

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ  
Учреждение образования  
«Белорусский государственный технологический университет»



**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**  
**Тезисы докладов 79-й научно-технической конференции**  
**профессорско-преподавательского состава,**  
**научных сотрудников и аспирантов**  
**(с международным участием)**

Минск 2015

УДК 004:005.745(06)

ББК 32.97я73

И 74

**Информационные технологии** : тезисы 79-й науч.-техн. конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 2-6 февраля 2015 г. [Электронный ресурс] / отв. за издание И. М. Жарский; УО БГТУ. – Минск : БГТУ, 2015. – 27 с.

Сборник составлен по материалам докладов научно-технической конференции сотрудников Белорусского государственного технологического университета, в которых отражены новые успехи и достижения в информационных технологиях: алгоритмизации и программировании, передачи и обработки данных.

Сборник предназначен для работников различных отраслей народного хозяйства, научных сотрудников, специализирующихся в соответствующих областях знаний, аспирантов и студентов ВУЗов.

Рецензенты: д-р техн. наук, проф. кафедры информационных систем и технологий В.Л. Колесников;  
канд. техн. наук, зав. кафедрой информатики и компьютерной графики Д.М. Романенко;  
канд. физ.-мат. наук, доц., зам. декана факультета издательского дела и полиграфии Т.А. Долгова

Главный редактор

ректор, профессор И.М. Жарский

© УО «Белорусский государственный  
технологический университет», 2015

УДК 004.021

В. Л. Колесников, проф., д-р техн. наук;  
А. И. Бракович, доц., канд. техн. наук;  
Я. А. Жук, магистрант  
(БГТУ, г. Минск)

## **КОНСТРУИРОВАНИЕ И ВИЗУАЛИЗАЦИЯ СТОХАСТИЧЕСКИХ МОДЕЛЕЙ ЗАГРЯЗНЕНИЯ ПРИЗЕМНЫХ СЛОЕВ АТМОСФЕРЫ ПО ДАННЫМ НАБЛЮДЕНИЙ**

В настоящее время основой для моделирования загрязнения приземных слоев атмосферы является расчет распространения примесей в атмосферном воздухе от источника загрязнения с учетом параметров источника и окружающей среды. Процесс распространения промышленных выбросов в атмосфере происходит вследствие их адвентивного перенесения воздушными массами и диффузии, которая сопровождается турбулентными пульсациями воздуха. Для этого используются зависимости Гаусса, Лагранжа и Эйлера [1]. При этом увеличение и снижение содержания конкретного загрязняющего вещества нужно определять в каждой точке воображаемой пространственной сетки и за отдельные промежутки времени. Тогда моделирование можно свести к уравнению, которое может быть решено аналитически. В результате выводится формула, которая описывает шлейф с гауссовым распределением концентрации – так называемую гауссову перьевую модель.

Современные методы математического моделирования атмосферных процессов позволяют рассчитать на основе статистических данных об объемах выбросов загрязняющих веществ в контрольных точках и строить изолинейные карты распределения концентраций загрязняющих веществ. Основной областью применения расчетных методов является нормирование выбросов на уровне предприятий, но это не исключает их применения и при решении научных задач, связанных с оценкой экологической обстановки в пределах больших территорий. При расчете предельно допустимых выбросов (ПДВ) предприятий используются специальные расчетные методики, учитывающие параметры каждого источника загрязнения, климатические условия, характер подстилающей поверхности. Описанные методы моделирования загрязнения атмосферы, основанные на расчетах диффузионного и турбулентного рассеивания выбросов вредных веществ из устья точечного источника, оценивают экологическую ситуацию на больших расстояниях от источника и на больших площадях загряз-

ненных территорий. Кроме того, такие модели нельзя проверить на адекватность, поскольку отсутствует дисперсия воспроизводимости.

Данная работа дополняет описанную методологию, позволяет вычислить степень адекватности получаемых моделей и основана на проведении натуральных испытаний. Границы экспертируемых территорий составляют 10 – 20 км. Источником информации служат накопленные результаты замеров концентрации загрязняющих веществ, осуществляемых как стационарными так и передвижными лабораториями за произвольный отрезок времени.

Для решения перечисленных задач разработано программное средство для конструирования и визуализации разновидностей стохастических математических моделей (рисунок), описывающих загрязнение окружающей среды, путем подбора линейаризирующих преобразующих соответствий.

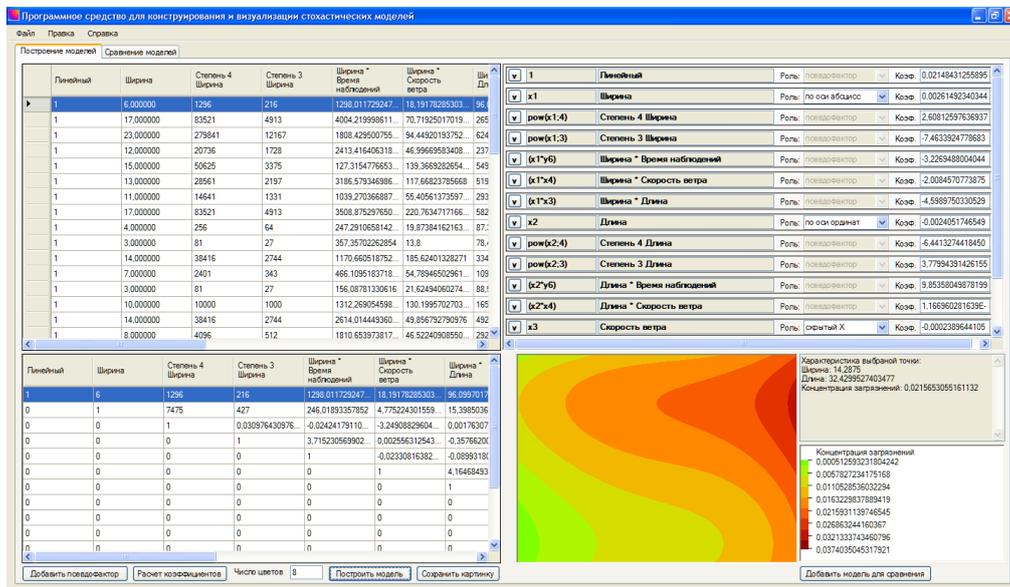


Рисунок - Интерфейс пользователя разработанного программного средства

Вводя псевдофакторы в таблично заданную функцию, можно увеличивать размерность расширенной матрицы, и, не меняя методики вычислений коэффициентов полиномиальных моделей, можно получать нелинейные, достаточно многообразные и сложные математические описания объектов.

## ЛИТЕРАТУРА

1. Колесников, В. Л. Компьютерное моделирование и оптимизация химико-технологических систем: учеб. пособие для вузов / В. Л. Колесников, П. П. Урбанович, И. М. Жарский. – Минск: БГТУ, 2004. – 532 с.

А. М. Шитько, магистрант;  
Н. В. Пацей, доц., канд. тех. наук  
(БГТУ, г. Минск)

## **ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА P2P ДЛЯ ЗАЩИЩЕННОГО ОБМЕНА ДАННЫМИ**

Одной из разновидностью p2p сети является частично децентрализованная (гибридная), в которой существует сервер, используемый для координации, поиска или предоставления информации о существующих участниках сети и их статусе.

Определена структура системы защищенного обмена данными, выбрана его элементная база. Сервер проектируется на языке Java с использованием Spring framework. В качестве реализации p2p-протокола выбрана библиотека JXTA. На сервере будет установлен SSL-сертификат для организации защищенного соединения с участниками сети. В качестве хостинга настроена Google App Engine. Вся передаваемая пользователями информация храниться в Google Cloud SQL, которая представляет собой реляционную базу данных, хранящаяся в «облаке» Google.

Важным преимуществом системы является упрощенная (для пользователя) регистрация на основе протокола авторизации OAuth 2.0. Он позволяет выдавать права на доступ к ресурсам пользователя без предоставления его логина и пароля. Вместо этого каждый пользователь получает «токен» доступа, который является результатом авторизации и пропуском к защищенному ресурсу.

В ходе процедуры регистрации «пир» посылает get-запрос на OAuth -сервер, в теле которого содержатся идентификатор клиента, полученный сервером социальной сети, URL перенаправления, на который будет направлен пользователь после успешной авторизации, и тип ответа «code» для получения кода от сервера. Дополнительно для пользователя создается универсальный уникальный идентификатор (UUID), генерируемый средствами библиотеки JXTA при создании объекта «Peer» и отсылается на сервер. После успешной авторизации на Spring-сервер отсылается «code». Далее для получения токена доступа с сервера посылается get-запрос. После чего на сервер приходит ответ в формате JSON с токеном доступа и идентификатором пользователя. Для получения персональных данных пользователя необходимо сделать еще один запрос на объект «users.get». Возвращается ответ в формате JSON с персональными данными клиента.

## **СТАТИЧЕСКИЙ АНАЛИЗ КОДА МОБИЛЬНЫХ ПРИЛОЖЕНИЙ КАК СРЕДСТВО ВЫЯВЛЕНИЯ ЕГО УЯЗВИМОСТЕЙ**

Проблема информационной безопасности мобильных систем на сегодняшний момент особо актуальна. Это связано с масштабностью такого явления как мобильность: 6 млрд. абонентов сотовой сети по всему миру, 1,7 млрд. мобильных устройств в сумме продано за прошлый год [1].

Рядовые пользователи не задумываются о безопасности конфиденциальной информации, которую злоумышленник может получить из их же мобильного устройства (личная переписка, финансовые данные, интеллектуальная собственность). Поэтому необходимо уделять проблематике безопасности мобильных систем особое внимание [2].

Можно привести следующую классификацию уровней угроз в отношении мобильных систем:

- физический (кража или непосредственное взаимодействие злоумышленника с мобильным устройством);
- аппаратный (закладки и уязвимости на аппаратном уровне, шпионские устройства, информация сотовых операторов);
- системный (закладки и уязвимости на уровне операционной системы);
- приложений (закладки и уязвимости в системных и сторонних приложениях, использование пользовательской информации хранящейся на сервере не по назначению);
- социальный (методы социальной инженерии).

Можно также привести классификацию для средств защиты используемых в мобильных системах:

- аппаратные (шифрование с использованием специальных модулей встраиваемых в устройство, механическое отключение радио-модулей);
- системные (шифрование с использованием средств встроенных в операционную систему, системные механизмы авторизации и аутентификации);
- прикладные (антивирусы для мобильных устройств, анализаторы приложений попадающих в маркеты, приложения для доступа к корпоративной сети);

- обучающие (материалы и курсы для повышение грамотности в сфере информационной безопасности).

Статический анализ кода – это проверка исходного кода приложения без реального выполнения на соответствие определенному набору правил. Такой вид анализа может использоваться для выявления ошибок и уязвимостей в исходном коде программного обеспечения. Программа выполняющая статический анализ называется статическим анализатором [3].

Анализ может проводиться либо над исходным кодом либо над объектным (MSIL, байт-код). Статический анализ не гарантирует 100% выявления ошибок и уязвимостей. Возможны ложные (false positive) и ложноотрицательные срабатывания (false negative) статического анализатора. По этой же причине статический анализатор в общем случае не предназначен для исправления найденных ошибок и уязвимостей. Он предупреждает программиста о подозрительных и потенциально проблемных участках кода [4].

Статический анализатор можно отнести к прикладному классу средств защиты используемых в мобильных системах. С помощью моделирования уязвимостей с последующим их внедрением в приложения, а также разработки алгоритма их определения можно построить статический анализатор, который будет выявлять уязвимости в приложениях для мобильных систем. Такой анализатор может использовать механизм синтаксических деревьев с целью обеспечения более высокоуровневой работы с исходным кодом при его анализе на соответствие условиям алгоритма выявления определённой уязвимости.

В докладе анализируется применение статического анализатора для выявления смоделированной уязвимости типа SQL Injection. Результаты анализа представлены в виде скриншотов.

#### ЛИТЕРАТУРА

1. Furnell, S. Mobile Security - A Pocket Guide. Ely: IT Governance, 2009. 82 p.
2. Drake, J. J. Android Hacker's Handbook. Indianapolis: Wiley, 2014. 576 p.
3. Bergman, N. Hacking Exposed: Mobile Security Secrets & Solutions. NY: Mc Graw Hill, 2013. 289 p.
4. Chess, B. Secure Programming with Static Analysis. Boston: Addison-Wesley Professional, 2007. 624 p.

**СПОСОБЫ РАБОТЫ С ТРЕХМЕРНОЙ АНИМАЦИЕЙ**

Компьютерную анимацию применяют не только в мультфильмах и фильмах, но и в симуляторах сложных систем. В таких программных тренажерах от точности представления взаимодействия с окружающей средой зависит полезность применения программы в процессе обучения.

Наиболее популярными программными комплексами для создания и анимации реалистичной визуальной среды являются 3D Studio Max и Maya.

Процесс создания анимированного объекта можно условно разделить на следующие основные этапы: проектирование модели, проектирование и описание атомарного движения, генерация сложных движений на основе последовательности атомарных движений, сохранение информации о движении и последующее ее воспроизведение.

Так как самым сложным объектом является человек, методы и расчеты для создания анимации будут рассмотрены на его примере.

Наиболее простая и широко используемая схема представления модели - в виде дерева. Суть его в том, что скелет персонажа представляется деревом  $S = D(V, E)$ , где  $V$  - множество звеньев скелета (вершин дерева),  $E$  - множество соединений (ребер дерева). За корень, как правило, принимается узел, совпадающий с центром масс персонажа, а от него ответвляются ветки рук, ног и т.д. [1]. Для того, чтобы определить положение, например, кисти руки персонажа в глобальной системе координат ( $V_w$ ), необходимо вычислить следующую формулу:

$$V_w = T_w(x, y) R_w(\Theta_w) T_s R_s(\Theta_s) T_c R_c(\Theta_c) T_b R_b(\Theta_b) T_f R_f(\Theta_f) T_h R_h(\Theta_h) V,$$

где  $T$  - матрицы относительного смещения,  $R$  - матрицы относительного поворота,  $\Theta$  - значение обобщенной координаты. Индексы указывают относительно каких элементов выполняются смещения и повороты. Вектор  $V$  - это положение точки на кисти в системе отсчета кисти, а  $V_w$  - положение этой точки в глобальной системе координат. Изменение значения обобщенных координат ведет к изменению положения и ориентации элементов скелета персонажа при задании его движения.

Рассмотренная задача определения положения и ориентации кисти персонажа в глобальной системе по известному набору обобщенных координат называется прямой задачей кинематики. Существует и обратная задача кинематики, когда по известному положению

звена необходимо рассчитать набор обобщенных координат. Как правило, такой метод используется следующим образом: на скелетной модели персонажа выбираются ключевые звенья и задаются их положения и ориентации, а значения промежуточных звеньев вычисляются, используя методы обратной кинематики. Таким образом, для задания движения достаточно определить последовательность значений в ключевых звеньях скелета персонажа. Метод обратной кинематики, как правило, используется в совокупности с другими методами описания анимации, например с методом анимации по ключевым кадрам, основанным на методе интерполяции.

Для моделирования движений, или эффектов, которые трудно воспроизвести с помощью ключевых кадров, используется процедурная анимация. В процедурной анимации рассчитывают текущие значения параметров анимации, основываясь на начальных значениях, заданных пользователем, и на математических выражениях, описывающих изменение параметров во времени.

Самым интересным методом анимации является метод захвата движений. Эта технология включает в себя наложение движений реальных актеров на модели виртуальных персонажей. На теле актеров закрепляется набор датчиков, отслеживающих движения, которые после оцифровываются и записываются в определенный формат. Метод захвата движения заключается в преобразовании данных о положении датчиков в последовательность значений обобщенных координат скелетной модели персонажа [2]. Эта технология максимально упрощает процесс создания анимации персонажа, позволяя использовать уже готовые движения актеров.

Для облегчения работы широко используется метод синтеза движений, что позволяет сократить число параметров необходимых для описания движения за счет использования комбинирования движений на основе высокоуровневой модели описания движения. Такой подход не требует от пользователя глубокого понимания динамики естественных движений моделируемых персонажей, все низкоуровневые детали, такие как движения каждой части тела, доработает компьютер.

#### ЛИТЕРАТУРА

1. Vieira da Silva, A New Interface Paradigm for Motion Capture Based Animation Systems. // Eurographics Workshop on Animation and Simulation, 1997.
2. Bobby Bodenheimer. The Process of Motion Capture: Dealing with the Data. // Eurographics CAS '97.

УДК 004.658

Ал-Исаум Висам Чяад Карим, магистрант;  
В.В. Смелов, канд. техн. наук, доц.  
(БГТУ, г. Минск)

## **МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУБД**

Одним из основных критериев выбора системы управления базами данных (СУБД) является уровень информационной безопасности, который она способна обеспечить. На сегодняшний день на рынке программного обеспечения с большим отрывом от других производителей лидируют три СУБД: Oracle (корпорация Oracle), DB2 (компания IBM) и Microsoft SQL Server (корпорация Microsoft) – эти продукты демонстрируют современные технологии управления данными. Анализ технологий обеспечивающих безопасное хранение больших объемов данных, позволил их обобщить и сформулировать в виде обобщенной модели информационной безопасности СУБД.

Модель представляет собой описание принципов взаимодействия, разбитых на девять вложенных уровней наборов объектов базы данных, сервера СУБД и операционной системы. Причем, на самом глубоком уровне вложенности рассматриваются реляционные таблицы БД, а на самом внешнем – пользователи, роли, процессы, службы и файлы операционной системы. В общей сложности, на всех девяти уровнях модели, описывается взаимодействие 28 различных типов объектов. Кроме того, модель включает описание трех процессов: аутентификации, авторизации и аудита.

Модель является обобщенной и поэтому в полной мере, всеми свойствами и технологиями, рассмотренными в модели не обладает ни одна из перечисленных СУБД, но можно говорить об уровне соответствия любой СУБД (применяется термин «конформности») данной модели.

Предлагаемая модель может быть использована для обобщенного описания принципов обеспечения информационной безопасности современными СУБД, а также как эталон, применимый для сравнения различных СУБД. Во втором случае, модель необходимо дополнить метриками, позволяющими получить количественные оценки уровня конформности исследуемой СУБД данной модели.

УДК 004.422.8

Мирончик. А.В., магистрант; В.В. Смелов, доц.  
(БГТУ, г. Минск)

## **АВТОМАТИЗАЦИЯ ПРОЦЕССОВ КОМПЛЕКТАЦИИ И ПОИСКА АВАРИЙНЫХ ТЕЛЕЖЕК СТАНЦИИ СКОРОЙ ПОМОЩИ**

Аварийная медицинская тележка – это набор кюветов, выдвижных ящиков и полок, передвигаемая на колесах, используется в больницах для транспортировки оборудования, медикаментов и применения их в экстренных случаях для реанимации больных.

Содержимое аварийной тележки может различаться в разных больницах [1]. Любая неисправность оборудования аварийных тележек, неполная их комплектация, а также несвоевременная их доставка может создать угрозу жизни человека, поэтому процедуры проверки комплектации и поиска подходящих аварийных тележек являются актуальными задачами.

Проблема навигации аварийных медицинских тележек внутри помещений не может быть решена с помощью GPS-технологии ввиду значительного ослабления сигнала в стенах и перекрытиях зданий и недостаточной точностью позиционирования. Поэтому для решения данной проблемы предлагается использовать систему позиционирования в режиме реального времени Quipra, позволяющую обрабатывать сигнал BLE(Bluetooth low energy)-маяков.

Для автоматизации проверки аварийных тележек была применена технология NFC. У каждой медсестры на мобильном Android-телефоне установлено специальное программное обеспечение, принимающее уведомления о необходимости проверки комплектации определенной медицинской тележки. При этом каждой тележке крепится NFC-маяк, позволяющий считывать, содержащийся в ней перечень оборудования и медикаментов.

УДК 004.422.8

С.А. Пекарь, магистрант; В.В. Смелов, доц.  
(БГТУ, г. Минск)

## **ПРОГРАММНАЯ АНИМАЦИЯ СЛОЖНЫХ 3D ОБЪЕКТОВ В РЕАЛЬНОМ ВРЕМЕНИ**

Компьютерная анимация – вид мультипликации, создаваемый при помощи компьютера. В отличие от более общего понятия «графика CGI», относящегося как к неподвижным, так и к движущимся изображениям, компьютерная анимация подразумевает только движущиеся. На сегодняшний день она получила широкое применение как в

области развлечений, так и в производственной, научной и деловой сферах. Являясь производной от компьютерной графики, анимация наследует те же способы создания изображений: векторная графика, растровая графика, фрактальная графика, трёхмерная графика (3D).

Наибольший интерес представляет процедурная анимация. Процедурная анимация – это вид компьютерной анимации, который автоматически генерирует анимацию в режиме реального времени согласно установленным правилам, законам и ограничениям. В отличие от предопределённой анимации, когда аниматор вручную определяет каждый кадр и все параметры создаваемой анимации, при процедурной анимации результат может быть в некоторой мере непредсказуем и при каждом запуске может генерировать разнообразную анимацию.

Процедурная анимация используется для создания и моделирования системы частиц (дым, огонь, вода), ткани и одежды, динамики твёрдых тел, динамики волос и меха, а также для анимации гуманоидных и негуманоидных персонажей.

В компьютерных играх процедурная анимация часто используется для таких простых вещей, как поворачивание головы персонажа, когда игрок озирается по сторонам (например, в игре Quake III Arena).

УДК 681.5.015.42

Н. В. Пацей, доц., канд. тех. наук,  
(БГТУ, г. Минск)

### **ПРОГРАММНАЯ ИМИТАЦИОННАЯ МОДЕЛЬ ПАРАЛЛЕЛЬНОГО КАСКАДНОГО ДЕКОДИРОВАНИЯ НА ОСНОВЕ КОДОВ НИЗКОЙ ПЛОТНОСТИ ПРОВЕРОК НА ЧЕТНОСТЬ**

Под параллельным каскадным кодом понимается схема кодирования/декодирования, состоящая из двух параллельно соединенных через перемежитель кодов. Если совместно с кодом низкой плотности проверок на четность использовать еще один помехоустойчивый код корректирующая способность системы декодирования возрастает. Однако, дополнительный кодовый процесс добавляет проверочные биты и снижает скорость кода. Кроме того, дополнительное кодирование/декодирование усложняет и замедляет помехоустойчивую систему.

Задачей построенной параллельной модели было увеличение скорости декодирования за счет взаимной коррекции логарифмического отношения правдоподобия кодового слова (Log-likelihoods Ratios - LLR) декодеров после каждой итерации и распараллеливания процесса декодирования, что позволит сократить число итераций декодирования, а также снизить вероятность ошибочного декодирования.

ния.

Основная подсистема модели – блок-корректор. Он анализирует полученную с декодеров апостериорную вероятность после первой итерации, принимает жесткое решения по векторам и вычисляет синдромы для решения вопроса об окончании процесса декодирования, в противном случае взаимно корректирует апостериорные вероятности для следующей итерации.

Выполнено компьютерное имитационное моделирование системы передачи информации с параллельным декодированием. Для сравнения производительности представлены результаты работы систем на основе трех различных декодеров: параллельного каскадного, последовательного каскадного и одиночного. Минимальное расстояние ( $d = 10$ ) и скорость кодеров ( $R = 1/2$ ) одинаковые.

УДК 512.8; 681.55

Ю. О. Герман, ассист., канд. тех. наук (БНТУ, г. Минск);

О. В. Герман, доцент, канд. тех. наук (БГТУ, г. Минск)

### РАБОТА СО ЗНАНИЯМИ С ИСПОЛЬЗОВАНИЕМ МОДАЛЬНЫХ ОПЕРАТОРОВ

Практический интерес связан с системами нечетких модальных логик. Основные недостатки известных методов нечеткого модального вывода – не универсальность, большая вычислительная сложность и наличие ограничений на применение правил вывода. В настоящей работе предлагается процедура вывода с более широкими рамками применения, достигаемыми, правда, за счет аппроксимации логических заключений на базе многозначных логик Я. Лукасевича. Подход демонстрирует связь между  $n$ -значными логиками Я. Лукасевича и нечеткими модальными системами при  $n \rightarrow \infty$ . Заменим модальные формулы формулами 3-значной логики Я. Лукасевича. Формула  $x$  имеет значения  $\{0, 0.5, 1\}$  в 3-значной логике Лукасевича, причем 0 соответствует значению «невозможно», 0.5 – значению «не определено» и 1 – значению «необходимо». (в альтернативной нотации пишем  $val(z) = \{1, 2\}$  с  $val(z) = (n - ) \cdot val(x)$ ). Далее примем

$$\Box x \leftrightarrow val(x) = 1,$$

$$\Diamond \leftrightarrow val(x) \geq 0.5, \text{ т.к.}$$

$$\neg \Diamond x \equiv \Box \neg x \leftrightarrow val(x) = 0.$$

Для манипулирования формулами используем следующие замены ( $x_1, x_2, y_1, y_2$  – двузначные переменные):

$$x \equiv x_1 \cdot x_2, \neg \equiv \neg_1, \neg_2),$$

$$x \vee y \equiv x_1 \vee_1, x_2 \vee_2),$$

$$\neg \equiv \neg_1, \neg_2),$$

$$x \& y \equiv x_1 \&_1, x_2 \&_2),$$

$$x \rightarrow y \equiv \neg_1 \vee_1 = \neg_2 \vee_2, \neg_1 \vee_2).$$

Исходя из этого формула  $\diamond \leftrightarrow$  , а формула  $\Box x \leftrightarrow \cdot x_2$  , что позволяет перейти от модальных формул к классическим булевым формулам и использовать существующие методы логического вывода в классической логике (например, метод резолюций). Подход легко обобщается на нечеткие модальные формулы, а также на формулы модальной логики предикатов. Приведены практические примеры использования рассматриваемых систем знаний.

УДК 003.26+347.78

Шутько Н. П., асп.; Романенко Д.М., канд. техн. наук;  
Урбанович П. П., д-р техн. наук  
(БГТУ, Минск)

### **МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ ТЕКСТОВОЙ СТЕГАНОГРАФИИ НА ОСНОВЕ МОДИФИКАЦИИ ПРОСТРАНСТВЕННЫХ И ЦВЕТОВЫХ ПАРАМЕТРОВ СИМВОЛОВ ТЕКСТА**

Объект исследования — стеганографические методы защиты прав интеллектуальной собственности на текстовые документы.

Предмет — модели стеганографических процессов на основе использования параметров шрифта: цвет, кегль, апрош и кернинг.

В докладе рассматриваются и анализируются подходы к построению указанной математической модели на основе модификации пространственных и цветовых параметров шрифта. Электронный документ-контейнер,  $B$ , представляем через дискретную функцию  $f(x,y) \in \{0,1\}$ , которая определяет координату для каждого пикселя изображения в двумерном пространстве (или массиве)  $A$ . Для анализа и описания процессов осаждения/извлечения тайной информации используются горизонтальный и вертикальный профили: проекции массива пикселей, формирующих растр изображения текста, значения элементов которых определены функцией  $f(x,y)$  на одну из осей —  $x$  или  $y$ .

Вводится понятие «дополнительный ключ» стегопреобразования,  $K_d$ : конкретное секретное значение криптографического алгоритма, используемое для зашифрования и расшифрования сообщения (или, например, для помехоустойчивого кодирования/декодирования) соответственно при осаждении и извлечении авторской информации.

На основании выполненного исследования сформулированы выводы.

1. Моделируемой стеганографической системой называем совокупность сообщений,  $M$ , контейнеров,  $B$ , ключей (основной —  $K$  и  $K_d$ ), стегосообщений,  $S$ , и преобразований (прямое — осаждение,  $F$ , и

обратное – извлечение,  $F^{-1}$ ), которые их связывают:  $\Sigma = (M, B, K, K_d, S, F, F^{-1})$ .

2. Рассматриваемый тип стегопреобразования предложено классифицировать как «двухключевая стegosистема».

3. Математическая модель основывается на теоретико-множественном определении функции.

4. Алгоритм осаждения/извлечения тайного сообщения  $M_i$  в контейнер (из контейнера)  $B_j$  основывается на модификации и анализе горизонтальных и вертикальных профилей битовой карты фрагментов текста.

УДК 004.021

С.И. Акунович, доц., канд. тех. наук  
(БГТУ, г. Минск)

## **ФОРМАЛИЗАЦИЯ ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ НА РАЗРАБОТКУ СИСТЕМ ЛОГИЧЕСКОГО УПРАВЛЕНИЯ**

Логическое управление - вид управления, который основывается на истинности и ложности каких-либо предпосылок и высказываний.

Автоматизация логического управления осуществляется с помощью аппаратных и программных средств, получивших название устройств или систем логического управления (УЛУ или СЛУ).

Проектирование СЛУ начинается с выработки технического задания (ТЗ) на проектирование. В ТЗ содержатся основные сведения об объекте проектирования, условиях его эксплуатации, а также требования, предъявляемые заказчиком к проектируемому изделию.

Требования могут выражаться в виде текстовых утверждений и графических моделей. При разработке требований часто возникают проблемы двусмысленности, неполноты, и несогласованности отдельных требований. Устранение этих проблем на этапе разработки требований стоит на несколько порядков меньше, чем устранение этих же проблем на поздних стадиях разработки.

Требования обычно используются как средство коммуникации между различными заинтересованными лицами. Это означает, что требования должны быть просты и понятны для обычных пользователей и разработчиков.

Вопрос об интеллектуальном взаимопонимании специалистов зачастую играет ключевую, основополагающую роль и во многом определяет успех сложных проектов.

Ведущими в области автоматизации фирмами мира до сих пор не был выбран (разработан) единый язык формализации требований для задач логического управления.

Под формализацией требований будем понимать представление человеческих знаний на формальном или частично формальном языке.

В докладе рассматривается язык формализации требований для сложных задач логического управления, имеющий следующую концептуальную структуру:

*Команды* - внешние воздействия на СЛУ;

*Входы* - воздействия датчиков управляемого объекта на СЛУ, а также внутренние воздействия от входных соединителей;

*Выходы* - воздействия на управляемый объект, а также внутренние воздействия на выходные соединители;

*Формулы* - структура СЛУ в виде логические формул;

*Супервизоры* - формулы запрещенных ситуаций в СЛУ;

*Валидаторы* - формулы соответствия входов и выходов СЛУ;

*Алгоритмы* - поведение СЛУ в виде текстовых или графических форм алгоритмов;

*Запуск алгоритмов* - условия запуска алгоритмов;

*Таймеры* - временные зависимости СЛУ и управляемого объекта;

*Соединители* - разъемные соединения частей СЛУ;

*Функциональные блоки* - дочерние алгоритмы СЛУ, а также модели «вход - выход» непрерывных элементов;

*Функции* - функции, вызываемые из *Формул, Супервизоров, Валидаторов, Алгоритмов, Таймеров* и *Функциональных блоков*.

Предлагаются программные средства верификация требований, целью которой является обнаружение и устранение противоречий и неоднозначностей в требованиях, их уточнение и систематизация;

Для валидации требований, которая решает задачу оценки правильности сформулированных требований, в первую очередь, соответствия причинно - следственных отношений вход - выход СЛУ, разработаны средства их функционально - эквивалентных преобразований в инструментальные среды моделирования и анализа.

Таковыми средами являются:

- электронные таблицы (MS EXCEL, VBA);
- исполняемые графические программы на языках LD, FBD и SFC стандарта IEC 61131-3 (ISAGRAF 6);
- программы на языке высокого уровня DELPHI (RAD STUDIO XE 7);
- наглядные графические представления структуры СЛУ (логических формул) и алгоритмов функционирования в приложении MS Visio.

И. А. Веялкин, магистрант;  
Д. В. Шиман, доц., канд. тех. наук,  
(БГТУ, г. Минск)

## ОБЗОР СТРУКТУРЫ АЛГОРИТМОВ ПОИСКА НА ОСНОВЕ ОТПЕЧАТКОВ АУДИО ДАННЫХ

Системы на основе алгоритмов отпечатков аудиоданных относятся к классу задач распознавания образа, включают в себя, в частности, задачу музыкального поиска и применяются для решения различного рода проблем, среди прочих:

- автоматический мониторинг радиовещания с целью проверки авторских прав на ротируемые музыкальные произведения;
- поиск аудио файлов по записанному с микрофона фрагменту;
- поиск дубликатов в музыкальной коллекции.

Отпечаток аудиоданных - есть компактная сигнатура на основе данных аудио сигнала, которая обобщает аудиозапись. В процессе получения отпечатков аудиоданных (в системах идентификации аудио на основе содержимого аудио сигнала) извлекают перцепционный дайджест части аудио сигнала (то есть отпечаток) и сохраняют его в базе данных.

Перцепционный дайджест – это свертка, краткое изложение на основе признаков (англ. *features*), относящихся к восприятию человеческого слухового аппарата.

Проблема автоматической идентификации аудио сигнала происходит из-за большой размерности и значительного варьирования звуковых данных для схожего на слух содержимого.

Когда поступает фрагмент неизвестного аудио сигнала, его отпечаток рассчитывается и сравнивается с теми, что сохранены в базе данных. Используя отпечатки и алгоритмы поиска соответствия (англ. *matching algorithms*), которые характеризуются набором параметров и методами проверки и оценки соответствия, даже существенно искаженные версии записи могут быть идентифицированы и сопоставлены с эталонным аудио файлом из предварительно составленной базы данных аудио записей.

В докладе рассматривается общий подход и структура алгоритмов поиска на основе отпечатков аудио данных, а также приводятся примеры частных реализаций с указанием причин выбранных решений. Описываются проблемы поиска, специфичные контексту рассматриваемых задач, и возможные комбинации методов для их преодоления. Описываются параметры оценки эффективности, сложности и адекватности алгоритмов поиска, применяемых для принятия решения о целесообразности выбора конкретного подхода для решения конкретной прикладной задачи.

УДК 004.021

М. В. Гладкий, магистрант; П. П. Урбанович, проф.  
(БГТУ, г. Минск)

## **БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЙ НА ПЛАТФОРМАХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ**

Одной из проблем в области практического использования облачных технологий является их безопасность. Следует постоянно модернизировать существующие и разрабатывать новые средства и механизмы защиты, способные обеспечить решение данной проблемы.

При использовании облачных вычислений периметр сети размывается или исчезает. Это приводит к тому, что защита более уязвимой части облака определяет общий уровень защищенности.

Можно провести следующую классификацию угроз в отношении облачных вычислений [1]:

- разграничение сети;
- динамичность виртуальных машин;
- уязвимости и атаки внутри виртуальной среды;
- защищенность данных и приложений;
- доступ системных администраторов к серверам и приложениям;
- защита бездействующих виртуальных машин;
- влияние традиционной безопасности на производительность;
- управление обновлениями.

Услуги по защите информации предлагают немало компаний. Но лишь некоторые из них этих предложений обеспечивают достаточно эффективную защиту, позволяющую в полном объеме обезопасить приложения от всех возможных видов атак. Данные атаки в зависимости от типа угроз и уровня воздействия можно разделить на следующие классы [2]:

- традиционные атаки на ПО;
- функциональные атаки на элементы облака;
- атаки на клиента;
- атаки на гипервизор;
- атака на виртуальные машины при их переносе с одного узла на другой;
- атаки на системы управления.

В свою очередь средства защиты в виртуальных средах можно условно подразделить на две группы.

К первой относятся средства защиты, которые поставляются в виде готовых аппаратных решений или в виде виртуальных устройств. Преимущества таких решений – быстрая скорость развертывания и

ввода в эксплуатацию, использование существующих аппаратных мощностей заказчика, экономия ресурсов (место в стойках, электропитание, кондиционирование) [3].

Вторую группу образуют средства, предназначенные для защиты непосредственно виртуальных машин и контроля коммуникаций в виртуальной среде (на уровне гипервизора). К ним относятся:

- межсетевые экраны (брандмауэры);
- средства обнаружения и предотвращения вторжений;
- средства контроля целостности;
- средства защиты от вредоносных программ, учитывающие виртуализацию;
- средства защиты от несанкционированного доступа;
- средства контроля политик безопасности в виртуальных инфраструктурах.

Основным преимуществом этих средств является специализация на защите виртуальных сред и коммуникаций в них. Среди производителей средств защиты для виртуальных сред можно отметить следующие компании: Trend Micro, Symantec, CheckPoint, StoneSoft, «Код Безопасности», Reflex Systems [4].

Рассмотренные в докладе методы и средства защиты имеют свои достоинства и недостатки. Зашифровав только одну часть облака, не предоставляется возможность защитить конфиденциальную информацию. Соответственно, для защиты данных на платформах облачных вычислений нужен комплексный подход, совмещающий использование шифрования с другими средствами защиты, включающих в себя программную реализацию межсетевого экрана, обнаружения и предотвращения вторжений, контроля целостности, защиты от вредоносного кода и анализа журналов.

#### ЛИТЕРАТУРА

1. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. Москва: ДМК Пресс, 2012.
2. Степаненко, В. Облачная обработка данных – миф или реальность? Москва: Сети и бизнес, 2010.
3. Риз, Д. Облачные вычисления. Санкт-Петербург: БХВ-Петербург, 2011.
4. Александров, А. Как предотвратить вторжение: второй уровень защиты. Москва: ВУТЕ, 2009.

УДК 004.853

Н. И. Гурин, канд. физ.-мат. наук, доцент,  
Я. А. Жук, магистрант  
(БГТУ, г. Минск)

## **ГЕНЕРАТОР СЕМАНТИЧЕСКОЙ СЕТИ КАК РЕЛЯЦИОННОЙ БАЗЫ ДАННЫХ**

Разработан генератор базы знаний информационной системы для функционирования ее виртуального консультанта, использующего модули генерации базы знаний и обеспечения диалога с пользователем. Для организации базы знаний используется модель представления знаний в виде семантической сети и, в частности, наиболее компактное ее представление в виде списка дуг и информационных объектов в таблице реляционной БД.

Полями данной таблицы выступают две информационные единицы и тип связи между ними. Главной особенностью разработанной семантической сети является связь типов отношений с заранее составленными наборами грамматических шаблонов простых предложений при помощи внешнего ключа.

Процесс генерации семантической сети на основе БД представляет собой формирование SQL-запросов на добавление строк в описанную таблицу. Для этого генератор семантической сети выполняет ряд последовательных операций. В первую очередь выполняется удаление из текста информационной системы оборотов, не несущих смысловой нагрузки. Далее происходит расшифровка сокращений, содержащих точки, которая позволяет перейти к следующему этапу – разбиению текста на предложения, как основные единицы значения. Затем следует дальнейшее разбиение сложных предложений на логические блоки по запятым и скобкам. Полученные в результате неполные логические блоки дополняются до самостоятельных простых предложений при помощи предыдущих блоков или причастий внутри блока. Далее следует сравнение простых предложений с подготовленными грамматическими шаблонами при помощи регулярных выражений для определения типа связи. Затем по подходящему грамматическому шаблону выполняется выделение в предложении семантически связанных информационных единиц. На заключительном этапе информационные единицы приводятся в именительный падеж и записываются вместе с типом связи в виде строки SQL-запроса на вставку.

Генератор базы знаний разработан на языке программирования Python и успешно апробирован для функционирования виртуального консультанта в компьютерной сети.

УДК 681.391

Кудлацкая М. Ф., асп. (БГТУ, г. Минск)

### ПРОГРАММНАЯ РЕАЛИЗАЦИЯ ИМИТАЦИОННОЙ МОДЕЛИ АДАПТИВНОГО МНОГОПороГОВОГО ДЕКОДИРОВАНИЯ

Программная модель адаптивной системы кодирования (декодирования) [1] включает следующие функциональные блоки: кодер, декодер, генератор ошибок, имитацию реального канала связи, алгоритм выбора пороговых значений [3], алгоритм идентификации кратности ошибок [2]. Адаптивная система кодирования/декодирования позволяет в режиме без отключения связи локализовать единичную битовую ошибок, т.е. определить параметр BER [1], за счет использования алгоритма определения кратности исправляемой ошибки, что позволяет определить качество канала (таблица 1) [1].

**Таблица 1 - Вероятность определения кратности ошибки в процессе декодирования**

Длина информационной последовательности	Кратность ошибки		
	1	2	3
	вероятность определения ошибки		
64	1	0,99	0,98
128	0,99	0,74	0,76
256	0,92	0,95	0,73

В том случае если качество канала не соответствует желаемому, система динамически изменяет параметры кода [1]. Т. о. разработанная система адаптируется к качеству канала связи, уменьшая скорость кода и повышая надежность передачи информации.

#### ЛИТЕРАТУРА

1. Виткова М.Ф. Адаптивная система кодирования/ декодирования на основе многомерных итеративных кодов и многопороговых декодеров. / М.Ф. Виткова, Д.М. Романенко // Труды БГТУ. Сер. VI, Физ.-мат. науки и информатика. – 2014. – С. 116-120.
2. Виткова, М.Ф. Анализ возможности оптимизации многопорогового декодирования многомерных итеративных кодов // Сборник научных работ 63-ой НТК студентов и магистрантов БГТУ, 23-28 апреля 2012. – Минск, БГТУ – Ч4 – 2012, с. 332 – 335.
3. Разработка теоретических основ адаптивного декодирования избыточных кодов с исправлением многократных, модульных ошибок и стираний в спутниковых каналах связи: отчет о НИР (промеж.) / БГТУ; рук. темы Д. М. Романенко. – Минск, 2013. – 40 с. – № ГР 20131234.

## **ОСОБЕННОСТИ ПРОГРАММНОЙ ИМИТАЦИОННОЙ МОДЕЛИ ПРОЦЕССА ДЕКОДИРОВАНИЯ ЛИНЕЙНЫХ ИЗБЫТОЧНЫХ КОДОВ С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ**

Повышение эффективности существующих кодов – одна из основных задач в помехоустойчивом кодировании. Существует тенденция использования нейронных сетей для решения данной задачи

Нейронные сети являются весьма противоречивым, но перспективным методом работы с информацией. Следует отметить, что нейронные сети используются для решения целого ряда задач, таких как аппроксимация, кластеризация, прогнозирование и распознавание образов.

В помехоустойчивом кодировании нейронные сети можно использовать как декодер для линейных блочных кодов. В качестве примера приведем применение нейронной сети для декодирования кода Хэмминга, рассмотренное далее.

При использовании кода Хэмминга 7,4 передаются по сети 7 бит. Однако информационных только 4 бита, что дает нам 16 вариантов сообщений после кодирования. Будем использовать нейронную сеть для декодирования полученного сообщения на предмет выбора одного из этих вариантов. Фактически необходимо решить задачу классификации. Наиболее подходящей для решения такой задачи является сеть Геленбе. Исходные данные – это 7 бит сообщения после кодирования и 16 вариантов этих сообщений. Строим сеть с входом в 7 бит и рекуррентной связью между нейронами. Данный слой позволит найти корреляцию между битами информации. Следующий слой из 16 нейронов, связанный прямой связью с предыдущим слоем, произведет классификацию. На выходе сети предполагается получать нулевое значение в одной из ячеек и единицы в других ячейках. Сеть обучается на примерах входных и выходных значений, по методу градиентного спуска, где происходит минимизация количества ошибок при классификации.

После обучения сети, полученные характеристики можно использовать в алгоритмах декодирования, при этом вычисления значительно уменьшаются. Данный метод предполагает универсальность применения к блочным кодам и показывает более высокие характеристики обнаружения ошибок, которые близки к «мягкому» декодированию. Однако увеличение кодовой последовательности значительно усложняет процесс декодирования, что определяет необходимость дальнейших исследований в данной области.

УДК 004.031.43 – 044.962

А. С. Кобайло, доц.; Н.А. Жилияк, доц. (БГТУ, г. Минск)

## СИНТЕЗ СПЕЦИАЛИЗИРОВАННЫХ ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВ НА БАЗЕ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ С ЗАДАНЫМИ ХАРАКТЕРИСТИКАМИ

До сегодняшнего времени созданы системы автоматизированного проектирования БИС и СБИС [1], цифро-аналоговых [2], логических [3,] структур, трассировки, компоновки, выпуска технической документации (САПР P-CAD, AUTOCAD, OrCAD и др.). В то же время отсутствуют средства автоматизации структурного и функционального проектирования, что связано, в первую очередь, с отсутствием математических методов решения проблемы [4].

Вышесказанное обуславливает необходимость разработки математических методов синтеза вычислительных систем на основе математических моделей или алгоритмов их функционирования с учетом требований реализации вычислительного процесса в реальном времени.

Непосредственно синтез математических моделей с требуемыми свойствами осуществляется посредством преобразования графа алгоритма реализации исходной (базовой) математической моделью в соответствии с полученными векторами параметров, обеспечивающих удовлетворение совокупности требуемых свойств. Таким образом, в качестве исходных данных программа синтеза математических моделей вычислительных процессов (моделирующих физические процессы, технические системы) с требуемыми свойствами использует:

а) аналитическое выражение исходного процесса

$$Y = F(X), \quad (1)$$

где  $X$  – вектор параметров базовой математической модели;  $Y$  – вектор выходных данных;

б) векторы параметров математических моделей с требуемыми свойствами

$$\{X_r(P_r)\},$$

где  $P_r$  –  $r$ -й вектор совокупности требуемых свойств.

Множество векторов параметров математической модели были получены в результате реализации алгоритма формирования векторов параметров с требуемыми свойствами, который можно представить следующими шагами:

– формирование характеристической логической функции (ХЛФ) совокупности требуемых свойств при известных ХЛФ отдельных свойств;

– определение наборов переменных, при единичном значении которых ХЛФ совокупности свойств принимает единичное значение;

– исключение векторов параметров, полученных при выполнении предыдущего пункта, векторов, для которых ХЛФ отдельных свойств не равны единице.

После прохождения всех шагов алгоритма формируется граф алгоритма реализации математической модели  $F(x)$  с требуемыми свойствами, посредством выполнения операции простого элементарного гомоморфизма над парой вершин  $u$  и  $v$  графа алгоритма реализации базовой математической модели вычислительного процесса.

В результате выполнения различных преобразований над исходным графом получаем множества графов  $\{Gr = (Vr, Er)\}$  алгоритмов реализации усеченных математических моделей со свойствами  $\{Pr\}$ . И далее выполняем обратный переход для каждого из графов  $\{Gr\}$  от топологии и его спецификации к аналитическому выражению математической модели с требуемыми свойствами.

Рассмотренная методика синтеза математических моделей с заданными характеристиками использовалась при синтезе специализированных вычислительных устройств для формирования отраженных сигналов.

Синтезированные устройства, по сравнению с использованием обобщенной математической моделью, обладают следующими свойствами: простота, низкие себестоимость, энергопотребление, вес, габариты, высокая надежность.

## ЛИТЕРАТУРА

1. Горбатов, В.А. Автоматизация проектирования сложных логических структур / В. А., Горбатов, В. Ф. Демьянов., Г. Б. Кулиев; Под ред. В. А. Горбатого. – М.: Энергия, 1987. – 352 с.
2. Автоматизация проектирования аналогово-цифровых устройств / Э. И. Гитис, Б. Л. Собкин, А. Н. Подколзин и др.; под ред. Э. И. Гитиса. – М.: Энергоатомиздат, 1987. – 182 с.
3. Автоматизация проектирования вычислительных структур / А. В. Каляев, В. Н. Меликов., В. М. Курейчик и др. – Ростов н/Д.: Изд-во Ростовского университета, 1983. – 221 с.
4. Анкудинов, Г.И. Синтез структуры сложных объектов: Логико-комбинаторный подход / Г. И Анкудинов. – Л.: Изд-во Ленинградского ун-та, 1986. – 212 с.

## **СТАТИЧЕСКИЕ ХАРАКТЕРИСТИКИ ИЗМЕРИТЕЛЬНЫХ КАНАЛОВ ПРОМЫШЛЕННЫХ КОНТРОЛЛЕРОВ**

Наличие автоматизации технологических процессов стало обязательным условием в современных экономических условиях. Период экстенсивного пути повышения уровня автоматизации за счет установки измерительных приборов с необходимой точностью и настройкой локальных контуров практически завершился. Получение конкурентных преимуществ требует применения более сложных алгоритмов, адаптации локальных контуров под действием изменяющихся контуров и оптимизации в реальном времени.

На сегодняшний момент основные задачи управления реализуются с помощью программируемых логических контроллеров (ПЛК) для построения распределенных систем управления. Основные алгоритмы управления реализуются обычно на данном уровне управления. Это касается как локальных контуров стабилизации основных технологических параметров, так и более сложных многоконтурных алгоритмов. Более сложные алгоритмы реализуются резидентно на ПЛК на базе программного обеспечения промышленных компьютеров и серверов. Источником информации для первичного и вторичного уровня все равно выступает первичная информация с модулей аналогового ввода ПЛК. В большинстве своем они имеют ограничение разрядности на уровне 10-12 bit. Основные результаты теории управления получены для случая присутствия в измерительных каналах белого шума.

С целью оценки свойств случайных возмущений в измерительных каналах был проведен ряд экспериментов, базой для которых служил контроллер VIPA 200V. Он относится к серии средних ПЛК. К входам были подключены датчики температуры и давления различных производителей. Анализ информации проводили в системе MatLAB.

Встроенные в MatLAB тесты: Jarque–Bera, Lilliefors, Kolmogorov–Smirnov – указывают на то, что измерительные каналы подвержены влиянию шумов с нормальным распределением. Более строгий тест Kolmogorov–Smirnov указал на нормальность только при большой длительности наблюдения. Визуально распределение плотности в большинстве соответствовало «колоколу» Гаусса с различным значением дисперсии. Однако один из каналов кроме основного центрального пика имел боковые лепестки, что говорит о необходимости аккуратно применять методы теории автоматического регулирования разработанные для случая белого шума и оценка особенностей случайной информации в измерительном канале не будет лишней.

Е. А. Блинова, аспирант  
П. П. Урбанович, профессор, докт. тех. наук,  
(БГТУ, г. Минск)

## **КЛАССИФИКАЦИЯ И СРАВНИТЕЛЬНАЯ ОЦЕНКА МЕТОДОВ ТЕКСТОВОЙ СТЕГАНОГРАФИИ**

Стеганография – такой способ передачи скрытого сообщения по открытому каналу или хранение скрытого сообщения в открыто хранящемся объекте, при котором не возникает подозрений о наличии скрытого сообщения. Секретное сообщение встраивается в не привлекающий внимания объект, который направляется адресату или размещается в общедоступной области. Основными критериями оценки стеганографических методов являются пропускная способность, незаметность, помехоустойчивость и безопасность.

Для передачи стегосообщений используются различные виды других сообщений, называемых контейнерами: изображения, звуковые и видео-файлы, использование особенностей работы протоколов передачи данных.

В докладе рассматриваются синтаксические и лингвистические методы текстовой (контейнером является текстовый документ) стеганографии, производится их сравнительная оценка. Синтаксические методы основаны на изменении отображения текста, лексические – на формировании или модификации текста-контейнера, в зависимости от метода, с помощью которого будет передаваться стегосообщение.

Рассматриваются методы, представляющие собой комбинацию синтаксических и лексических методов в применении к содержащим текст объектам, например к HTML-страницам. Для передачи скрытого сообщения в HTML-файлах могут быть использованы: нечувствительность тегов HTML к регистру, возможность страницы содержать пробелы и знаки табуляции после закрывающихся тегов, безразличие к порядку следования атрибутов в тегах для интерпретатора HTML.

Рассматривается также отдельный подкласс методов, который формирует стегоконтейнер в зависимости от используемых исходных данных.

## СОДЕРЖАНИЕ

<i>Колесников В.Л., Бракович А.И., Жук Я.А.</i> Конструирование и визуализация стохастических моделей загрязнения приземных слоев атмосферы по данным наблюдений	3
<i>Шитько А. М., Пацей Н. В.</i> Использование протокола р2р для защищенного обмена данными	5
<i>Цыганенко Н. П.</i> Статический анализ кода мобильных приложений как средство выявления его уязвимостей	6
<i>Смолич Е. Ю.</i> Способы работы с трехмерной анимацией	8
<i>Ал-Исаум Висам Чяад Карим, Смелов В.В.</i> Модель информационной безопасности СУБД	10
<i>Мирончик. А.В., Смелов В.В.</i> Автоматизация процессов комплектации и поиска аварийных тележек станции скорой помощи	11
<i>Пекарь С.А.</i> Программная анимация сложных 3d объектов в реальном времени	11
<i>Пацей Н. В.</i> Программная имитационная модель параллельного каскадного декодирования на основе кодов низкой плотности проверок на четность	12
<i>Герман Ю. О., Герман О. В.</i> Работа со знаниями с использованием модальных операторов	13
<i>Шутько Н. П., Романенко Д.М., Урбанович П. П.</i> Математическая модель системы текстовой стеганографии на основе модификации пространственных и цветовых параметров символов текста	14
<i>Акунович С. И.</i> формализация технических требований на разработку систем логического управления	15
<i>Веялкин И. А., Шиман Д. В.</i> Обзор структуры алгоритмов поиска на основе отпечатков аудио данных	17
<i>Гладкий М. В., Урбанович П. П.</i> Безопасность приложений на платформах облачных вычислений	18
<i>Гурин Н. И., Жук Я. А.</i> Генератор семантической сети как реляционной базы данных	20
<i>Кудлацкая М. Ф.</i> Программная реализация имитационной модели адаптивного многопорогового декодирования	21
<i>Драко А. М.</i> особенности программной имитационной модели процесса декодирования линейных избыточных кодов с использованием нейросетевых технологий	22
<i>Кобайло А. С., Жиляк Н.А.</i> Синтез специализированных вычислительных устройств на базе математических моделей с заданными характеристиками	23
<i>Сухорукова И.Г.</i> Статические характеристики измерительных каналов промышленных контроллеров	25
<i>Блинова Е.А., Урбанович П.П.</i> Классификация и сравнительная оценка методов текстовой стеганографии	26