случаев перекрываются с требованиями ФСБ и ФСТЕК (в частности, СТО разрешает использование только сертифицированных ФСТЭК и ФСБ средств защиты информации, в том числе и криптографических). В итоге такой подход окажется эффективнее, чем выполнение в первую очередь пусть и меньшего количества требований ФСТЭК и ФСБ, которые в основном направлены на защиту персональных данных.

УДК 519.713.1

## О ВОПРОСАХ РЕШЕНИЯ ЗАДАЧ СИНТЕЗА И АНАЛИЗА КОНЕЧНЫХ АВТОМАТОВ, ЗАДАННЫХ ПОЛИНОМАМИ С РАЦИОНАЛЬНЫМИ КОЭФФИЦИЕНТАМИ

**М.Д. Сластихина**

(Саратовский государственный технический университет им. Ю.А. Гагарина)

**Научный руководитель – д.ф.-м.н., доцент Т.Э. Шульга**

(Саратовский государственный технический университет им. Ю.А. Гагарина)

В работе рассматриваются возможности обеспечения адаптивности системы за счет ее функциональной избыточности. Для исследования таких систем в данной статье выбрана одна из наиболее распространенных моделей – конечный детерминированный автомат (КДА), а именно конечный детерминированный автомат Медведева.

Пусть дан автомат Медведева $A = (X, S, \delta)$. Занумеруем состояния автомата натуральными числами $S = \{0, 1, ..., m-1\}$ и представим функцию переходов данного автомата в виде обобщенных подстановок:

$$\delta_x : \begin{pmatrix} 0 & 1 & \dots & m-1 \\ s_0 & s_1 & \dots & s_{m-1} \end{pmatrix}, x \in X. \qquad (1)$$

Обозначим $s = (0, 1, \dots, m)$. Для краткости также будем использовать запись подстановки (1) в виде $\delta_x(s)$.

**Определение 1.**

Пусть задано семейство автоматов $\{A_i = (X_i, S, \delta^{(i)})\}_{i \in I}$, $|S|=m$. Автомат $A = (X, S, \delta)$

назовем универсальным для семейства автоматов $\{A_i\}_{i\in I}$, если

$$(\forall x \in X_i)(\forall i \in I)\,(\exists t_x \in X^*)(\bar{\delta}_{t_x}(s) = \delta_x^{(i)}(s)), \quad \text{где } s = (0,...,m-1),$$

т.е. для любого входного сигнала x любого автомата из семейства $\{A_i\}_{i\in I}$ существует последовательность входных сигналов автомата *A*, индуцирующая преобразование, эквивалентное преобразованию, индуцируемому сигналом x автомата из семейства $\{A_i\}_{i\in I}$.

В рамках работы рассматриваются следующие задач теории универсальных автоматов, решение которых приводит к функциональной избыточности системы:

– задача синтеза: представляет из себя задачу нахождения автомата, который может моделировать работу нескольких заданных автоматов, или целого класса автоматов.
– задача анализа: заключается в нахождении автоматов, работа которых может моделироваться за счет заданного автомата.

В общем случае эти задачи являются алгоритмически неразрешимыми, в связи с этим предлагается решать эти задачи для определенных классов автоматов. В работах Т.Э. Шульги описаны методы решения данных задач для класса автоматов, заданных полиномами с рациональными коэффициентами, однако недостатком данного подхода является то, что не каждый автомат может быть задан полиномами с целочисленными коэффициентами. Следовательно, было принято решение рассматривать автоматы, заданные полиномами с рациональными коэффициентами.

Рассмотрим следующий способ задания функции перехода автомата:

$$\delta_{x_i}(s) = a_0(x_i) + a_1(x_i)s + a_2(x_i)s^2 + ... + a_{m-1}(x_i)s^{m-1} =: f_{x_i}(s), \qquad (2)$$

$s \in S$, $a_k(x_i) : X \to Q$, где $Q$ – множество рациональных чисел, $k = \overline{0,(m-1)}$, $x_i \in X$.

**Определение 2.**

Будем говорить, что поведение конечного автомата Медведева *A* определяется семейством полиномов $\{f_x\}_{x\in X}$ с рациональными коэффициентами, если подстановка из семейства $\{\delta_x\}_{x\in X}$ представима в виде (3) для каждого $x_i \in X$, т.е. $f_{x_i}(s) = \delta_{x_i}(s)$. Будем говорить, что в таком случае подстановка $\delta_x$ равна полиному $f_x$.

Было доказано, что любой конечный детерминированный автомат может быть задан семейством полиномов с рациональными коэффициентами. Для данного класса автоматов были решены задачи синтеза и анализа автоматов. Временная сложность разработанного алгоритма по решению задачи анализа экспоненциально зависит от размера входных данных, что затрудняет использование метода для больших объемов данных.

Таким образом, в рамках данного исследования были разработаны методы:

– перехода от автоматов, заданным матрицей переходов, к автоматам, заданным семейством полиномов с рациональными коэффициентами;
– решения задачи синтеза универсального автомата;
– решения задачи анализа универсального автомата;
– ряд вспомогательных методов.

Все разработанные методы были реализованы в качестве библиотеки на языке GAP. На данный момент исследуются возможности реализации решения задачи анализа с меньшими временными затратами. Кроме этого исследуется применимость разработанных методов для разработки алгоритмов в парадигме автоматного программирования.

УДК 004.738

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ В ИНТЕРНЕТ-БАНКИНГЕ

**А.В. Халёв**
**Научный руководитель – к.э.н., доцент О.А. Цуканова**

С развитием информационных технологий стали широко применяться так называемые электронные документы, использование которых значительно ускоряет процесс документооборота и позволяет экономить время. В связи с этим все большая часть информации хранится и распространяется в мире в электронном виде. Особое значение в данном случае начинает приобретать не только обеспечение юридической силы электронного документа, но и безопасность его использования.

Быстрорастущий сегмент дистанционного банковского обслуживания привлекает внимание все большего числа мошенников. Поэтому сегодня очень важен взвешенный подход к аутентификации клиентов системы «Интернет-Банкинг». Клиенты не заинтересованы в сложных механизмах, следовательно, у банка должно быть продуманное централизованное решение аутентификации, которое будет применяться для всех клиентов независимо от приобретенных ими продуктов.

Вслед за активным продвижением интернета в странах СНГ растет популярность Интернет-Банкинга. Все больше и больше банков активно развивают дистанционные каналы обслуживания клиентов.

Классический способ аутентификации (наиболее часто применяется в Интернет-Банкинге) предполагает использование дополнительных мер защиты пользователя. Например:

– ограничение срока действия пароля. Задается максимальный срок действия пароля, по истечении которого пользователю необходимо получить новый пароль;
– ограничение числа попыток входа в систему. Используется временное или постоянное блокирование возможности входа в Интернет-Банкинг в случае исчерпания допустимого количества неверного ввода логина/пароля;
– принудительный выход из системы при бездействии клиента в течение определенного времени.

Таким образом, для входа в Интернет-Банкинг могут использоваться различные способы и сценарии ввода идентификаторов для аутентификации пользователя.

Одним из наиболее важных аспектов функционирования систем «Интернет-Банкинг» является обеспечение информационной безопасности, т.е. обеспечение конфиденциальности и достоверности информации, передаваемой между клиентом и банком.

Для обеспечения информационной безопасности в системах «Интернет-Банкинг» применяются различные средства и методы защиты информации, начиная с паролей и заканчивая многоуровневыми системами безопасности на основе современных криптографических протоколов и алгоритмов, реализующих шифрование и работу с электронными цифровыми подписями (ЭЦП). Выбор средств и методов защиты информации зависит от вида системы «Интернет-Банкинг» и способа доступа к этой системе.

В настоящее время на рынке наблюдается повышенное внимание банков к развитию альтернативных каналов обслуживания. Розничные игроки активно развивают дистанционные сервисы и привлекают клиентов к их использованию. Вводятся специальные тарифы, которые все более выгодно отличаются от аналогичных тарифов за обслуживание в офисах банка. Банки работают над повышением удобства и безопасности систем «Интернет-Банкинг».

Пользователи интернета, являющиеся основной целевой категорией, финансово и технически более грамотны. Однако не всегда этой грамотности достаточно, чтобы клиент:

– в достаточной степени доверял дистанционному сервису, предлагаемому банком;
– обладал достаточным уровнем осведомленности для соблюдения правил безопасной работы с банком по дистанционным каналам.

Поэтому банки должны постоянно проводить разъяснительную работу с клиентами в части выполнения ими рекомендаций для обеспечения безопасной работы в системах «Интернет-Банкинг». Рекомендации могут быть следующими:
– хранить в секрете и не передавать никому свои пароли, карты переменных кодов, носители с криптографическими ключами, токены и другие средства доступа к системе «Интернет-Банкинг»;
– использовать для работы в системе «Интернет-Банкинг» компьютеры, программное обеспечение которых полностью контролируется;
– в случае утраты паролей, карты переменных кодов, токена, носителей с криптографическими ключами или других средств доступа в систему «Интернет-Банкинг», а также в случае выявления доступа к ней посторонних лиц немедленно блокировать свою работу в системе «Интернет-Банкинг».

В ходе проведенного анализа сравнения методов можно сделать вывод, что все методы имеют свои преимущества и недостатки. Однако выбор какого-либо метода защиты в системе «Интернет-Банкинг» зависит от типа системы и политики безопасности конкретного банка. С уверенностью можно сказать, что на сегодняшний день многие крупные банки имеют комплексную защиту, применяя в купе несколько методов. Это способствует удорожанию системы, но предоставляется выбор того или иного метода клиентам системы «Интернет-Банкинг», в зависимости от удобства и цели использования метода. Например, для больших компаний, часто совершающих в крупном размере платежи через систему «Интернет-Банкинг» лучше использовать вместе с Сертифицированным ЭЦП и OTP-токены для подтверждения проведения платежа. Для предприятий среднего и малого бизнеса помимо ЭЦП желательно использовать OTP-коды на скретч-картах либо OTP-коды, передаваемые по SMS. Использование технологии OTP при подписании платежных документов приравнивается к подписанию документа собственноручно в соответствии с п. 2.3 Временного Положения ЦБ РФ от 10.02.1998 № 17-П «О порядке приема к исполнению поручений владельцев счетов, подписанных аналогами собственноручной подписи при проведении безналичных расчетов кредитными организациями».

УДК 004.418

## ИНТЕГРАЦИЯ CRM И BPM, КАК ПУТЬ РАЗВИТИЯ CRM СИСТЕМ

**А.С. Шувалов**
(Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики)
**Научный руководитель – А.Д. Береснев**
(Компания «Ротэк»)

**Введение.** CRM (Customer Relationship Management) это современная бизнес-стратегия, нацеленная на рост и повышение доходности бизнеса компании путем повышения лояльности клиента на протяжении всего цикла взаимодействия с ним [1].

По оценкам TAdviser, в 2011 году российский рынок внедрений CRM-систем вырос в объеме на 30% и составил 22,44 млрд. рублей (в 2010 году он равнялся 17,26 млрд. рублей). В долларовом эквиваленте объем рынка за 2011 год составил около $680 млн. Прогноз роста рынка от TAdviser на 2012 год – сохранение темпов роста на уровне 25–30% [2]. Несмотря на то, что рынок CRM стремительно увеличивается, все они имеют схожую функциональность. Поэтому для получения конкурентного преимущества может возникнуть необходимость в

интеграции с внешними системами, например с системами класса BPM (Business Process Management). Аналитики Gartner уверены, что к 2014 году 40% руководителей крупнейших компаний мира будут использовать те или иные решения категории BPM [3].

**Цель работы** – выявление преимуществ интеграции BPM и CRM систем с точки зрения расширения функциональности последних.

**Постановка проблемы.** Эксперты в области CRM выделяют несколько основных проблем. CRM системы представляют из себя совокупность модулей которое может доходить до 20 штук и более, в таком случае пользователю системы изначально очень сложно разобраться в последовательности или очередности операций которые он должен выполнить для достижение определенного эффекта, т.е. пользователю предоставляется полная свобода выбора его действий, что может не лучшим образом сказываться на эффективности его работы.

Немаловажной проблемой является и то, что CRM системы не работают на результат. Показатели работы сотрудника доступные в большинстве CRM, такие как количество контактов, не связаны с целью реализации бизнес процессов CRM [4]. Кроме этого, в большинстве CRM затруднена регламентация бизнес процессов CRM.

**Основной результат.** По мнению автора работы, существенно уменьшить список проблем и еще больше автоматизировать процесс продаж поможет интеграция CRM и BPM систем, которая позволит упростить регламентацию бизнес процессов взаимодействия с клиентом, а также позволит управлять этим бизнес процессом.

Интеграция BPM и CRM систем обладает тремя главными достоинствами:

– стандартизация логики бизнес-процессов дает экономию времени и денег за счет устранения ненужных и дублирующих работ;
– улучшается обслуживание клиентов: идет сосредоточение на тех процессах, которые ценятся клиентами и находятся в сфере их интересов;
– совершенствуются правила, по которым должны идти процессы: если они не существуют или не согласованы, возможность отслеживания бизнес процессов существенно ухудшается, а компания подвергается риску [5].

Кроме этого, за счет формализации бизнес процессов, оперативный контроль становится более эффективным, полностью исключается возможность непреднамеренных ошибок. Какой бы сложной ни была бизнес-логика, ее в любом случае можно реализовать.

**Вывод.** Интеграция BPM и CRM систем предоставляет ряд преимуществ, остается лишь исследовать вопросы ограничений использования по видам деятельности предприятий, использующих подобные системы.

**Литература**

1. Есина Л.Б. Внутренний маркетинг как инструмент повышения производительности труда персонала и качества услуг гостеприимства и туризма. Автореф. дис. к-та экон. наук. – Пенза, 2008.
2. CRM (рынок России) [Электронный ресурс] – Режим доступа: http://www.tadviser.ru/index.php/CRM, своб.
3. Синергия BPM [Электронный ресурс] – Режим доступа: http://www.osp.ru/cw/2011/05/13007096/, своб.
4. CRM-системы. Частые вопросы. [Электронный ресурс] – Режим доступа: http://www.ronix.ru/hosting/ronix/newronixsite.nsf/va_WebPages/FrequentQuestionsRus, своб.

5. Сахаров Д.Е. BPM как основа организации предприятия // Известия Южного федерального университета. Технические науки. – 2009. – Т. 93. – №4. – С. 194–200.

УДК 004.056.53

## ПРИНЦИПЫ КОНТРОЛЯ ДОСТУПА К ФАЙЛОВЫМ ОБЪЕКТАМ С АВТОМАТИЧЕСКОЙ РАЗМЕТКОЙ ФАЙЛОВ

**К.А. Щеглов**
**Научный руководитель – д.т.н., профессор А.А. Ожиганов**

**Введение.** В работе [1] автор ввел классификацию файловых объектов, подразделив их на создаваемые (и/или модифицируемые) в процессе работы пользователей и на статичные, к которым могут быть отнесены файлы, исходно присутствующие в системе и не модифицируемые в процессе работы пользователей – системные файлы. Применительно к решению задачи защиты создаваемых файлов в [1] предложены принципы контроля доступа, основанные на исключении сущности «объект доступа» из разграничительной политики, за счет автоматической разметки создаваемых в системе файлов, позволяющие корректно в общем случае решать задачу контроля доступа к создаваемым файловым объектам и в значительной мере упростить задачу администрирования. Предложенные принципы использованы при построении, как дискреционного, так и мандатного методов контроля доступа в ряде коммерческих средств защиты семейства «Панцирь», в том числе на этих принципах реализована система защиты от запуска вредоносных программ СЗ «Панцирь», основанная на запрете исполнения всех созданных в процессе работы системы файлов. Однако эти результаты были получены лишь в отношении создаваемых файловых объектов.

**Постановка задачи.** При реализации контроля доступа к статичным (системным) файлам на сегодняшний день используются те же известные принципы – первичным при назначении разграничений прав доступа в известных методах контроля доступа является объект, реализуется разграничительная политика доступа субъектов к объектам. Практическая реализация разграничительной политики доступа к системным файлам, основанная на этих принципах, еще сложнее, чем к создаваемым, предназначенным для хранения обрабатываемой информации. А вместе с тем, защита системных ресурсов является крайне актуальной современной задачей защиты от атак, направленных на нарушение работоспособности или корректности работы системы и приложений. Однако автоматически размечать можно не только файлы, предназначенные для хранения информации, при их создании, но и статичные (системные файлы) при их использовании системой и приложениями, т.е. потенциально они автоматически идентифицируемы в процессе работы системы, что может быть использовано при реализации разграничительной политики доступа к системным файлам.

**Базовые положения исследования.** Принципы контроля доступа на основе автоматической разметки файлов:

1. сущность «объект» исключается из разграничительной политики доступа;
2. при обращении к файлу, он автоматически размечается средством защиты (диспетчером доступа) – в атрибуты (резервные) файла им помещается информация о типе файла (статичный или создаваемый, в зависимости от зафиксированного обращения) и о субъекте, получившим доступ к файлу (в общем случае, исходное имя пользователя, полнопутевое имя процесса, эффективное имя пользователя);
3. разграничительная политика доступа реализуется между субъектом совершившим доступ к файлу, что отражено в разметке файла, и субъектами, запрашивающими впоследствии

доступ к размеченному файлу. Т.е. только между субъектами.

**Промежуточные результаты.** Применительно к создаваемым файловым объектам, при реализации контроля доступа, требуется обнаруживать факты создания (операция «запись») новых файлов (либо модификации уже существующих, но неразмеченных файлов, к слову сказать, сюда подпадают и системные файлы, которые могут быть несанкционированно удалены, либо модифицированы) и автоматически «размечать» создаваемые/модифицируемые файлы – записывать в качестве атрибута, либо непосредственно в «теле» файла, в зависимости от реализации, учетную информацию субъекта, создавшего/модифицировавшего этот файл.

Для статичных файлов ситуация принципиально иная, применительно к ним удаление и модификация (операции «удаление», «переименование» и «запись») являются несанкционированными действиями (если подобные действия в отношении файла разрешены, то подобный файл уже следует отнести к создаваемым, реализовав для него соответствующие принципы контроля доступа). В отношении этих файлов следует разрешать только операции «чтение» и «исполнение» (для исполняемых файлов).

Как следствие, размечать статичные файлы необходимо совсем иначе – следует записывать в качестве атрибута, либо непосредственно в «теле» файла, в зависимости от реализации, учетную информацию субъекта, прочитавшего/исполнившего этот файл, и выполненное им действие в отношении статичного файла (чтение или исполнение).

В качестве примера рассмотрим технологию защиты исполняемых файлов, основанную на изложенных принципах и реализованную в СЗ «Панцирь+». Для реализации защиты размечать следует статичные исполняемые файлы, а в качестве разметки используемого статичного файла достаточно указывать признак файла – исполняемый. Диспетчер доступа при исполнении файлов, автоматически их помечает, присваивает им признак исполняемого. Заметим, что фиксировать нужно именно исполнение файла, а не открытие файла на исполнение, в противном случае будет много ложных срабатываний. Правила доступа в данном случае простейшие – к файлу, помеченному, как исполняемый, запрещается доступ любым субъектом на удаление, модификацию, переименование. При последующих обращениях к размеченному статичному файлу, диспетчером предотвращается возможность его удаления, модификации, переименования. Как следствие, исполняемый файл (автоматически размеченный средством защиты) не может быть несанкционированно удален, модифицирован, переименован.

**Основной результат.** В работе сформулированы (были апробированы на реальных коммерческих средствах защиты информации) единые принципы контроля доступа к файловым объектам, основанные на автоматической разметке файлов. Общность данных принципов обусловливается возможностью их практического применения при реализации защиты, как создаваемых, предназначенных для хранения обрабатываемой информации, так и статичных – системных, файлов. Их реализация позволяет исключить сущность «объект» из разграничительной политики доступа – все разграничения устанавливаются непосредственно между субъектами, в результате чего, кардинально пересмотреть существующие подходы к решению основополагающей задачи защиты информации.

**Литература**

1. Щеглов К.А. Принципы контроля доступа к создаваемым файловым объектам // Сборник трудов молодых ученых и сотрудников кафедры ВТ. – Вып. 3. – СПб, 2012. – С. 85–86.