МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

ИНЖЕНЕРНЫЕ КАДРЫ – БУДУЩЕЕ ИННОВАЦИОННОЙ ЭКОНОМИКИ РОССИИ

Материалы II Всероссийской студенческой конференции

Йошкар-Ола, 21-25 ноября 2016 г.

Часть 4

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – ОСНОВА СТРАТЕГИЧЕСКОГО ПРОРЫВА В СОВРЕМЕННОЙ ПРОМЫШЛЕННОСТИ

Йошкар-Ола
2016

УДК 378:004
ББК 74.58
И 62

И 62 **Инженерные кадры – будущее инновационной экономики России:** материалы II Всероссийской студенческой конференции (Йошкар-Ола, 21-25 ноября 2016 г.): в 8 ч. *Часть 4. Информационные технологии – основа стратегического прорыва в современной промышленности.* – Йошкар-Ола: Поволжский государственный технологический университет, 2016. – 248 с.
ISBN 978-5-8158-1789-0
ISBN 978-5-8158-1790-6 (Часть 4)

В рамках Всероссийской студенческой конференции представлены результаты научно-исследовательских работ студентов, магистрантов, аспирантов в области информационных технологий с перспективой их практического использования.

УДК 378:004
ББК 74.58

ISBN 978-5-8158-1790-6 (Часть 4)
ISBN 978-5-8158-1789-0

ПРЕДИСЛОВИЕ

В настоящем издании представлены материалы секции «Информационные технологии – основа стратегического прорыва в современной промышленности» Всероссийской студенческой конференции «Инженерные кадры – будущее инновационной экономики России», которая проходила в рамках одноимённого Форума 21-25 ноября 2016 года в Поволжском государственном технологическом университете (г. Йошкар-Ола). Это мероприятие входило в широкомасштабный профориентационный молодёжный проект «Работай в России!», инициированный Союзом машиностроителей России. Состав и география её участников показали, что конференция вызвала большой интерес студентов не только в нашем регионе, но и в стране в целом.

Тематика секции связана с применением информационных технологий в различных областях: промышленности, строительстве, медицине, образовании и т.п. Материалы конференции отражают результаты молодежных исследований в актуальных сегодня областях:

- сетевые технологии,
- встраиваемые системы,
- информационная безопасность,
- САПР,
- высокопроизводительные вычислительные системы,
- системы хранения данных.

Статьи, представленные для публикации, рассмотрены программным комитетом конференции. Лучшие из них включены в настоящий сборник. По результатам представлений докладов многие из авторов отмечены дипломами соответствующей степени.

Организаторы конференции выражают уверенность в том, что заинтересованный обмен мнениями с коллегами и единомышленниками послужит важным импульсом для дальнейших научных исследований и получения новых практических результатов в области применения информационных технологий.

Редакционная коллегия благодарит всех авторов статей, их научных руководителей и консультантов за материалы, представленные для публикации, и надеется на дальнейшее сотрудничество.

УДК 004.35

Асланов Антон Сергеевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Морохин Дмитрий Витальевич, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем,
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

УЛЬТРАЗВУКОВЫЕ ДАТЧИКИ

Введение

Выбранная тема является важной для процесса разработки систем определения качества изделия, диагностики организма, измерения расстояний. Из всех вышеперечисленных областей наиболее актуальным является применение данных датчиков в локальных системах позиционирования. Главная идея состоит в том, чтобы создать систему из ультразвуковых датчиков, которая позволит осуществлять автономную навигацию мобильных роботов. Применение данной идеи возможно при организации систем сортировки на складах, рассадке семян в палисаднике и, в принципе, при автоматизации любой рутинной работы по перемещению объектов в закрытых помещениях.

Среди различных способов определения расстояния используются следующие рассмотренные нами методы:

- ультразвуковой, основанный на принятии отражённого звука от объекта измерения;
- инфракрасный, основанный на принятии отражённого света от объекта измерения.

Ультразвуковые помехи встречаются намного реже, чем помехи освещённости. По этой причине был выбран ультразвуковой метод.

Работа ультразвуковых датчиков основана на измерении времени между излучением и приятием отражения. Соответственно ультразвуковой датчик состоит из модуля, излучающего ультразвук, модуля, принимающего ультразвук, системы, управляющей вышеперечисленными модулями.

Режимы работы ультразвуковых датчиков

Встречаются три основных режима работы, которые определяют устройство ультразвуковых датчиков: оппозитный, диффузионный и рефлекторный режимы.

Для *оппозитного режима* характерны два отдельных устройства, передатчик и приемник, которые монтируются друг напротив друга. Если ультразвуковой пучок прерывается объектом, выход активизируется. Такой режим подходит для работы в тяжелых условиях, когда важна устойчивость к интерференции. Ультразвуковой пучок только один раз проходит сигнальное расстояние. Такое решение отличается высокой стоимостью, поскольку требуется монтаж двух устройств – передатчика и приемника.

Диффузионный режим обеспечивается передатчиком и приемником, находящимися в одном корпусе. Стоимость такого монтажа значительно ниже, однако время срабатывания дольше, чем при оппозитном режиме. Диапазон обнаружения здесь зависит от угла падения на объект и от свойств поверхности объекта, поскольку луч должен отражаться от поверхности самого обнаруживаемого объекта.

Для *рефлекторного режима* излучатель и приемник также находятся в одном корпусе, однако ультразвуковой луч теперь отражается от рефлектора. Объекты в диапазоне обнаружения обнаруживаются как путем измерения изменений в расстоянии, которое проходит ультразвуковой луч, так и путем оценки потерь на поглощение или отражение в отраженном сигнале. Звукопоглощающие предметы, а также предметы с угловыми поверхностями легко обнаруживаются при таком режиме работы датчика. Важное условие – не должно изменяться положение опорного рефлектора.

Обзор технических характеристик ультразвуковых датчиков

− *Максимально возможное измеряемое расстояние*. Данный параметр зависит от мощности излучения, от чувствительности приёмника, от условий среды.

− *Рабочая зона*. Под данным термином подразумеваются угол работы датчика.

− *Слепая зона*. Область, при нахождении в которой передатчика приёмник не сможет получить излучённый ультразвук.

Также датчики обладают характеристиками, которые относятся к большинству электрических устройств: напряжение питания, потребляемый ток и т.д.

Области применения ультразвуковых датчиков

Как уже было сказано выше, ультразвуковые датчики используются для диагностики организма. УЗИ аппараты являются одним из основных инструментов диагностики. Оборудование передает импульсы с частотой 1-18 МГц с помощью преобразователя ультразвука в тело об-

следуемого пациента. Сигналы распространяются по телу к границе между разными тканями. Некоторые волны частично отражаются обратно, а остальные продолжают движение в теле. Отраженные сигналы поступают на датчик, а затем в центральный процессор, который обрабатывает их и выдает картинку на дисплей.

Также ультразвуковые датчики применяются в системах «умного» дома. На основе датчиков движения можно организовать управление светом, управление бытовой техникой или же охранные системы.

Возможно применение в сельскохозяйственной технике, например, определение высоты растений для более эффективного распыления химических веществ. В промышленных и частных автомойках, где необходим контроль уровня мыла и воска в автоматических автомойках. Емкостные датчики способны выявить уровень жидкости в пластиковых резервуарах, что помогает операторам произвести своевременную замену и т.д., и т.п.

Подводя итоги, отметим, что были рассмотрены датчики измерения расстояния в общем и ультразвуковые датчики в частности. В данный момент ведётся разработка ультразвукового датчика, в котором излучатель и приёмник расположены в различных местах, и организация их работы.

Список литературы

1. Малов В. В. Пьезорезонансные датчики. – М.: Энергия, 1978.

2. Дж. Фрайден. Мир электроники. Современные датчики: справочник. – М.: Техносфера, 2005.

3. Ультразвук. Основы теории распространения ультразвуковых волн [Электронный ресурс]. – URL: http://engineering-solutions.ru/ultrasound/theory/#radiator_feature

4. Суслов П. А. Система локального позиционирования // Инженерные кадры – будущее инновационной экономики России: материалы Всероссийской студенческой конференции: в 8 ч. – Йошкар-Ола: ПГТУ, 2015. – Часть 4. Информационные технологии – основа стратегического прорыва в современной промышленности. – С. 105-107.

5. Ультразвуковые датчики. Особенности применения и выбора [Электронный ресурс]. – URL: http://mega-sensor.ru/articls/ultrazvukovye-datchiki-osobennosti-primenenija-i-vybora.html

УДК 512.57, 512.64

Белогусев Андрей Климентьевич
направление Информатика и вычислительная техника
(магистратура), гр. ИВТм-11

Научный руководитель
Малашкевич Василий Борисович, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СИСТЕМА ТАРГЕТИРОВАННОЙ РЕКЛАМЫ

Таргетированная реклама (англ. target – цель) – это Интернет-реклама (текстовые или мультимедийные объявления), тематика и состав которой подбирается индивидуально для каждого пользователя в соответствии с его интересами и предпочтениями. Выбор тематики рекламных сообщений основан на личных данных потребителя рекламы, таких как адрес нахождения, возраст, пол, образование, должность, интересы и др. Индивидуальный подход обеспечивает высокую эффективность таргетинговых рекламных компаний и быстрое достижение таких целей, как формирование и поддержка спроса, побуждение пользователей к действию, улучшение узнаваемости бренда. Это обеспечивает высокий спрос на организацию и проведение таргетинговых рекламных компаний. Поэтому проблема разработки автоматизированных систем таргетинговой рекламы является актуальной задачей.

В современном Интернет можно найти ряд примеров реализации технологий таргетинговой рекламы. К ним относятся системы индивидуальной рекламы поисковых сайтов. Здесь выбор темы рекламы для конкретного пользователя опирается на поисковые запросы этого пользователя. Большое распространение системы таргетинговой рекламы нашли в социальных сетях. В качестве примера таких систем можно отметить сервис Autopilot сети ВКонтакте.

К недостаткам этих систем следует отнести их закрытость и жесткую привязку к конкретному сайту.

Задачей разработки является создание универсальной подсистемы таргетинговой рекламы, обеспечивающей конфигурирование и настройку под сайт заказчика системы.

Для решения поставленной задачи проведен анализ технологических процессов таргетированной рекламы. В частности выявлены следующие модули системы:

- База данных, содержащая сведения о потребителях рекламы
- База данных, содержащая рекламные материалы
- Блок опознавания пользователей
- Блок подбора рекламных материалов.

Основой таргетированной рекламы являются знания о предпочтениях и интересах пользователей. Эти знания формируются на основе личных сведений о пользователях, сохраняемых в базе данных. При этом пользователи могут оставаться анонимными – достаточно соотнести посетителя сайта с его идентификатором в базе данных. Знания об интересах пользователя могут извлекаться из любых доступных данных: анкет, заполняемых пользователем при регистрации, сообщений, оставляемых пользователем, истории посещений и т.д. Для извлечения знаний могут применяться методы Data Mining [2], нечеткой логики [3], решающих деревьев. Знания о пользователях должны периодически обновляться и учитывать наиболее актуальные интересы пользователей.

Источником рекламы являются заказчики рекламных компаний. Предоставляемые ими рекламные материалы должны храниться в базе данных в классифицированном и отсортированном виде. Это обеспечит быстрый отбор рекламы, наиболее отвечающей предпочтениям конкретного пользователя. Самый простой способ достижения этой цели – классификации рекламы по ключевым словам.

Опознавание пользователей может основываться либо на идентификационных данных (логии/пароль), вводимых при посещении сайта, либо на доменном имени и IP-адресе хоста, на котором работает пользователь.

Задачей блока подбора рекламных материалов является сопоставление выявленных предпочтений пользователя с имеющимися рекламными материалами. Алгоритм подбора рекламных материалов должен учитывать не только прямые совпадения интересов пользователя с характеристиками рекламы, но и обеспечивать более широкое пространство и направления поиска индивидуальной рекламы. Например, если пользователь интересуется лекарством, ему, возможно, будут интересны и профильные медицинские центры, и рекомендации врачей и т.д.

Важной является также подсистема тарификации. Ее функция – оценка эффективности работы всей системы, на основе которой система должна подстраиваться и модернизироваться. Данные этой подсистемы также являются основой для ведения расчетов с заказчиками рекламы.

Решение поставленных задач требует разработки обработчиков и парсеров слабоструктурированных данных, применения алгоритмов обработки больших данных (BigData), приемов анализа сетевого трафи-

ка и др. Реализация проектируемых подсистем может быть выполнена с применением различных алгоритмических языков и средств программирования.

Список литературы
1. https://ru.wikipedia.org/wiki/Таргетинг
2. https://ru.wikipedia.org/wiki/Data_mining
3. https://ru.wikipedia.org/wiki/Нечёткая_логика
4. https://ru.wikipedia.org/wiki/Дерево_принятия_решений

УДК 630*434

Блинов Антон Владимирович
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Морохин Дмитрий Витальевич, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ЭЛЕКТРОННАЯ БАРАБАННАЯ УСТАНОВКА НА БАЗЕ ARDUINO MEGA

В основе принципа работы покупных электробарабанов лежат пэды (имитаторы барабанов с резиновой поверхностью), оснащенные датчиками. Они производят передачу звука через специальный звуковой модуль, состоящий из процессора эффектов, секвенсора, синтезатора звуков различных установок и целого набора других полезных функций.

В нашем случае модуль сделан на базе платы Arduino Mega. 16 аналоговых входов принимают сигналы с установки. С каждым барабаном, модуль соединен с помощью разъемов джек.

BQ0-BQ9 – пьезоэлементы;

G1-G3 – герконы;

A0-A15 – аналоговые входы Arduino.

К компьютеру плата подключается через USB.

Резисторы позволяют не только ограничить напряжение, но и регулировать чувствительность и громкость, тем самым обеспечивая точную настройку. Для барабанов очень важно, чтобы одиночный удар генерировал одиночный сигнал, без побочных колебаний. В этом также помогает пеноматериал конусоидальной формы, закрепленный на пьезоэле-

менте. Вся конструкция звукоснимателя закреплена в корпусе и прижата сеткой.

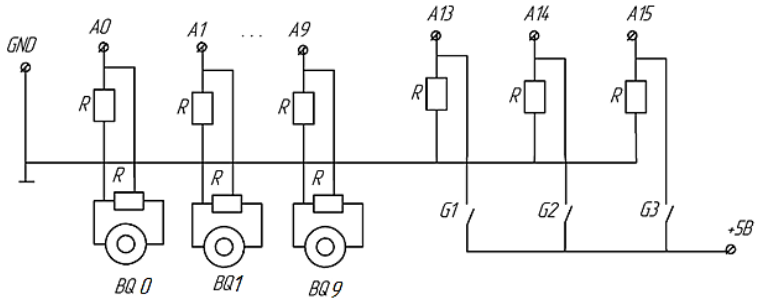


Рис. 1. Функциональная схема

Чтобы смягчить удары палочки по тарелкам, на «рабочую» область я наклеил пористую резину толщиной 5 мм. Датчик был приклеен к тарелке с обратной стороны на скотч.

Сигнал с педалей генерируется с помощью магнита и разомкнутого геркона. Магнитоуправляемый контакт (геркон) представляет собой электрический аппарат, изменяющий состояние электрической цепи посредством механического размыкания или замыкания ее при воздействии управляющего магнитного поля на его элементы.

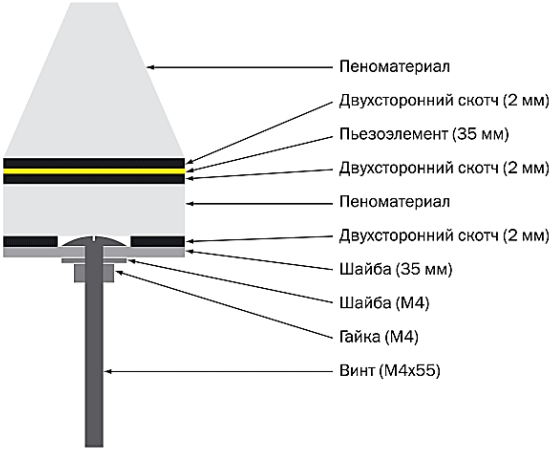


Рис. 2. Конструкция узла съема сигнала

Все звуки хранятся и воспроизводятся на компьютере, так как это гарантирует минимальную задержку.

Программа разработана в QT Creator на языке C++. Громкость каждого барабана регулируется отдельно. Она также позволяет отслеживать число приходящих сигналов, что помогает с настройкой.

Заключение

Данный проект можно дорабатывать до совершенства, т.е. до полной имитации акустической установки, еще очень долго. Передовые разработчики в этой сфере уже очень близки к этому. В нашем же случае это бюджетный вариант, который подходит начинающим барабанщикам.

В будущем планируется подключить mp3 shield с картой памяти, чтобы исключить зависимость от компьютера.

Список литературы

1. Русская документация по языку программирования и библиотекам [Электронный ресурс]. –URL: http://arduino.ru

2. Официальная страница QT Creator [Электронный ресурс]. – URL: http://wiki.qt.io/Category:Tools::QtCreator

УДК 621.391

Бондарев Сергей Юрьевич
направление Информационная безопасность (магистратура)
Ситников Игорь Владимирович
направление Информационная безопасность (аспирантура)

Научный руководитель
Сидоркина Ирина Геннадьевна, д-р техн. наук, профессор,
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

МЕТОД БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО ГОЛОСУ

В современном мире огромное внимание уделяется информационным технологиям. Тысячи программистов работают над тем, чтобы предотвратить запрещенный доступ в здания, к компьютерам, мобильным телефонам и многому другому, что является неотъемлемой частью нашей жизни. С каждым годом сделать это все сложнее и сложнее. Все чаще обычные пароли, PIN-коды, смарт-карты и другие подобные идентификаторы не в силах остановить злоумышленника. Но все большее

значение начинает приобретать идентификация личности по биометрическим параметрам. Это такие физиологические и поведенческие характеристики человека, которые делают его уникальным.

Биометрические свойства человека:

- отпечатки пальцев;
- геометрия лица;
- радужная оболочка глаза;
- голос;
- почерк и др.

К плюсам биометрической идентификации можно отнести то, что в отличие от обычных методов защиты данный метод исключает потерю идентификатора и соответственно кражу информации.

Актуальность темы. На сегодняшний день все учащаются случаи запрещенного доступа в сфере информационной безопасности. Злоумышленники легко взламывают пароли, проникают в здания с ограниченным доступом, преодолевая различные системы защиты. На смену обычным паролям приходят биометрические методы идентификации. Большинство из них являются более надежными, но далеко не все находят себе место в наши дни. Один из самых популярных методов – идентификация по опечаткам пальцев. Другие методы требуют большего развития, чтобы их стали чаще внедрять в повседневную жизнь. Также стоит отметить, что даже большие структуры хотят внедрять систему идентификации по голосу. С учетом вышесказанного нет сомнений, что разработка нового программного средства идентификации личности по голосу является весьма актуальной.

Задачей биометрической идентификации является создание системы, которая работала бы с минимальным количеством отказов в доступе пользователям, а также на 100 % исключала несанкционированный вход злоумышленника в компьютер или какое-либо помещение ограниченного доступа. У каждого человека есть свои уникальные биометрические данные, которые являются его отличительными характеристиками. Эти характеристики нужны для того, чтобы «извлечь» их из человека, записать в базу данных, и затем при идентификации сравнить особенности характеристик идентифицируемого человека с данными из базы системы.

Человеческую речь можно классифицировать на несколько видов:

- нормативная;
- патологическая;
- преднамеренно измененная;
- эмоционально насыщенная и др.

Система распознавания личности

Работа систем распознавания состоит из двух этапов:

- регистрация нового пользователя;

- идентификация зарегистрированного пользователя (процесс распознавания).

Каждый пользователь проходит регистрацию в системе, записав образец своего голос. Далее из образца извлекаются признаки, благодаря которым и происходит распознавание. На основе этих признаков строятся «шаблоны» пользователей. Такой «шаблон» является структурой, которая при данных признаках устанавливает степень подобия. Признаки только что записанного голоса сравниваются с признаками голоса из базы данных, после чего происходит идентификация или отказ в доступе.

Подытожив, можно выделить три основных этапа в системе распознавания личности:

• *этап обработки сигналов*. Здесь происходит обработка самого сигнала с целью выделить признаки, необходимые для распознавания. Речевой сигнал представлен в виде определенной последовательности векторов признаков;

• *этап моделей*. На данном этапе идет построение модели, так называемого шаблона, с помощью которого и высчитывается степень подобия между имеющейся моделью и признаками;

• *этап принятия решений*. С помощью вычисленной степени подобия и заданных порогов принимается решение.

Алгоритм метода

В системах распознавания по голосу данный метод считается одним из самых популярных. Суть метода заключается в следующем [4]:

1. Подача последовательности отсчетов определенной части сигнала, которая исследуется на итерации x_0, ..., x_{N-1}.

2. Применение весовой функции для уменьшения искажений. Чаще всего в качестве весовой функции используют окно Хэмминга:

$$\omega_n = 0{,}54 - 0{,}46\cos\left(2\pi\frac{n}{N-1}\right), n = 0, \dots, N-1,$$

где N – размер окна в отсчетах.

3. Дискретное преобразование Фурье:

$$X_k = \sum_{n=0}^{N-1} x_n \omega_n e^{\frac{-2\pi i}{N}kn}, k = 0, \dots, N-1.$$

где k соответствует частотам

$$f_k = \frac{F_s}{N} k, k = 0, \dots, N/2,$$

где F_s является частотой дискретизация.

Также можно использовать быстрое преобразование Фурье:

$$X_p(i) = \sum_{i=0}^{255} S_p\,(t) e^{-j\frac{2\pi}{n}ni}.$$

Основная идея быстрого преобразования Фурье заключается в том, что каждую вторую выборку можно использовать для получения половинного спектра. Формально это означает, что формула дискретного преобразования Фурье может быть представлена в виде двух сумм.

4. Далее с помощью треугольных фильтров идет разбиение на диапазоны. Границы этих фильтров рассчитываются в шкале мел. Мел – единица высоты звука, основанная на восприятии этого звука нашими ушами. Формула для перевода в мел-частотную область:

$$B(f) = 1127 \times \ln(1 + \frac{f}{700}).$$

Формула обратного преобразования:

$$B^{-1}(b) = 700(e^{b/1127} - 1).$$

Чаще всего используют 24 фильтра. Количество фильтров обозначим как N_{FB}. Фильтры применяются к квадратам модулей коэффициентов преобразования Фурье, а затем высчитывается логарифм:

$$e_m = \ln(\sum_{k=0}^{N} |X_k|^2 H_{m,k}), m = 0, \dots, N_{FB} - 1.$$

где $H_{m,k}$ – весовые коэффициенты фильтров, которые были получены.

5. Дискретное косинусное преобразование является последним этапом данного метода. На этой стадии происходит вычисление мел-частотных **кепстральных** коэффициентов (MFCC):

$$c_i = \sum_{m=0}^{N_{FB}-1} e_m \cos\left(\frac{\pi i(m + 0{,}5)}{N_{FB}}\right), i = 1, \dots, N_{MFCC}.$$

Коэффициент c_0 – энергия сигнала, поэтому он не используется. Количество мел-частотных кепстральных коэффициентов на практике – порядка 12.

Кепстральные коэффициенты, основанные на методе линейного предсказания.

В данном методе также участвуют кепстральные коэффициенты. Смысл линейного предсказания основывается на возможности аппроксимировать текущий отчет с помощью линейной комбинации некоторого количества отчетов, сделанных до настоящего времени.

$$x_n \approx \sum_{k=1}^{p} a_k x_{n-k}\,.$$

У линейной комбинации a_1, ..., a_p есть весовые коэффициенты. Их называют коэффициентами линейного предсказания. Чтобы найти эти коэффициенты, нужно использовать рекурсивный алгоритм Дарбина.

Далее с помощью уже известных коэффициентов линейного предсказания находятся кепстральные коэффициенты. Следует отметить, что их количество может превышать количество коэффициентов линейного предсказания.

$$c_n = \begin{cases} a_n + \sum_{k=1}^{n-1} \frac{k}{n} c_k a_{n-k,} & 1 \le n \le p; \\ \sum_{k=n-p}^{n-1} \frac{k}{n} c_k a_{n-k}\,, & n > p. \end{cases}$$

Заключение

Достигнутые характеристики систем идентификации личности по голосу могут удовлетворять требованиям практической применимости при управлении финансовыми операциями или доступе к конфиденциальной информации. Стоимость ошибки велика, и необходимо значительно уменьшить вероятность пропуска посторонних пользователей при сохранении вероятности отказа целевому пользователю.

Список литературы

1. Рамишвили Г. С. Речевой сигнал и индивидуальность голоса. – Тбилиси, 1976.

2. Михайлов А. А., Колосков А. А., Дронов Ю. И. Основные биометрические системы // Алгоритм безопасности. – 2016.

3. Кузин М. В. Идентификация по голосу. Скрытые возможности // Information Security. – 2006. – С. 29.

4. Рабинер Л., Гоулд Б. Теория применения цифровой обработки сигналов. – М.: Мир, 1978.

УДК 681.511:3

Гладышев Александр Павлович
направление Информационная безопасность (магистратура), гр. БИм-21

Научный руководитель
Кречетов Александр Александрович, канд. техн. наук, доцент,
кафедра Информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

МЕТОДЫ ЗАЩИТЫ АУДИОФАЙЛОВ ОТ НЕСАНКЦИОНИРОВАННОГО РАСПРОСТРАНЕНИЯ С ПОМОЩЬЮ ВОДЯНЫХ ЗНАКОВ

Задача защиты информации от несанкционированного распространения была актуальна во все времена на протяжении всей истории человечества. С развитием общества и технологии развивались также средства и методы защиты информации. Сегодня одна из задач защиты информации – защита интеллектуальной собственности. Развивающиеся интернет-технологии дают практически неограниченный доступ к мультимедийным ресурсам и их несанкционированному распространению. В частности, это актуально для аудиофайлов.

Одной из задач защиты интеллектуальной собственности является защита цифровых музыкальных произведений. С целью получения выгоды от продажи своих музыкальных произведений авторы не публикуют их в открытом доступе. Многие владельцы авторских прав стремятся защитить от любого незаконного копирования свои творения. В последнее время все чаще проводится работа по отслеживанию фактов несанкционированного распространения аудиофайлов. На страницах сети Интернет можно найти сотни и тысячи их копий. Кроме того, музыкальные файлы при несанкционированном распространении часто меняются, что затрудняет их выявление правообладателями. Поэтому автору не только необходимо отыскать все копии, существующие в сети, но и доказать свои авторские права.

В настоящее время проводится множество конференций по проблемам информационной безопасности. С каждым годом растет число публикаций, посвященных методам стеганографии. В этом направлении науки работают многие российские и зарубежные ученые: В. Г. Грибунин, И. Н. Оков, Б. Я. Рябко, И. В. Туринцев, А. Н. Фионов, Р. Бергмар, К. Качин, М. Чапман, Ж. Чень, Д. Фридрич.

Способы защиты аудиофайлов с помощью водяных знаков. Требования, предъявляемые к водяным знакам.

Существует несколько способов, позволяющих защитить аудиофайлы от несанкционированного копирования и распространения, позволяющие доказать их создателю свое авторское право.

Метод цифрового отпечатка звукового файла.

При использовании этого метода с оригинального аудиофайла делается цифровой отпечаток, который храниться базе данных. Ввиду того, что цифровой отпечаток занимает значительно меньше места в сравнении с оригинальным файлом, можно создать большую базу данных цифровых отпечатков.

Метод встраивания в аудиофайлы идентификационной метки.

С помощью специальных алгоритмов в аудио-файлы встраиваются специальные идентификационные метки, незаметные для человеческого слуха. Данные метки можно обнаружить только специальными детекторами.

Встраивание идентификационных меток в аудиофайлы относится к методам стеганографии, а именно к одному из направлений стеганографии – цифровым водяным знакам (ЦВЗ). Стеганография и цифровые водяные знаки имеют общие принципы, но отличаются конечными целями. Целью стеганографии является сокрытие передаваемой информации. Цифровые водяные знаки применяют для противоположной цели. При использовании цифровых водяных знаков контейнерами служат мультимедийные аудиофайлы, а скрываемой информацией будет информация для идентификации автора произведения.

Для защиты от попыток злоумышленника изменить аудиофайл, защищенный цифровым водяным знаком, сам цифровой водяной знак должен обладать следующими свойствами:

– скрываемая информация должна быть стойкой к наличию различных окрашенных шумов, сжатию с потерями, фильтрованию, аналогово-цифровому и цифро-аналоговому преобразованиям;

– скрываемая информация не должна вносить в сигнал искажения, воспринимаемые системой слуха человека;

– попытка удаления скрываемой информации должна приводить к заметному повреждению контейнера для цифрового водяного знака или его непригодности для восприятия;

– цифровой водяной знак должен однозначно идентифицировать автора защищаемого файла;

– скрываемая информация не должна вносить заметных изменений в статистику контейнера.

Цифровые водяные знаки имеют небольшой объём, однако при их встраивании должны использоваться сложные методы встраивания.

Методы встраивания водяных знаков

На сегодняшний день существует несколько методов создания цифровых водяных знаков для защиты аудиофайлов:

Метод замены наименьших значащих бит.

Этот метод является простейшим способом внедрения конфиденциальной информации в какую-либо структуру данных. Используя звуковой сигнал, путем замены наименьших значащих бит каждой точки осуществления выборки, представленной двоичной последовательностью, можно зашифровать значительный объем информации. В каждом значении амплитуды наименьший значащий бит заменяется на бит сообщения. Недостатком данного метода является слабая устойчивость к посторонним воздействиям на сигнал (сжатие, воздействие шумов).

Метод внедрения информации с использованием эхо-сигнала.

Данный метод предполагает встраивание цифровых водяных знаков в контейнер путем изменения параметров эхо-сигнала. К параметрам эха, которые несут внедряемую информацию, относятся: начальная амплитуда, время спада и сдвиг (время задержки между исходным сигналом и его эхо). Оригинальный сигнал смешивается с одной или несколькими точными копиями, которые слегка отстают во времени. Когда сдвиг между оригинальным сигналом и его эхо уменьшается, система слуха человека воспринимает эхо-сигнал как добавочный резонанс. Недостаток данного метода – он слабо устойчив к сжатию.

Метод фазового кодирования.

Он заключается в разбиении сигнала на сегменты и замещении фазы начального сегмента аудиосигнала на фазу, которая характеризует данные. Фазы последующих сегментов регулируются в целях сохранения разности фаз между сегментами. Метод фазового кодирования является одним из методов, который устойчив к сжатию и воздействию шумов.

Метод растяжения спектра.

В методе растяжения спектра псевдослучайная последовательность, представляющая собой «белый шум». Эта последовательность модулируется сигналом несущей, представляющей цифровой водяной знак, и затем добавляется к аудиосигналу-контейнеру. Данный метод является относительно устойчивым к посторонним воздействиям.

Метод изменения масштаба временной оси.

В данном методе временная ось делится на части, которые незначительно растягиваются и сжимаются. Местоположение и степень сжатия/растяжения являются величинами, которые используются для коди-

рования информации. Метод устойчив к сжатию и различным искажениям.

Заключение

Рассмотрены методы защиты аудиофайлов от несанкционированного копирования и распространения. Данные методы могут быть использованы для защиты авторских прав и предотвращения незаконного распространения. На сегодняшний день существует большое количество методов внедрения цифровых водяных знаков, каждый из которых обладает своими достоинствами и недостатками, их надо учитывать при использовании того или иного метода для защиты мультимедийных данных от незаконного распространения и модификации.

Список литературы

1. Иваненко В. Г. Родченко С. В. Встраивание цифровых водяных знаков в аудиосигналы // Безопасность информационных технологий. – 2011. – № 1. – С. 94–95.

2. Иваненко В. Г., Пивошенко Я. И. Способ защиты авторского права на аудиосигналы, основанный на пакетной вейвлет-декомпозиции // Безопасность информационных технологий. – 2013. – № 1. – С. 72–74

3. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. – М.: Салон-Пресс, 2009.

4. Борисова С. Н. Методы защиты аудиофайлов от несанкционированного копирования и распространения // Фундаментальные исследования. – 2015. – № 5-3. – С. 481-487.

5. Завьялов С. В., Ветров Ю. В. Стеганографические методы защиты информации: учеб. пособие. – СПб.: Изд-во Политехн. ун-та, 2012. − 190 с.

УДК 004.31

Горохов Валерий Павлович
направление Информатика и вычислительная техника
(магистратура), гр. ИВТм-21

Научный руководитель
Васяева Елена Семеновна, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА ПОЖАРНОГО РОБОТА НА ГУСЕНИЧНОЙ ПЛАТФОРМЕ

Рассматривается задача создания прототипа автономной роботизированной платформы повышенной проходимости для тушения локаль-

ных очагов возгорания в местах, труднодоступных или опасных для человека. В рамках данной цели решаются также образовательные задачи, направленные на изучение принципов работы цифровых и аналоговых датчиков и формирование комплексного представления у школьников сложной автономной системы, включающей как аппаратную, так и программную части.

Назначение и область применения

Робот предназначен для обнаружения и тушения локальных очагов возгорания в условиях затруднённого или невозможного доступа для человека, а также в условиях опасной окружающей среды (загазованность, задымление, радиация). Кроме того, он может использоваться для патрулирования ограниченных территорий, например, пастбищ, парков, складов, применяться в системах электроснабжения и вентиляции, в дата-центрах.

Пожар может возникнуть в помещениях, куда люди заходят редко, например, в дата-центрах, серверных, вентиляционных и других технических помещениях. Современные системы обнаружения пожара, безусловно, сообщат о пожаре, но робот, патрулирующий территорию, находится непосредственно на месте и может начать тушить очаг возгорания ещё до прибытия пожарных. Ему не страшны вредные удушливые газы, выделяющиеся в атмосферу при горении галогеносодержащего пластика, из которого сделано большинство современных кабель-каналов.

Кроме того, такой робот будет полезен как система для дотушивания мелких очагов, а также для контроля за теми частями территорий, куда человеку доступ затруднён (под стеллажами, за станками и т.д.).

Робот-пожарный патрулирует территорию, объезжая препятствия. Он умеет определять, с какой стороны объехать встретившуюся ему на пути преграду, выбирая более короткий маршрут.

Реализуемые функции:

- патрулирование территории;
- обнаружение очага открытого огня;
- определение расстояния до пожара;
- объезд препятствия на пути к пожару;
- определение высоты, на которой возник пожар;
- тушение пожара.

Описание структуры и принципа действия робота

Принцип действия гусеничного робота с двумя двигателями основан на использовании специальных сенсоров и датчиков и интерпретации их показаний, а также управлении силовыми приборами. Робот едет

вперёд и сканирует пространство перед собой. Обнаружив пламя, он подъезжает к нему на расстояние 10-15 см от стрелы, останавливается, поднимает стрелу крана для получения оптимального угла струи воды и включает помпу. Насос остаётся включённым до тех пор, пока датчик пламени не перестанет фиксировать огонь. Дотушив источник возгорания, робот опускает стрелу в исходное положение и продолжает патрулировать территорию.

Робот-пожарный на гусеничной платформе.
Состав используемого оборудования

Кран собран из деталей робоконструктора MakeblockUltimateRobotKit. К стреле крепятся датчик пламени, ультразвуковой дальномер и трубка водяной помпы. Поскольку ёмкость резервуара ограничена, был предусмотрен контроль за уровнем воды через зазор на стенке резервуара, оставленный незаклеенным. На резервуаре имеется отметка минимального уровня воды, поскольку включённый насос без воды может сгореть.

Когда робот видит препятствие, то он определяет, с какой стороны препятствие короче. Для этого предназначены боковые дальномеры.

Алгоритм объезда довольно простой.

Если, например, расстояние, определяемое левым дальномером, больше, чем расстояние, определяемое правым дальномером, значит, левый дальномер препятствие не видит и можно его объехать с левой стороны.

Если оба дальномера выдают приблизительно одинаковые расстояния, то робот не может определить, с какой стороны его объехать, и объезжает с левой стороны.

Робот состоит из следующих блоков.

Ходовая часть состоит из гусеничной платформы Rover-5 с двумя встроенными моторами 20 мм. На передней части платформы закреплена стрела крана, собранного из деталей робоконструктора Makeblock.

Ходовую часть питают 6 батареек типа АА, которые крепятся в специальном держателе. Управление моторами происходит через специальную плату расширения – адаптер Motor Shield.

Функции *командного блока* выполняет контроллер ArduinoUno. Он служит для загрузки и исполнения кода микропрограммы и сопряжения с платами расширения.

Блок навигации содержит 3 инфракрасных дальномера и трёхосный компас Pololu AltIMU-10 v4, которые обнаруживают препятствия и подключаются к плате расширения TroykaShield.

Центральный более мощный дальномер видит препятствие на расстоянии от 20 до 120 см. По обеим сторонам от него стоят дальномеры, которые видят на расстоянии от 10 до 80 см.

Использование разных дальномеров даёт более точный результат при определении расстояния до препятствия.

Трёхосный компас используется для того, чтобы при объезде препятствий робот не сбился с курса. Компас располагается на самом ровном месте робота – сверху конструкции, ограждающей резервуар с водой.

Блок обнаружения пламени содержит датчик пламени и инфракрасный дальномер, которые также подключаются к плате TroykaShield.

Блок подачи воды состоит из погружной водяной помпы, которая подает воду из специального резервуара в трубку. Высота подачи воды может контролироваться с помощью подъёмного механизма, работающего от 12-вольтового мотора.

На рисунке приведена структура робота, поясняющая состав используемого оборудования.

В ходе подготовки проекта разработчики столкнулись с рядом трудностей, среди которых: влияние помех на цифровой компас, засвечивание датчика пламени источниками света, естественная погрешность в работе дальномеров, связанная с перемещением робота в пространстве, и т.д. В связи с этим были модифицированы алгоритмы функционирования робота и сама его конструкция.

Список литературы

1. Бачинин А., Панкратов В., Накоряков В. Основы программирования микроконтроллеров. – М.: ООО «Амперка», 2013. – 207 с.

2. Васяева Е. С., Васяева Н. С. Специфика обучения школьников основам робототехники // Ресурсы робототехнических конструкций как инструмента воспитания и образования детей и юношества: сборник статей по материалам круглого стола в рамках XIX Вавиловских чтений – международной междисциплинарной научной конференции. – Йошкар-Ола: Поволжский государственный технологический университет, 2016. – С. 88-94.

3. Уэйт М., Прата С., Мартин Д. Язык СИ. Руководство для начинающих / пер. с англ. – М.: Мир, 1988. – 512 с., ил.

4. Видеоуроки по робототехнике [Электронный ресурс]. – URL: http://wiki.amperka.ru.

5. Проекты и чертежи яхт, катеров и лодок [Электронный ресурс]. – URL: http://www.vodnyimir.ru/proekty-lodok-dlya-samostoyatelnoi-postroiki-8.html

УДК 004.31

Горохов Валерий Павлович
направление Информатика и вычислительная техника
(магистратура), гр. ИВТм-21
Тоцкий Алексей Андреевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Васяева Наталья Семеновна, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ МОБИЛЬНОГО РОБОТА ДЛЯ ЕЗДЫ ПО ТРАЕКТОРИИ

В сфере автоматизации промышленности встречается задача езды роботов по траектории, обозначенной чёрной или белой линией, напри-

мер, в системах автоматической погрузки. В данной работе рассматриваются основные принципы разработки алгоритмов движения роботов по траектории.

Платформа для робота. При подготовке робота для езды по линии следует использовать колёсные или гусеничные платформы.

Наиболее важным элементом в конструкции робота является расположение датчиков. Датчики на платформе условно делятся на регистраторы и маневровые. Регистраторы отвечают за определение перекрёстков, а маневровые следят за линией. В случае отсутствия регистраторов их роль берут на себя маневровые датчики. Маневровые двигатели выгоднее располагать по центру платформы. Если такой возможности нет, то маневровые двигатели располагаются спереди как можно ближе к центру. Такое расположение обеспечивает более плавное ведение линии и снижает риск съезда с неё.

Датчики линии. Датчик линии представляет собой плату, состоящую из оптопары (инфракрасный светодиод и фоторезистор) и нагрузочного резистора. Фоторезистор соединён с нагрузочным резистором, образуя делитель напряжения, который вырабатывает выходное напряжение между 0 В и VIN (обычно 5 В) в зависимости от отражённого инфракрасного сигнала. Низкое входное значение свидетельствует о большем отражении. В некоторых случаях несколько датчиков линии объединяют в одну плату. Например, модуль PololuQTR-8A состоит из восьми оптопар, каждая из которых имеет свой аналоговый выход на плате. В настоящее время различными производителями представлены разнообразные цифровые и аналоговые датчики.

У цифрового датчика в цепи фототранзистора используется разряд конденсатора, который позволяет цифровой линии ввода-вывода микроконтроллера считывать аналоговый отражённый инфракрасный сигнал путём измерения времени разряда конденсатора. Более короткое время разряда конденсатора является показателем большего отражения.

Одно из преимуществ аналоговых датчиков перед цифровыми в том, что вместо аппаратной калибровки датчика можно использовать программную. Процедура программной калибровки датчиков происходит следующим образом: во время калибровки датчик перемещается из наиболее светлой области в наиболее тёмную, в этот момент записываются максимальные и минимальные показания датчика, после чего во время работы показания датчиков преобразуются по формуле

$$ALS = \frac{(value - \min) * (S_{\max} - S_{\min})}{\max - \min} + S_{\min}.$$

Очень важно, чтобы во время калибровки каждый из калибруемых датчиков побывал как в наиболее светлой области, так и в наиболее тёмной, иначе робот может повести себя непредсказуемым образом.

Алгоритмы управления роботом. Разработка оптимального алгоритма управления является, пожалуй, основным моментом на пути создания робота, который безошибочно перемещался бы по линии при любых условиях освещенности.

Линейный алгоритм

Линейный алгоритм строится на цифровых датчиках, для него нужно минимум два датчика. Датчики должны быть расположены по краям линии. Робот должен стараться удерживать датчики на белом, если один из датчиков заехал на линию, то робот поворачивает в его сторону. Но для алгоритма на двух датчиках возникает проблема со съездом с линии, так как алгоритм не в состоянии его определить.

Проблема решается добавлением центрального датчика, который должен всегда находиться над линией. В таком случае, когда все датчики потеряли линию, считается, что это съезд, и робот начинает поворачивать в сторону датчика, который последним видел линию.

Аналоговые датчики тоже можно использовать в линейном алгоритме вместо цифровых. Для этого показания аналогового датчика преобразуются в двоичное значение с использованием пороговой функции. Данный подход позволяет значительно снизить вероятность засвета датчика, но не избавляет от него полностью. В случае если среда работы датчика сильно сместилась в светлую или тёмную сторону после калибровки, то показания могут быть ошибочны.

Линейный алгоритм можно адаптировать и под пять датчиков. При этом три центральных датчика будут отвечать за повороты линии, а крайние – за обнаружение перекрёстков. В этом случае крайние датчики следует располагать на расстоянии, превышающем две ширины линии, от центрального датчика.

ПИД-регулятор

Несмотря на то, что аналоговые датчики позволяют значительно снизить ошибку линейного алгоритма в сравнении с цифровыми датчиками, все же основная область применения аналоговых датчиков – ПИД-регуляторы.

ПИД-регулятор – это устройство в управляющем контуре с обратной связью. Он состоит из трёх составляющих: пропорциональная составляющая (текущая ошибка), интегрирующая составляющая (накопленная ошибка) и дифференцирующая составляющая (скорость изменения ошибки). Все три составляющие имеют своё влияние в регуляторе, ко-

торое выражается коэффициентом.

В алгоритме езды по линии на вход ПИД-регулятора подаются показания с аналоговых датчиков линии, а на выходе получаем скорости моторов. В зависимости от количества датчиков ошибка для пропорциональной составляющей может рассчитываться различными способами:

● для ПИД-регулятора с одним датчиком ошибка получается вычитанием из показания датчика половины от максимально значения;

● для ПИД-регулятора с двумя датчиками ошибка является разницей между показаниями датчиков;

● для ПИД-регулятора с тремя и более датчиками ошибка рассчитывается по формуле

$$error = \frac{val_0 * S_{\max} * 0 + val_1 * S_{\max} * 1 + val_2 * S_{\max} * 2 + \cdots}{val_0 + val_1 + val_2 + \cdots}.$$

Дифференцирующая составляющая представляет собой разницу между текущим состоянием ошибки и предыдущим.

Интегрирующая – сумма всех ошибок. Ошибка должна быть в пределах от **–a** до **a**, параметр «**a**» – это половина максимального значения коэффициента усиления, который может быть подан на двигатели. Обычно максимальный коэффициент равен 256, следовательно, параметр «a» принимается равным 128. Все получаемые поправочные коэффициенты должны быть приведены до этого значения.

В случае, если ошибка в интервале от **0** до **a**, нужно приводить ошибку к области от **–a/2** до **a/2.**

Алгоритмы перекрёстков

Редко встречаются соревнования, где надо просто проехать по линии. Чаще бывают соревнования типа траектория, где нужно проехать от старта до финиша по определённому маршруту, не съезжая с линии. Поля для таких соревнований обычно изобилуют перекрёстками. Отсюда возникает ещё одна задача – как определить перекрёсток. Для решения данной задачи требуется как минимум два датчика линии, так как робот с одним датчиком просто не сможет отличить заезд на линию от перекрёстка.

Наиболее популярны два подхода к решению:

1) определение перекрёстка ведётся основными датчиками;

2) для определения перекрёстков ставятся дополнительные датчики.

В первом случае за перекрёсток считаем состояние, когда два или более датчиков оказались на чёрной линии, в случае трёх и более датчиков также можно определить тип перекрёстка. Во втором случае ставятся два или три дополнительных датчика: один по центру, два по краям

чуть позади первого. Данное расположение позволяет более точно определять перекрёстки и их тип. Также это дает возможность отличить прямой или слишком острый угол от перекрёстка.

Список литературы

1. Бачинин А., Панкратов В., Накоряков В. Основы программирования микроконтроллеров. – М.: ООО «Амперка», 2013. – 207 с.
2. Васяева Е. С., Васяева Н. С. Специфика обучения школьников основам робототехники // Ресурсы робототехнических конструкций как инструмента воспитания и образования детей и юношества: сборник статей по материалам круглого стола в рамках XIX Вавиловских чтений – международной междисциплинарной научной конференции. – Йошкар-Ола: Поволжский государственный технологический университет, 2016. – С. 88-94.
3. Уэйт М., Прата С., Мартин Д. Язык СИ. Руководство для начинающих / пер. с англ. – М.: Мир, 1988. – 512 с., ил..
4. Видеоуроки по робототехнике. Робототехника [Электронный ресурс]. – URL: http://wiki.amperka.ru.
5. Классический ПИД-регулятор [Электронный ресурс]. – URL: http://www.bookasutp.ru/Chapter5_2.aspx.

УДК 681.518

Григорьева Ольга Юрьевна
направление Информатика и вычислительная техника
(магистратура), гр. ИВТм-11

Научный руководитель
Морохин Дмитрий Витальевич, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ЕДИНАЯ СИСТЕМА УПРАВЛЕНИЯ ЖИЛЫМ ПОМЕЩЕНИЕМ С ЭЛЕМЕНТАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Рассматриваются подходы к разработке и созданию единой системы управления жилым помещением с элементами искусственного интеллекта. Предполагается создание системы автоматизации/автоматики (комплекс систем автоматизации/автоматики), который облегчит повседневную жизнь людей. Функциями системы могут быть автоматическое включение/выключение света, полив цветов, закрытие дверей дома и проч. Также предполагается внедрение в функционал системы распо-

знавание лиц и анализ данных о ежедневных привычках людей для подбора оптимальных настроек функциональных узлов системы.

Выбранная тема является актуальной и относится к приоритетному направлению развития науки EnergyNet (распределенная энергетика от personal power до smart grid, smart city), определенному агентством стратегических инициатив [3]. По мере того, как быстро возрастает количество устройств и датчиков в разного рода помещениях, возникает потребность в их централизованном мониторинге и управлении. Главная идея состоит в том, что необходимо создать для решения данной проблемы единую сеть автоматизации, доступ к которой был бы как непосредственно через контрольный узел, так и удаленно с помощью мобильного телефона.

Кроме того, как правило, все современные датчики создают огромный объем данных, который можно использовать для задания оптимальной конфигурации системы управления жилым помещением. Также эти данные содержат чрезвычайно ценную информацию о том, какие из составляющих системы работают хорошо, а какие – нет. Если их не подвергать анализу, последствия могут стать весьма неприятными.

С технической точки зрения, система автоматизации дома состоит из пяти блоков:

− *Устройства, находящиеся под управлением*, например, бытовая техника. Все большее число компонентов поставляются с каким-либо встроенным интерфейсом связи, например, WLAN, которые позволяют осуществлять прямое подключение к сети управления. Другие компоненты должны быть оснащены адаптерами для того, чтобы интегрировать их в «умную» домашнюю инфраструктуру, пример такого «переходника» – PowerLine-адаптер [2].

− *Сенсоры*. Под данным термином подразумеваются датчики широкого спектра применений: от измерения температуры до датчиков движения или шума.

− *Исполнительные механизмы*. В эту категорию входят включатели/выключатели, приводы, клапаны и т.п.

− *Сеть для управления элементами*. Сеть управления обеспечивает связь между устройствами, находящимися под контролем, датчиками и исполнительными механизмами, с одной стороны, и контроллером вместе с удаленными устройствами управления, с другой стороны. Также необходимо выбрать то, как устройства будут обмениваться информацией: связь посредством ЛЭП, проводная передача либо использование варианта беспроводной передачи данных.

− *Контроллер системы*. Контроллер – ядро всего проекта, которое будет действовать как мозг системы автоматизации. Он собирает всю

информацию с датчиков и передает команды для управления какими-либо устройствами системы. Данный узел будет иметь доступ к сети Интернет.

− *Дистанционное устройство управления*: пульт дистанционного управления, смартфон или планшет [1].

На рисунке представлена примерная схема взаимодействия компонентов для подобного рода систем.

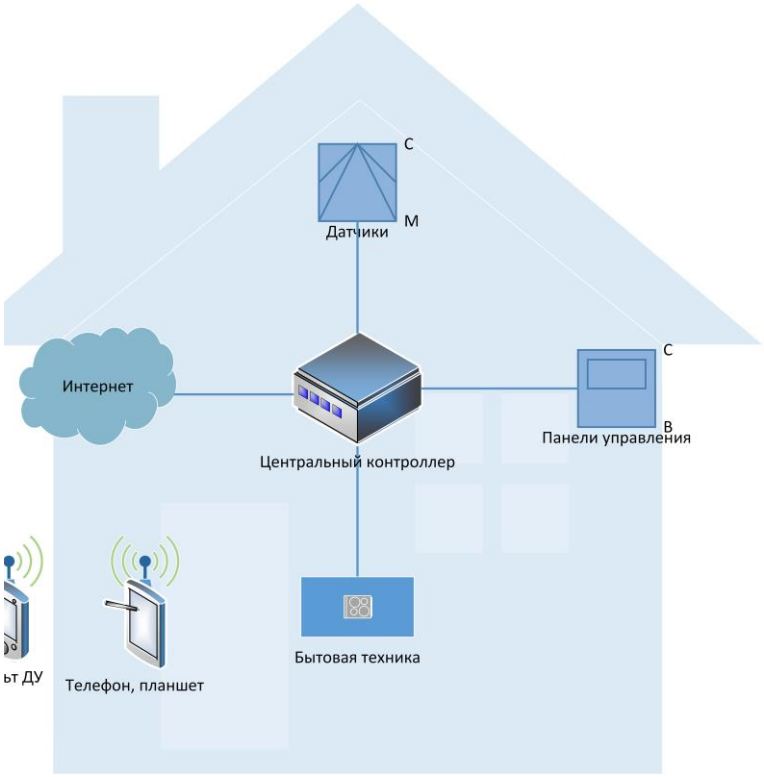


Схема управления домом

Использование элементов искусственного интеллекта в системе управления, в первую очередь, призвано осуществлять анализ данных, генерируемых всеми устройствами системы, поскольку проводить подобную работу с большими данными человеку просто не представляется возможным. Вся аналитика данной информации предполагает подбор оптимальной конфигурации и схемы работы системы управления в за-

висимости от ранее полученных сведений о предпочтениях людей в данном конкретном помещении. Для реализации данной функции в планах использование машинного обучения; самостоятельное регулирование уровня освещения, информирование, подбор музыки – перспективы его использования [5].

Резюмируя, можно сказать, что машинное обучение – это единственный способ эффективно анализировать сгенерированные данные, способный повысить скорость и точность анализа большого объема данных для того, чтобы функциональные узлы дома могли подстраиваться под режим жильцов, предугадывать их желания, понимать привычки [4].

Единая система управления жилым помещением с элементами искусственного интеллекта и будет являться результатом исследований в области разработок по автоматизации жилого помещения. Её практическое использование позволит не только вывести качество жизни людей на новый уровень путем облегчения взаимодействия человек-техника, но и поможет решить проблему доступности среды для людей с ограниченными возможностями.

Планируется, что данная система будет выборочно включать в себя функции по следующим категориям:

1) Система электропитания и освещения:

– управление уровнями освещения (с использованием алгоритмов машинного обучения).

2) Система аудио- и видеотехники Мультирум:

– автоматическое приглушение музыки при поступлении телефонного, дверного звонка;

– система интеркома (аудиосвязь различных комнат).

3) Компьютерные системы:

– управление всеми системами через Internet;

– чтение полученных электронных сообщений с любой сенсорной панели.

4) Система видеонаблюдения.

5) Система вентиляции и кондиционирования воздуха:

– управление температурой и/или влажностью в комнатах (климат-контроль);

– сбор метеоинформации внутри помещения (температура, влажность, давление).

6) Система обслуживания территории:

– орошение газона по графику;

– полив цветов в доме.

7) Система оповещения:

– голосовое оповещение в случае срабатывания датчиков;

– отражение необходимой информации на устройствах визуализации.

Список литературы

1. Каяс О. Умный дом: Шаг за шагом руководство к вашему личному Интернету вещей (4 издание). – N.Y.: Key Concept Press, 2016. – 332 с.

2. Тесля Е. В. «Умный дом» своими руками. Строим интеллектуальную цифровую систему в своей квартире. – СПб.: Питер, 2008. – 370 с.

3. Направления НТИ [Электронный ресурс]. – Режим доступа: https://asi.ru/nti/#napr. – Национальная технологическая инициатива | Агентство стратегических инициатив. – (Дата обращения: 22.09.2016).

4. Dawson F. The House That Learns: Bringing Artificial Intelligence Into The Home [Электронный ресурс]. – Режим доступа: http://www.forbes.com/sites/freddiedawson/2016/05/24/the-house-that-learns-bringing-artificial-intelligence-into-the-home/#5f68907483dc. – Forbes (дата обращения 01.10.2016).

5. Как можно использовать искусственный интеллект (ИИ) [Электронный ресурс]. – Режим доступа: http://innotechnews.com/innovations/1125-kak-mozhno-ispolzovat-iskusstvennyj-intellekt. – Innotech: новости технологий (дата обращения 22.09.2016).

УДК 378.147.88

Зарубин Константин Валентинович
направление «Информационная безопасность» (магистратура)

Научный руководитель
Пекунов Андрей Ананьевич, доцент,
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

МЕТОДЫ ВЫЯВЛЕНИЯ СЕТЕВЫХ УЗЛОВ, УЧАСТВУЮЩИХ В НЕСАНКЦИОНИРОВАННОЙ РАССЫЛКЕ СООБЩЕНИЙ ЭЛЕКТРОННОЙ ПОЧТЫ

Введение

Эффективность деятельности и уровень информационной безопасности предприятия напрямую зависит от уровня защиты данных в системе электронной почты. В связи с этим появляется необходимость создания надежной защиты.

Ввиду недостаточной защиты почтовых систем пользователи электронной почты сталкиваются с множеством проблем (спам, вирусы).

Как показывает практика, одномоментное решение проблемы защиты электронной почты невозможно. Для того чтобы защита электронной почты была на достаточном уровне, а достижение этого уровня не требовало больших затрат, необходим и комплексный подход к решению данной проблемы.

Для предложения метода обеспечения информационной безопасности предприятия необходимо провести анализ способов выявления сетевых узлов, участвующих в несанкционированной рассылке сообщений электронной почты.

Многие отечественные и зарубежные авторы рассматривали в своих работах проблемы выявления сетевых узлов, участвующих в несанкционированной рассылке сообщений электронной почты: А. В. Лукацкий, А. Баутов, С. Симонов, А. Кононов, Д. Ловцов, А. Васильев, А. Волоткин, М. Давлетханов, И. Конев, А. Беляев, А. Маношкин, В. Мельников, В. Трайнев, С. Петренко, А. Садердинов, Ю. Уфимцев, В. Шпак, Р. Уитти, А. М. Уилхайт, С. Норткатт, Ж. Брассар и др.

Исследователи выявляют лишь отдельные аспекты проблем информационной безопасности, в связи с чем необходим комплексный подход к применению усовершенствованных методов.

Для применения комплексного подхода обеспечения информационной безопасности предприятия необходимо решить следующие задачи:

- исследовать способы выявления сетевых узлов, участвующих в несанкционированной рассылке сообщений;
- систематизировать информационные риски в несанкционированной рассылке сообщений электронной почты;
- разработать методы оценки к управлению несанкционированной рассылкой сообщений электронной почты;
- разработать алгоритм оценки остаточных информационных рисков участвующих в несанкционированной рассылке сообщений электронной почты на предприятии;
- разработать методы обеспечения информационной безопасности в несанкционированной рассылке сообщений электронной почты предприятия.

1. Разбор служебных заголовков

Спецификация протокола SMTP обязывает каждого почтового транспортного агента (MTA), через которого проходит сообщение, добавлять к сообщению свой заголовок «Received», в заголовке «Received» обычно указывается, от кого и кем было получено почтовое сообщение.

Электронное почтовое сообщение в процессе пересылки может проходить через некоторое количество промежуточных почтовых систем, так что наличие в электронном почтовом сообщении нескольких заголовков «Received» означает, что сообщение проходило через несколько почтовых серверов, но это также может означать, что некоторая часть заголовков фиктивна.

Задачи поиска сетевого узла, которым было первоначально сформировано электронное сообщение (определения источника несанкционированной рассылки), решает анализ последовательности заголовков «Received» почтовых сообщений. Ввиду того, что только в заголовке «Received» содержатся данные о сетевых узлах, участвующих в передаче электронного сообщения, – разбор служебных заголовков электронного почтового сообщения является единственным способом определения источника рассылки.

В ходе проведения анализа предполагается, что заголовок, сформированный на последнем (в соответствии с маршрутом следования почтового сообщения) почтовом сервере, является истинным, так как его сгенерировал доверенный почтовый сервер.

Для описания решения задачи анализа последовательности заголовков «Received», с целью поиска фиктивных заголовков, используются методы теории конечных автоматов.

2. Условия, которые указывают на присутствие фиктивных заголовков

В процессе анализа заголовков электронных почтовых сообщений различных категорий (обычные почтовые сообщения, рассылка вредоносных программ, спам и т.д.) были введены условия, проверка которых позволит определить, истинный или поддельный заголовок «Received». Этими условиями являются:

- соответствие заголовка формату (формат заголовков «Received» должен удовлетворять требованиям протокола – RFC 2821 и RFC 2822);
- для доменного имени, указанного в заголовке в качестве MTA, должна быть соответствующая запись «MX» или «A»;
- доменное имя, указанное в заголовке в качестве MTA, должно быть не выше третьего уровня;
- связность заголовков «Received»;
- связность полей by и from заголовка «Received»;
- проверка доступности из сети Интернет почтовой службы (TCP/25, TCP/110, TCP/143, TCP/465) на сервере, указанном в качестве MTA.

3. Математическая модель выявления фальсифицированных служебных заголовков почтового сообщения

Иногда невозможно однозначно определить источник рассылки, для этого был введен следующий параметр - N, который зависит от значений параметров из множества $Y = \{R,C_R,C_{Jb},D_{MX},D_A,L,S\}$. Этот параметр характеризует степень достоверности указанных в заголовке служебных данных. Любому набору параметров из множества Y ставится в соответствие натуральное число. Чем больше значение этого параметра, тем больше достоверность указанных в заголовке данных.

Множество всех возможных наборов параметров из множества Y определим как - W. Число его элементов, т.е. мощность множеств $|W| = 2^{|Q|}$, где $|Y|$ – мощность множества Y. Для $Y = \{R,C_R,C_{Jb},D_{MX},D_A,L,S\}$, мощность $|W| = 2^7 = 128$. Если исходить из того, что без выполнения условия $R = 1$, $C_R = 1$ определение источника рассылки является практически невозможным (случаи, когда $R = 0$ или $C_R = 0$, принимаются за один случай), на практике мы имеем $|W| = 2^5 + 1 = 33$.

Степень достоверности данных, указанных в заголовке N, может принимать натуральные значения, лежащие в диапазоне [0…33].

Если $N = 0$, то это соответствует крайней степени недоверия к данным, находящимся в заголовке, и показывает, что данный заголовок поддельный.

Для того чтобы задать значения параметра N для каждого из наборов $w_i \in W$, необходимо упорядочить наборы входящих в них параметров по степени влияния на достоверность данных, которые указаны в заголовке.

После упорядочивания необходимо пронумеровать наборы. Номера наборов будут использоваться в качестве значения параметра N.

4. Алгоритм определения источника несанкционированной рассылки

Для того чтобы упростить процедуру определения начальной точки формирования почтового сообщения, которая сводится к анализу служебных почтовых заголовков, необходимо провести подготовительные операции. Очистка служебных заголовков – первая процедура определения начальной точки формирования почтового сообщения.

Алгоритм очистки служебных заголовков необходимо разбить на ряд этапов. Далее будет рассмотрен вариант предварительной очистки заголовков почтового сообщения.

1. Удаление всех заголовков, кроме «Received».

Другие заголовки можно не рассматривать, т.к. в первую очередь нас интересует вопрос нахождения IP-адреса источника почтовой рассылки, которым было первоначально сформировано сообщение.

2. Удаление заголовков «Received», в которых нет ключевого слова «from» с указанным IP-адресом отправителя.

3. Удаление заголовков «Received», в поле «from» которых указывается немаршрутизируемый в Интернет IP-адрес.

Как правило, немаршрутизируемые в Интернет IP-адреса в поле «from» заголовка «Received» появляются в двух случаях:

- электронное письмо было сформировано в локальной вычислительной сети некоторой организации;

- при прохождении электронного почтового сообщения через почтовую систему (с несколькими почтовыми серверами) некоторые сервера (в данной почтовой системе) имели адреса локальной сети.

Произвести проверку почтовых заголовков «Received» на соответствие формату, описанному в стандартах RFC 2821, RFC 2822.

Проверка почтовых заголовков на соответствие стандартам позволяет отсечь заведомо фиктивные (фальсифицированные) почтовые заголовки.

Очередной задачей является разбор цепочки заголовков «Received», полученной на предварительном этапе (этапе очистки заголовков электронного почтового сообщения) с целью определения источника несанкционированной рассылки или узла, наиболее близкого (по заголовкам) к нему, с учётом возможного наличия ложных заголовков «Received».

Самым главным требованием для решения этой задачи является то, что решением не должен оказаться узел, не принимавший участия в несанкционированной рассылке (т.е. подставной узел).

Для того чтобы оценить долю электронных почтовых сообщений, требующих дополнительной проверки наличия ложных заголовков «Received», необходимо проанализировать заголовки электронных почтовых сообщений двух категорий: «спама» и сообщений, содержащих вирусы.

Как показало исследование механизмов, используемых для сокрытия источника рассылки, определение ложных заголовков «Received» путем формального анализа заголовков и их связи может оказаться неэффективным, так как имеется возможность соблюсти все формальные условия формирования заголовков, а также их зависимости.

Чтобы определить узел, который участвует в несанкционированной рассылке электронных почтовых сообщений и наиболее «близок» к ис-

точнику рассылки (или сам является источником) необходимо использовать следующие правила:

Первый заголовок «Received» (который добавляется почтовой системой на стороне получателя) является истинным, и IP-адрес, который указан в поле «from» этого заголовка, есть решение по умолчанию – IP ($from_i$).

Когда в сообщении присутствует больше одного заголовка, то их список просматривается до конца или до появления первого фиктивного заголовка. IP-адрес, указанный в поле «from» последнего не фиктивного заголовка, становится решением – IP ($from_i$), где i – номер последнего, не фиктивного заголовка.

Заключение

В данной статье был предложен способ выявления сетевых узлов, которые участвуют в распространении вредоносного программного обеспечения и «спама» с помощью протокола SMTP.

Также была разработана математическая модель выявления фиктивных служебных заголовков электронного почтового сообщения.

Численное значение степени достоверности заголовка зависит от того, какие из имеющихся условий присутствия фиктивных заголовков выполнены.

Был предложен алгоритм определения параметра «показатель корреляции заголовков», который используется в математической модели выявления фиктивных служебных заголовков.

Для определения сетевых узлов, участвующих в распространении вредоносного программного обеспечения и спама, предложен метод анализа заголовка почтового сообщения, с учётом возможного присутствия в нём фальсифицированных (фиктивных) данных.

Метод заключается в последовательном анализе цепочки служебных заголовков почтового сообщения. Истинность или фиктивность каждого заголовка устанавливается в соответствии с математической моделью выявления фальсифицированных служебных заголовков.

Список литературы

1. Рудик К. П. Определение заражённых вредоносными программами сетевых узлов путём анализа заголовков распространяемых ими электронных почтовых сообщений, содержащих инфицированные вложения // Методы и технические средства обеспечения безопасности информации: сборник научных трудов XIV общероссийской научно-технической конференции. – СПб.: СПбГПУ 2005. – С. 99.

2. Рудик К. П. Построение активной сетевой защиты // Проблемы информационной безопасности в системе высшей школы: сборник научных трудов XI Всероссийской научно-технической конференции. – М., 2004. – С. 130-131.

3. Рудик К. П. Выявление источников рассылки вредоносного программного обеспечения при использовании протокола SMTP // Проблемы информационной безопасности в системе высшей школы: сборник научных трудов XIII Всероссийской научно-технической конференции. – М., 2006. – С. 98-99.

4. Рудик К. П. Исследование способов выявления сетевых узлов, участвующих в несанкционированной рассылке сообщений электронной почты // Методы и технические средства обеспечения безопасности информации: сборник научных трудов XVII Общероссийской научно-технической конференции. – СПб.: СПбГПУ, 2008.

УДК 004.75

Иванов Константин Владимирович
кафедра информационно-вычислительных систем (аспирантура)

Научный руководитель
Васяева Наталья Семеновна, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

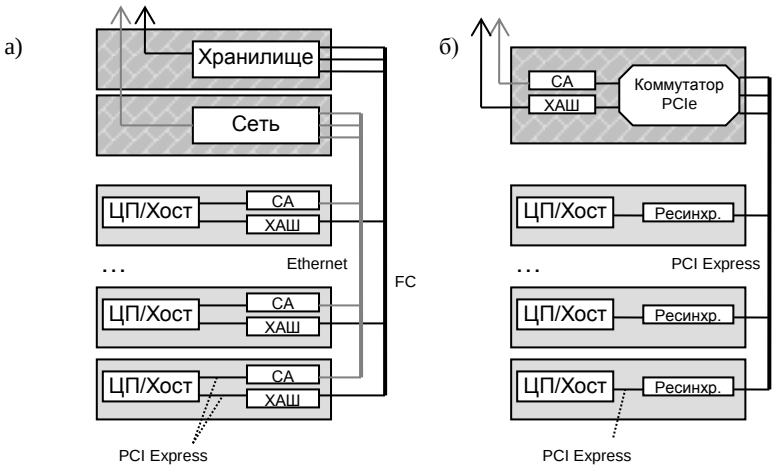
ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ PCI EXPRESS ДЛЯ ПОСТРОЕНИЯ КЛАСТЕРНЫХ СИСТЕМ

В настоящее время круг задач, требующих для своего решения применения мощных вычислительных ресурсов, постоянно расширяется. Вследствие широкого распространения вычислительной техники, значительно усилилась роль моделирования и численного эксперимента в организации научных исследований, в частности, в решении прикладных задач физики, химии, геологии и других естественных наук. Суперкомпьютеры, предназначенные для решения подобных задач, часто являются кластерными системами, поскольку они легко масштабируются и обладают высокой производительностью.

На производительность кластерной вычислительной системы влияет не только производительность процессорных элементов отдельных узлов, но и характеристики каналов связи между узлами (такие, как пропускная способность и вносимые задержки). Причем, в зависимости от решаемых кластером задач, отсутствие задержек может быть предпочтительнее высокой скорости передачи. Поэтому актуальной задачей является поиск эффективных методов улучшения данных характеристик.

Традиционная для кластеров система ввода/вывода, изображенная на рисунке (а), использует технологию Ethernet для связи между узлами и Fibre Channel для взаимодействия с хранилищем данных. Подобная архитектура имеет ряд недостатков: хост-адаптеры шины (ХАШ) Fibre Channel и сетевые адаптеры (СА) используются недостаточно интенсивно, при этом имеют большую стоимость и потребляют до 5-8 ватт каждый. Что касается задержек при передаче, сам факт наличия в системе нескольких технологий межсоединения говорит о том, что время передачи порции данных будет больше из-за необходимости преобразования сообщения из одного формата в другой и обратно.

Анализ источников [1, 2] показал, что решить данные проблемы можно при помощи использования технологии PCI Express для внешних соединений. Система PCI Express включает в себя коммутатор и представляет собой сеть с соединениями «точка-точка». На рисунке (б) видно, что можно построить систему с меньшим количеством сетевых адаптеров и хост-адаптеров шины. При этом они будут использоваться более интенсивно, так как множество узлов будут иметь общий доступ к ним. При необходимости в узлах устанавливаются ресинхронизаторы PCI Express, которые дешевле сетевых адаптеров и хост-адаптеров, а также имеют потребление электроэнергии около 1 ватта.



Организация системы ввода/вывода: а) традиционная; б) на основе PCI Express

Многие процессоры и материнские платы изначально имеют поддержку PCI Express, поэтому при обмене данными между близкими уз-

лами сообщения преобразовываться не будут, что сокращает задержку при передаче. Аппаратная поддержка QoS в PCI Express также помогает сократить задержки. Скорость передачи при использовании кабеля может достигать 40 Гбит/с в одном направлении (для кабеля с 16 линиями), что выгодно выделяет PCI Express по сравнению с технологией Ethernet. При этом нужно иметь в виду, что стандарт PCI Express развивается и в будущем вполне можно ожидать увеличения скорости передачи.

Среди прочих достоинств использования технологии PCI Express в кластерных системах можно отметить сравнительную простоту программирования подобных систем. Дело в том, что при использовании внешнего коммутатора PCI Express с поддержкой трансляции адресов каждый узел, соединенный с коммутатором, имеет доступ к памяти других подобных узлов. Таким образом, получается, что узлы системы имеют общую память.

В силу некоторых причин, таких как, в частности, жёсткие ограничения на длину кабельных соединений, технология PCI Express пока не завоевала большой популярности в сфере кластерных систем и сетей хранения данных. Тем не менее, системы с применением внешнего коммутатора PCI Express существуют. К ним можно отнести решение для сетей хранения данных ExaSAN фирмы Maxtronic International, а также отечественную коммуникационную систему «МВС Экспресс», на основе которой построен и функционирует одноименный вычислительный кластер.

Исходя из вышесказанного, можно сделать вывод, что технология PCI Express имеет перспективы в области кластерных вычислительных систем. Модификация таких подсистем PCI Express, как арбитр коммутатора, с целью ускорения обработки пакетов может привести к дальнейшему уменьшению задержек при передаче [3], а следовательно, и к улучшению производительности кластерных систем.

Список литературы

1. Mallampati K. PCI Express vs. Ethernet – selecting the superior technology for real-time, embedded systems // RTC Magazine. – 2014. – Vol. 15, № 12. – P. 28-31.

2. PCI Express Base 3.0 Specification [Электронный ресурс]. – URL: http://www.pcisig.com/specifications/pciexpress/base3/

3. Иванов К. В., Кошпаев А. А., Васяева Н. С. Программная модель системы арбитража коммутатора PCI Express // Кибернетика и программирование. – 2014. – № 4. – С. 66-75. – URL: http://e-notabene.ru/kp/article_12758.html.

УДК 004.056

Имшенецкий Александр Иванович
направление Информационная безопасность (магистратура), гр. БИм-21

Научный руководитель
Кречетов Александр Александрович, канд. техн. наук, доцент,
кафедра Информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИССЛЕДОВАНИЕ И АНАЛИЗ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ, ИСПОЛЬЗУЮЩИХ ИНТЕЛЛЕКТУАЛЬНЫЕ ТЕХНОЛОГИИ (НЕЙРОННЫЕ СЕТИ)

Эффективность функционирования современных информационных систем напрямую связана с проблемой защиты обрабатываемой в них информации. Сложность процессов обработки информации, сопровождающая современные системы, приводит к появлению большого количества ошибок в программном коде информационной системы. Эти ошибки способствуют появлению уязвимостей в программном коде и, как следствие, разнообразных атак, другими словами – способов получения несанкционированного доступа к ресурсам информационной системы.

Анализ современных систем защиты информации показывает, что их возможности не позволяют обеспечить безопасность информационной системы на достойном уровне. Причиной этого является то, что процесс создания систем обнаружения атак сопряжен с рядом нерешенных научно-технических задач. Существующие системы обнаружения вторжений используют простейшие алгоритмы обработки поступающей информации, что не позволяет обнаружить значительное количество атак на информационные системы.

Система обнаружения вторжений – это программная или аппаратная система, которая автоматически просматривает события, возникающие в компьютерных системах или сетях, анализируют их и делает заключение о безопасности. Английский термин – Intrusion Detection System (IDS). Для краткости будем называть эту систему СОВ [1].

На данный момент времени распространенными методами обнаружения атак приняты:

- сигнатурный анализ – надежный метод выявления уже известных и классифицированных атак, но этот метод не способен обнаружить новые способы нападений;

- метод, обнаруживающий аномалии, которые позволяют выявить новые варианты атак, но он имеет низкую надежность по причине высокого процента ложных срабатываний.

В большинстве случаев СОВ представляет собой специализированное программно-аппаратное обеспечение с типовой архитектурой, включающей в себя следующие компоненты:

- сенсорная подсистема – модули-датчики для сбора событий из сетевого трафика;

- подсистема анализа и выявления атак – обрабатывающая собранные датчиками данные с целью обнаружения угроз;

- подсистема хранения информации об обнаруженных атаках, а также конфигурационной информации, как правило это стандартная СУБД;

- подсистема управления компонентами СОВ (консоль управления), предназначенная для ее конфигурирования, просмотра выявленных атак, наблюдения за защищаемой системой и самой СОВ, а также может выступать подсистемой реагирования на обнаруженные угрозы (в данном случае решение принимает администратор).

Системы, основанные на эвристическом и статистическом анализе, широкого распространения не получили по причине недостатков, присущих этим методам (множественные ложные срабатывания).

Лидирующее место среди методов, используемых СОВ, выступают: экспертные системы (ЭС), нейронные сети и комбинация этих методов.

ЭС решает, к какому классу угроз отнести произошедшее событие, решает на основе базы знаний, хранящейся в БД. База знаний – основной набор правил, существующий для работы системы, который необходимо регулярно обновлять. Атаки «первого дня» – совершенно новый вид угроз, нейросетевая модель позволяет их обнаружить, что повышает уровень защищённости всей системы от неопределенных источников и является главным преимуществом этой модели [4].

Применение экспертных систем подразумевает решение сложных для человека задач, эффективность и качество которых может принять только эксперт. Характерные черты таких задач:

- невозможность решить задачи в числовой форме;

- невозможность выразить цели точно определенной целевой функцией;

- невозможность решить задачи алгоритмически;

- невозможность решить задачу, если есть такое решение, по причине ограниченности ресурсов.

Нейронная сеть искусственного происхождения – это система взаимосвязанных друг с другом элементарных процессоров, которые назы-

вают искусственными нейронами. Каждый процессор этой сети, контактирует только с сигналами, которые получает от сенсоров, или другими процессорами и передаваемыми сигналами.

Постоянно увеличивающееся число Интернет-трафика и большая волатильность характера сетевых атак сильно влияют на сложность построения системы защиты, представляющую собой комбинацию высокой пропускной способности, эффективности обнаружения системой возможных (как известных, так и новых) атак и гибкую настройку СОВ, не допускающую ложных срабатываний. Одним из решений поставленной задачи могут быть СОВ, в основе которой лежит метод искусственных нейронных сетей, освобожденная от жесткого структурирования, характерного для систем, в основе которых лежат правила.

Преимуществом нейронных сетей является способность анализа неполной информации или информации, искаженной различными помехами. Еще одно серьезное отличие – нелинейный анализ состоявшихся событий. Данные свойства не заменимы в реальной сети, где информация искажается как умышленно, так и естественными причинами. Также вторжение может осуществляться из большого числа источников. Именно в этом случае центральная роль системы – это нелинейная обработка множества потоков данных.

Скорость реакции СОВ на вторжение – одна из важнейших характеристик, любое промедление нанесет неисправимый ущерб информационной системе государственных органов или предприятия. Системы обнаружения вторжений, основанные на нейросетевых технологиях, впечатляют скоростными показателями детектирования чужеродных воздействий и принятия защитных мер, что значительно минимизирует возможный ущерб.

Следующее особое качество нейронных сетей – способность к прогнозированию будущих событий и угроз, она основана на результатах, сделанных накануне анализов, а ими являются вероятности. В процессе самостоятельного обучения СОВ увеличивает опыт, оптимизирует способности по обнаружению закономерностей отдельных событий, их последовательности, различными связками, позволяющими как вариант в более короткие сроки локализовать атаку или предпринять упреждающие защитные меры и таким образом отразить атаку без причинения вреда.

«Самообучение», свойственное искусственным нейронным сетям, является основной способностью для анализирующего аппаратно-программного комплекса СОВ. Эта способность позволяет классифицировать изначально заданные события – списка, по которому происходи-

ло «обучение» системы, и «изученных» системой сигнатур вероятных угроз в процессе функционирования, а также новых вторжений, которых система не знает и которые не совпадают с произошедшими в прошлом инцидентами. Чтобы уменьшить количество ложных срабатываний, оповещение о возможной атаке будет происходить после превышения порога вероятности или момента, когда угроза будет воспринята как потенциально значимая [3].

Все преимущества искусственных нейронных сетей в системах обнаружения вторжений остаются не у дел при реализации аппаратно-программных комплексов из-за ряда присущих им недостатков, таких как:

- большая стоимость проектирования и программно-технической реализации, наладки, эксплуатации и ремонта интеллектуальных технологий;
- трудоемкость первичного «обучения» системы, а это ключевое действие, напрямую влияющее на качество работы в будущем.

Громадные объемы данных, необходимых для «обучения», – миллионы последовательностей атак, на данный момент это – практически труднодостижимые величины.

Недостатком, который стоит во главе угла эксплуатации нейронных сетей не только в системах обнаружения и предотвращения вторжений, но и в интеллектуальных технологиях как перспективной области, является неопределенный результат, который выдает «обученная» система. Точнее, когда достигается пороговый уровень успеха классификации накопленных в БД событий, точность обнаружения превращается в величину, не всегда известную. Озвученная проблема является первостепенной областью в исследовании теории искусственных нейронных сетей.

На данный момент реализовано два вида СОВ, в основе которых лежат искусственные нейронные сети. Первый – сочетание экспертной системы и нейросетевого метода. Система двухступенчатого анализа. Через нейронную сеть проходит весь сетевой трафик, при детектировании вероятной угрозы, информация передаётся для анализа в экспертную систему, которая в свою очередь принимает финальное решение. Ценность данного воплощения заключается в увеличении чувствительности ЭС, получающей информацию только о событиях, расцененных на данный момент как вероятные угрозы. Но необходимость постоянного обновления базы знаний экспертной системы является ее недостатком. Если этого не делать, то все новые виды атак, обнаруженные нейронными сетями, не будут распознаны экспертной системой как вторжения [2].

Следующий вид реализации СОВ осуществлен на основе нейронных сетей как автономной системы. Если сравнивать с вышесказанным, то данная реализация имеет более высокую скорость реакции по причине наличия всего одной ступени анализа. И эта реализация делает возможным для нейросети исчерпывающе воспользоваться потенциалом «самообучения» и выйти далеко за пределы базы знаний экспертной системы. Следующим достоинством является отсутствие необходимости регулярно обновлять базы знаний, как это делается в системах, основанных на правилах.

Нужно отметить, что интеллектуальные технологии расширяют диапазон возможностей стандартной системы обнаружения вторжений и являются актуальным, востребованным, развивающимся направлением в защите информации, требующим новых решений в обозначенных выше проблемах.

Выводы

Проведенное исследование показало, что применение интеллектуальных технологий в СОВ позволяет:

- предоставить высокий уровень защищенности информационной системы;
- уменьшить время реакции системы на угрозы, а это значит минимизировать наносимый системе вред или принять меры, полностью блокирующие вторжение;
- увеличить объемы анализируемого трафика;
- противодействие многочисленным атакам одновременно.

В данной статье была отражена проблема актуальности использования интеллектуальных технологий в системах обнаружения вторжений, их уникальные возможности, преимущества и недостатки методов перед традиционными способами выявления угроз данных систем.

Список литературы

1. Kohlenberg Toby (Ed.), Alder, Raven, Carter, Dr. Everett F. (Skip), Jr., Foster, James C., Jonkman Marty, Raffael, and Poor, Mike, Snort IDS and IPS Toolkit, Syngress, 2010. – 768 с.
2. Джарратано Дж., Райли Г. Экспертные системы. Принципы разработки и программирование. – М.: Издательский дом «Вильямс», 2007. – 1152 с.
3. Москаленко Ю. С. Организация систем, основанных на знаниях. – Владивосток: Изд. дом Дальневосточного федерального университета, 2013. – 242 с.
4. Ясницкий Л. Н. Введение в искусственный интеллект. – М.: Издательский центр «Академия», 2005. – 176 с.

УДК 612.822

Исаев Владимир Юрьевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Глозштейн Александр Моисеевич, ст. преподаватель,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СИСТЕМА АНАЛИЗА ТОПОГРАФИИ ВИСОЧНО-НИЖНЕЧЕЛЮСТНОГО СУСТАВА

В настоящее время большую роль в развитии медицины оказывают информационные технологии. С каждым днем совершенствуется медицинская техника, появляются новые технологии, которые помогают определить врачам болезни на ранних стадиях, оказывают большую помощь в определении диагноза по тем или иным критериям, а также упрощают или вовсе автоматизируют процессы, которые ранее приходилось делать вручную.

В работе была поставлена задача создать многопользовательское Web-приложение, определяющее по алгоритму особенности строения ВНЧС (височно-нижнечелюстного сустава) в зависимости от вида прикуса и изменения ВНЧС при концевых и включенных дефектах зубных рядов в боковом отделе. Приложение показывает специалисту изменение топографии (взаимоотношения элементов) сустава в зависимости от потери зубов и вида прикуса.

Для выполнения данной работы была использована одна HTML-страница с разметкой для каждого окна, необходимые CSS-стили для управления дизайном и адаптацией приложения под разные виды устройств, а также код самой программы на языке JavaScript с применением фреймворка jQuery и плагина LightBox.js. В файле JavaScriptбыл реализован алгоритм для каждого вида прикуса, а также была настроена логика работы программы, в том числе переход между окнами и озвучивание нажатия на кнопки. jQuery был выбран с целью упростить и ускорить разработку приложения. Плагин LightBox.js использован для увеличения графических изображений.

При запуске приложения появляется окно с приветствием и предложением начать работу.

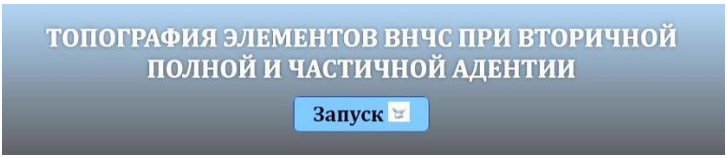


Рис. 1. Стартовая страница приложения

По клику на кнопку «Запуск» специалист выбирает прикус пациента. На данный момент реализовано 6 видов прикуса: ортогнатический, глубокий, открытый, дистальный, перекрестный и мезиальный.

Рис. 2. Выбор вида прикуса

Подразумевается, что специалист самостоятельно определяет тип прикуса и выбирает необходимый нажатием на кнопку.

Следующим шагом является выбор отсутствующих зубов.

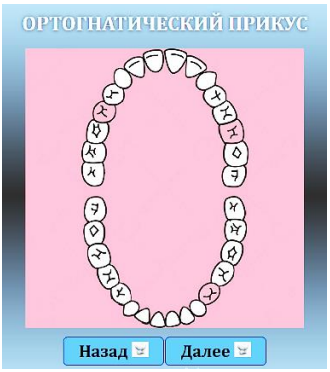


Рис. 3. Выбор отсутствующих зубов

Специалист также визуально определяет количество и позицию отсутствующих зубов и выбирает их нажатием на эти зубы и нажимает кнопку «Далее».

Программа по алгоритму определяет тип смещения и выдает результат, соответственно открывая необходимое окно. По нажатию кнопки «Далее» можно просмотреть тип смещения, прочесть некоторую информацию о данном типе и увидеть, как выглядит соотношение челюстей при таком виде прикуса и смещении с 3 сторон (справа, анфас, слева).

Рис. 4. Соотношение челюстей

После этого специалисту также предлагается просмотреть следующее окно, где показана топография элементов ВНЧС с присутствующими отклонениями.

Рис. 5. Топография элементов ВНЧС

В данном окне специалист может переключить вид с левого ВНЧС на правый ВНЧС и просмотреть, в какую сторону и на сколько сдвинулись элементы височно-нижнечелюстного сустава.

На основе полученных данных от специалиста программа анализирует состояние ВНЧС и показывает данные для дальнейшего анализа. Таким образом, данное приложение упрощает работу стоматолога и сохраняет его драгоценное время.

Список литературы

1. Височно-нижнечелюстной сустав: его болезни и их предпосылки [Электронный ресурс]. – URL: http://bolit-sustav.ru/bolezni/visochno-nizhnechelyustnoj-sustav-ego-bolezni-i-ih-predposylki/

2. Особенности обследования височно-нижнечелюстного сустава [Электронный ресурс]. – URL: http://tvoisustavy.ru/osobennosti-obsledovaniya-visochno-nizhnechelyustnogo-sustava.html

УДК 004.62::519.71

Козлова Ксения Алексеевна
направление Информационная безопасность автоматизированных систем (специалитет), гр. БИС-31

Научный руководитель
Бородин Андрей Викторович, канд. экон. наук, профессор,
кафедра информатики и системного программирования
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ПУЛ ПЕРЕМЕННЫХ ПРОГРАММЫ КАК ОБЪЕКТ-ХРАНИЛИЩЕ С РАНДОМИЗАЦИЕЙ КАРТЫ ПАМЯТИ

Под пулом переменных программы будем понимать совокупность соотнесений идентификаторов структур данных программы с областями виртуальной и/или физической памяти вычислительной системы. В этом смысле отслеживание изменения состояния пула данных – ключевой фактор в процессе рефакторинга программы. Не последнее место такое отслеживание играет и в задачах идентификации конкретных исходных данных программы по образцу последовательности состояний пула. Также идентификация исходных данных в определенных ситуациях возможна по образцу временных диаграмм адресных

шин, а также по профилю радиоизлучения контроллера памяти. Все эти примеры можно рассматривать как случаи утечки информации по побочным каналам.

Бороться с такого рода утечками можно различными методами: от организационных, когда, например, критические вычисления реализуются случайным образом на фоне «мусорных», до технических, использующих аппаратно-программные методы контроля доступа к памяти или к адресным шинам контроллера и/или применяющих методы зашумления радиоканала. Важно отметить, что, несмотря на эффективность указанных подходов, возможности их применения ограничены, а экономическая эффективность этих мер может оказаться очень низкой.

Возможным подходом к решению описанной здесь проблемы может стать путь возложения мер противодействия к утечкам по побочным каналам на саму программу, в частности за счет рандомизации обращений к оперативной памяти. Структура данных с некоторым идентификатором может как бы «гулять» по адресному пространству сегмента данных, причем перемещение структуры в оперативной памяти удобно совместить с операцией присваивания ей нового значения. Перемещение структуры может происходить по некоторому псевдослучайному закону с рандомизацией начального значения датчика псевдослучайных чисел (ДПСЧ) от младших бит часов реального времени вычислительной системы. Операцию сохранения данных при этом можно совместить с их зашифровыванием на базе гаммирования с тут же выработанным псевдослучайным ключом, а операцию считывания – с соответствующей процедурой расшифровки. Описанный подход, по сути, является методом обфускации пула переменных программы, особенно эффективным в части противодействия активным (динамическим) методам исследования программ. Подход можно считать творческим развитием идей, изложенных в работах [1-4].

Реализацию предложенного метода обфускации пула переменных для императивных языков программирования высокого уровня удобно осуществить в рамках объектно-ориентированной парадигмы, рассматривая пул переменных как один или несколько объектов. Каждая структура данных программы при этом является свойством объекта. Конструктор объекта резервирует память под структуры данных программы с коэффициентом запаса по объему, достаточным для организации их перемещения, осуществляет инициализацию ДПСЧ, первичное размещение структур данных и инициализацию памяти под ними (с зашифровыванием, если функция шифрования данных включена). Метод, свя-

занный со считыванием свойства, при необходимости расшифровывает данные. Метод, связанный с присвоением значения свойству, выбирает новый адрес размещения структуры, сохраняет его, зашифровывает данные при необходимости и размещает их по новому адресу. Деструктор объекта освобождает память, выделенную в конструкторе для размещения структур данных. Идеальный случай – размещение всех структур данных в одном объекте, так как этот случай реализует максимальную степень рандомизации по адресам. Предложенный метод обфускации не более чем линейно увеличивает требования программы к памяти и ресурсам процессора, что подпадает под традиционное понимание обфускации [1, 4].

В настоящее время предложенный подход проходит апробацию в составе программного комплекса автоматизированной обфускации программ, написанных на языке программирования VBA. В частности он использован при обфускации отдельных модулей пакета прикладных программ «МультиМИР» [5, 6].

Список литературы

1. Бородин А. В. Линейные конгруэнтные последовательности максимального периода в задачах обфускации программ // Кибернетика и программирование. – 2016. – № 6. – С. 1-19. – DOI: 10.7256/2306-4196.2016.6.18499.

2. Бородин А. В., Долгушев Е. Д. Обфускация пула констант как задача построения минимальной системы целочисленных линейных комбинаций // Образование, наука, бизнес: развитие и перспективы: материалы III международной научно-практической конференции (6 мая 2016 г.). – Саратов: Издательство ЦПМ «Академия Бизнеса», 2016. – С. 7-13.

3. Бородин А. В., Долгушев Е. Д. Постановка задачи обфускации пула констант // Новое слово в науке: перспективы развития: материалы IX Международной научно–практической конференции (Чебоксары, 7 августа 2016 г.). – Чебоксары: ЦНС «Интерактив плюс», 2016. – № 3(9). – С. 89-93. – DOI: 10.21661/r-112829.

4. Перспективные тренды развития науки: техника и технологии. Т. 1 / И. Я. Львович, В. А. Некрасов, А. П. Преображенский и др. – Одесса: КУПРИЕНКО СВ, 2016. – 197 с.

5. Уразаева Т. А. Пакет прикладных программ «МультиМИР»: архитектура и применение // NB: Кибернетика и программирование. – 2014. – № 5. – С. 34–61. – DOI: 10.7256/2306–4196.2014.5.12962.

6. Уразаева Т. А. Функциональность и приложения пакета прикладных программ «МультиМИР» // IX Международная научно-практическая конференция «Инновационное развитие российской экономики»: Т. 3: Информационно-коммуникационные технологии. – М.: ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2016. – С. 79-83.

УДК 004.65

Кошпаев Андрей Алексеевич
направление Вычислительные машины, комплексы и компьютерные сети
(аспирантура)

Научный руководитель
Васяева Елена Семеновна, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

АНАЛИЗ ПРОТОКОЛОВ КОГЕРЕНТНОСТИ ПАМЯТИ И ИХ ПРИМЕНИМОСТЬ В СИСТЕМАХ ХРАНЕНИЯ ДАННЫХ

Кэширование – неотъемлемая часть любых эффективных систем, поскольку она позволяет увеличить пропускную способность и уменьшить время доступа. В типичных реализациях подсистема внешней памяти СХД соединяется с вышестоящими уровнями системы через коммутационную матрицу. В СХД каждый узел имеет симметричный доступ к подсистеме внешней памяти. Следовательно, он может получить доступ и изменить ресурс в файловой системе в любое время. В определенных СХД, после открытия ресурса, узел считывает данные в собственный локальный кэш и полагается на кэшированную копию данных для выполнения операций. Когда ресурс одновременно открыт несколькими узлами в режиме записи, где множество узлов могут изменять данные, то должна быть обеспечена когерентность данных [2].

В настоящей работе рассматривается задача определения оптимального варианта обеспечения когерентности данных в СХД. Областью исследования являются системы хранения данных, предмет исследования – алгоритмы и методы, обеспечивающие когерентность данных. Критерием оптимальности выбора тех или иных алгоритмов и методов служит достижение большей производительности СХД при наименьших аппаратных затратах.

Решение поставленных задач основывается на применении общенаучного метода теоретического уровня исследования – логический метод, предполагающий выявление эмпирических характеристик предмета, знание которых важно как для уяснения функционирования предмета, так и для косвенного установления общих законов его развития.

Проблема когерентности решается программным (задача возлагается на компилятор и ОС) и аппаратным способами. Аппаратные методы обеспечивают более высокую производительность, поскольку издержки, связанные с когерентностью, имеют место только при возникновении ситуации некогерентности. В общем случае для поддержания когерентности аппаратными способами в системах с разделяемой памятью применяются следующие подходы [1, 2]: разделяемая кэш-память; некэшируемые данные; широковещательная запись; протоколы наблюдения; протоколы на основе справочника. Из рассмотренных методов наиболее часто используемыми являются протоколы наблюдения и протоколы на основе справочника. Оба эти метода рассматривались с позиции эффективности использования в СХД.

В протоколе на основе справочника справочник хранит состояние каждого блока и кэш-контроллеры посылают все запросы к справочнику. Справочник либо отвечает на запрос, либо перенаправляет запрос к одному или нескольким другим контроллерам когерентности, которые затем отвечают. Транзакции когерентности обычно включают либо два шага (одноадресный запрос, сопровождаемый одноадресным ответом), либо три шага (одноадресный запрос, $K \geq 1$ перенаправленных запросов, и К ответов, где К - это количество совладельцев). Некоторые протоколы имеют также четвертый шаг либо из-за того, что ответы идут косвенно, через справочник, либо из-за того, что инициатор запроса уведомляет справочник о выполнении транзакции [1]. Напротив, протоколы наблюдения распространяют состояние блока ко всем возможным контроллерам когерентности. Так как не существует централизованной справки об этом распространенном состоянии, запросы когерентности должны быть широковещательно переданы ко всем контроллерам когерентности. Транзакции когерентности, таким образом, обычно включают два шага.

Отличительной чертой СХД является высокая масштабируемость. Из всех описанных выше протоколов когерентности лучше всего масштабируются к большому количеству ядер протоколы на основе справочника из-за целенаправленной передачи сообщений. Кроме того, выбор протокола влияет на соединительную сеть: протокол наблюдения характерен для систем на базе шины, т.к. легче реализовать наблюдение и широковещательную передачу; протокол на основе справочника характерен для сложных систем, таких как СХД, где узлы объединены многоступенчатой иерархической сетью.

Справочник в кэш-памяти содержит полное подмножество набора записей справочника. Таким образом, ключевая проблема проекти-

рования – обработка неудачных обращений в кэш-память справочника. Существует несколько способов обработки неудачных обращений [1]: хранить полный справочник во внешней памяти; хранить в справочнике только состояния блоков, которые кэшируются на микросхеме (исчерпывающий кэш справочника) и вообще отказаться от использования кэш-памяти справочника, при этом контроллер справочника просто перенаправляет запрос ко всем контроллерам когерентности.

Способы обработки неудачных обращений в кэш-память справочника

	Кэш с внешним справочником	**Исчерпывающие кэши справочника**		**Отсутствующий кэш справочника**
Расположение справочника	DRAM	LLC (кэш последнего уровня)		нет
Промах в справочнике подразумевает	Кэш справочника должен получить доступ к DRAM	Блок должен быть в недействительном состоянии		Широковещательная передача
Требования вложенности	нет	LLC включает кэши первого уровня		нет
Затраты на внедрение	DRAM + отдельный внутренний кэш	Большие блоки LLC; высокоассоциативный LLC	Большие блоки LLC	нет

Учитывая, что в СХД большая частота запросов, необходимо, чтобы соединительная сеть обладала большой пропускной способностью, а запросы были целенаправленными. При отказе от использования кэш-памяти требуется широковещательная передача, что снижает пропускную способность канала. Первые два метода обладают высокой производительностью, но первый метод требует наличия наборно-ассоциативной кэш-памяти с большим числом каналов, а второй – большого объема внешней памяти. В СХД передаются, обрабатываются и хранятся большие объемы данных, из чего следует необходимость использования большого объема внешней памяти, что, однако, не является критичным параметром и не окажет большого влияния на затраты реализации, по сравнению с первым методом.

Обращая внимание на большой объем хранимых данных и большое количество ядер, было бы нецелесообразно использовать справочник, который поддерживает подробное состояние для каждого блока, включая полный набор ядер, которые совместно используют копии блока данных. Существует два основных способа уменьшения струк-

туры справочника: укрупненные справочники, где каждый бит в списке совладельцев отображает несколько кэшей, и ограниченные справочники, где может отображаться только часть кэшей. Ограниченные справочники привлекательны тем, что они эффективно используют пропускную способность канала, при этом не используя большого количества памяти.

Представление структуры справочника

Таким образом, оптимальным вариантом для крупномасштабных СХД является протокол когерентности на основе справочника, использующий в качестве способа представления структуры справочника – ограниченные справочники; справочник расположить в кэш-памяти, а при промахе обращаться к полному справочнику, расположенному во внешней памяти.

Список литературы

1. D. J. Sorin, M. D. Hill, D. A. Wood A Primer on Memory Consistency and Cache Coherence. Morgan&Claypool Publishers, 2011.

2. Орлов С. А., Цилькер Б. Я. Организация ЭВМ и систем: учебник для вузов. – 3-е изд. Стандарт третьего поколения. – СПб.: Питер, 2014. – 668 с.

3. Васяева Е. С., Сибиряков М. А. Модификация и моделирование алгоритмов обработки данных в кэш-памяти систем хранения данных // Кибернетика и программирование. – 2016. – № 4. – С. 44-57.

УДК 004.93

Кузиков Артем Анатольевич
направление ИТС (бакалавриат), гр. ИТС-21

Научный руководитель
Ипатов Юрий Аркадьевич, канд. техн. наук, доцент,
кафедра информатики
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА И МОДЕЛИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ

В данной статье представлена корпоративная сеть небольшой фирмы, разработанная в программе моделирования компьютерных сетей Cisco Packet Tracer [1]. В процессе изучения компьютерных сетей многие сталкиваются с проблемой отсутствия необходимого оборудования для получения нужных навыков. Одним из решений является использование программ моделирования и имитации работы сетей.

Архитектура подразумевает представление сети в виде системы элементов, каждый из которых выполняет определенную частную функцию, при этом все элементы вместе согласованно решают общую задачу взаимодействия компьютеров.

На рисунке 1 представлен общий вид смоделированной компьютерной сети.

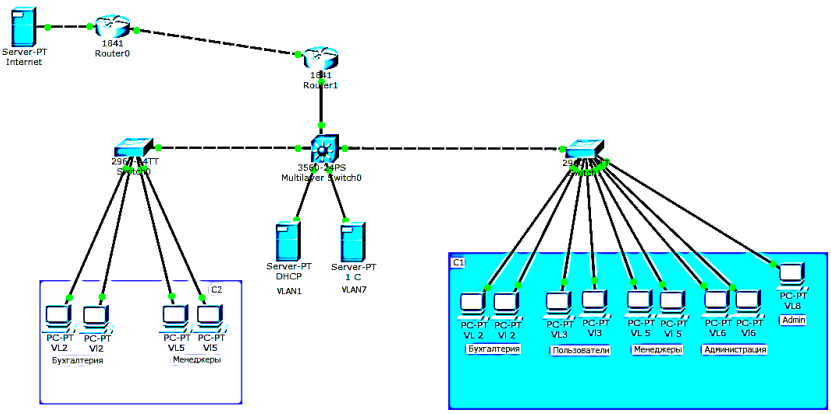


Рис. 1. Общий вид моделируемой сети

Топологией данной сети является древовидная структура [2], большая несколько сегментная локальная сеть на территории до нескольких километров в поперечнике, объединяющая локальные сети близко расположенных зданий.

С1 и С2 – это две локальные сети, находящиеся в соседних зданиях, подключенные к коммутатору 3 уровня. Каждая сеть имеет разделение на сеть отделов, которая привязана к своему vlan. VLAN — техника виртуальных локальных сетей позволяет разбивать коммутируемую локальную сеть на несколько обособленных логических сегментов, предотвращающих распространение нежелательного трафика по всей сети, кроме того, это свойство улучшает управляемость сети. Каждый vlan имеет собственную подсеть, для простоты понимания порядковый номер vlan соответствует 3 октету ip адреса подсети. Данное решение представлено в ниже приведенной таблице с пояснением.

Vlan 1	DHCP сервер имеет собственный vlan, ip адрес 192.168.1.1
Vlan 2	Отдел бухгалтерии находится в подсети 192.168.2.0
Vlan 3	Штатные сотрудники находятся в подсети 192.168.3.0
Vlan 5	Менеджеры находятся в подсети 192.168.5.0
Vlan 6	Руководство фирмы – подсеть 192.168.6.0
Vlan 7	Серверу 1С выделена своя подсеть с IP адресом 192.168.7.2
Vlan 8	Админы также имеют свою подсеть 192.168.8.0

Моделирование работы службы DHCP

DHCP – сетевой протокол [3], позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

На рисунке 2 показана полная настройка DHCP сервера, включающая в себя настройку шлюза, максимальное число пользователей, которые могут быть подключены к определенному vlan, маску подсети, а также начальный IP адрес, с которого начнется раздача IP адресов в vlan’е.

Автоматическое получение IP адресов настроено на всех vlan, привязанных к компьютерам сети. Серверы имеют статичные IP адреса, вписанные вручную администратором сети.

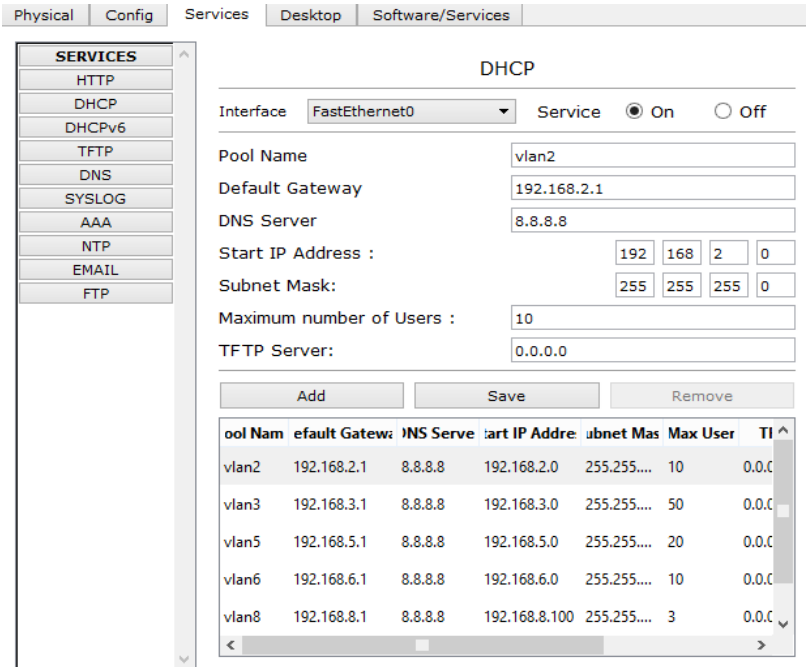


Рис. 2. Настройка DHCP сервера

Моделирование работы 1С сервера

1С сервер моделирует работу сервера бухгалтерии. К этому серверу имеют доступ только отдел бухгалтерии и администратор сети. Для этого достаточно прописать команду ping в командной строке компьютера бухгалтерии.

Параметры доступа к 1С серверу реализованы с помощью Access - листов, прописанных на роутере [4] локальной сети Router1. На рисунке 3 показаны разрешающие команды Access - листа.

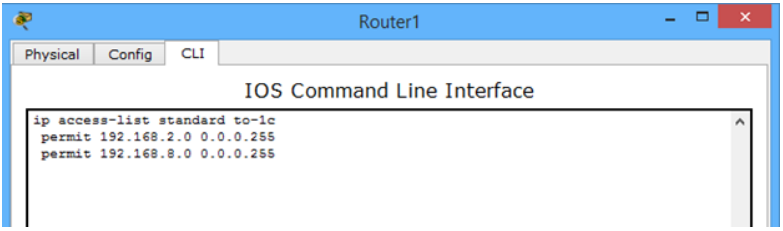


Рис. 3. Access - лист 1С сервера

Мы видим 2 разрешающие команды на доступ подсетям бухгалтерии и администратора сети. Также существует неявное правило, которое запрещает доступ к серверу остальным пользователям.

Моделирование доступа к внешней сети – Интернет.

Данная сеть имеет доступ к сети Интернет, реализованный в виде сервера Internet и роутера провайдера Router0. Сервер имеет внешний белый IP адрес 210.234.20.2. Прописав IP адрес в адресной строке браузера на компьютере, мы видим главную страницу первого в мире сайта. С помощью access - листов мы запретили доступ с внешней сети Интернет к локальной сети.

В данной статье была рассмотрен метод моделирования компьютерных сетей в программе Cisco Packet Tracer. Данная программа имеет большой функционал для проектирования и настройки сетей, а та же отлично подходит для детального изучения и понимания основ функционирования сетей, настройки сетевого оборудования (VLAN, IP адресация, маршрутизация).

Список литературы

1. Уэнделл Одом. Официальное руководство по подготовке к сертификационным экзаменам CCENT/CCNA ICND1. – М.: Вильямс, 2009. – 672 с.
2. Олифер В., Олифер Н. Топология физических связей // Компьютерные сети. Принципы, технологии, протоколы. – 2010. – С. 55.
3. RFC 2131. Dynamic Host Configuration Protocol March 1997 [Электронный ресурс]. – URL: https://tools.ietf.org/html/rfc2131 (дата обращения 04.01.2016).
4. Танненбаум Э. Компьютерные сети / Computer Networks. – 4-е изд. – СПб.: Питер, 2008. – С. 992.

УДК 004.056.55

Лопатин Юрий Александрович
направление Информационная безопасность (магистратура), гр. БИм-21

Научный руководитель
Леухин Анатолий Николаевич, д-р физ.-мат. наук, профессор,
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

МЕТОД ШИФРОВАНИЯ НА ОСНОВЕ ГОМОМОРФНЫХ ОТОБРАЖЕНИЙ В ПОЛЯХ ГАЛУА

Введение

Криптография уже давно гарантированно выполняет многие задачи по сохранению конфиденциальности информации. Однако в связи с

ростом и развитием средств передачи информации, телекоммуникаций и компьютерных сетей, особенно Интернета, перед криптографией появляются новые задачи. Одной из таких задач является обеспечение вычислений над зашифрованными данными. То есть шифрование данных на основе гомоморфных отображений позволяет оперировать зашифрованными данными так же, как и открытыми.

Впервые такую задачу поставили в 1978 году Рональд Риветс, Леонард Адлеман и Майкл Дертузо: *Можно ли делать произвольные вычисления над данными, в то время как они остаются зашифрованными, никогда не расшифровывая их?* Однако их первые попытки потерпели неудачу. Тогда авторы решили, что их идея не подлежит реализации.

С тех пор более 30 лет не было реализации гомоморфного шифрования. Хотя и предпринимались попытки создать такую систему: в 1982 году Шафи Гольдвассер и Сильвио Микали, в 1999 году Паскалем Пэйе, в 2005 году Дэн Бонэ, Ю Чжин Го и Коби Ниссим. Лишь в 2009 году предложенная Крэйгом Джентри система получила развитие, и в 2013 году в IBM схема получила название BGV (Бракерски-Гентри-Вайкунтанатан). В нашей стране вопрос гомоморфного шифрования развивают Л. К. Бабенко, Ф. Б. Буртыка, О. Б. Макаревич, А. В. Трепачева, А. О. Жиров, А. О. Жирова, С. Ф. Кренделев.

Арифметика поля Галуа широко используется в криптографии, только обзора метода шифрования на основе гомоморфных отображений в полях Галуа не представлено среди существующих методов гомоморфного шифрования. Цель данной статьи – познакомить читателя с основами поля Галуа, необходимыми для реализации метода шифрования на основе гомоморфных отображений в полях Галуа.

1. Поля Галуа

Рассмотрим сведения по теории полей Галуа, необходимые для шифрования на основе гомоморфных отображений.

Множество элементов называется полем, если заданы операции сложения и умножения, удовлетворяющие следующим законам [1, 2] (табл. 1).

Поле, содержащее конечное число элементов q, называется *конечным полем* и обозначается $GF(q)$ (GF – означает Galois Field – поле Галуа). *Порядком конечного поля* называется число элементов поля [4].

Элементами конечного поля могут быть числа и полиномы, для нашего метода необходимо рассмотрение полиномов над конечным полем.

Полином $A(x) = \sum_{i=0}^{n} a_i x^i$ называется полиномом над полем $GF(p)$, если его коэффициенты a_i принадлежат полю $GF(p)$. Степенью полинома $A(x)$ называется наибольшее число n такое, что $a_n \not\equiv 0 \pmod p$.

Таблица 1 – **Законы, выполняющиеся в поле**

Закон	Операция	
	сложение	умножение
Замкнутость: для каждой пары элементов $a,b \in M$ существует, и притом единственный, элемент $c \in M : c = a * b$	A1. $a + b = c$	M1. $ab = c$
Ассоциативность: $(a * b) * c = a * (b * c)$	A2. $(a+b)+c = a+(b+c)$	M2. $(ab)c = a(bc)$
Коммутативность: $a * b = b * a$	A3. $a+b=b+a$	M3. $ab=ba$
Наличие единичного элемента: существует элемент $e \in M$ такой, что $a * e = e * a = a$, где $a \in M$	A4. $a + e = e + a = a$ $(e = 0)$	M4. $ae = ea = a$ $(e = 1)$
Наличие обратных элементов: для любого $a \in M$ существует элемент $\bar{a} \in M$ такой, что $a * \bar{a} = \bar{a} * a = e$	A5. $a + \bar{a} = \bar{a} + a = 0$ $(\bar{a} = -a)$	M5. $a\bar{a} = \bar{a}a = 1$ $(\bar{a} = a^{-1}, a \neq 0)$
Дистрибутивность	D1. $a(b + c) = ab + ac$ D2. $(b + c)a = ba + ca$	

Сравнение полиномов $A(x)$, $B(x)$ по модулю полинома $F(x)$ [1, 2]

$$A(x) \equiv B(x)(\text{mod } F(x)) \quad (1)$$

по определению эквивалентно равенству

$$A(x) - B(x) = K(x)F(x) \quad (2)$$

для некоторого полинома $K(x)$.

Все операции в сравнении (1.1) выполняются по модулю p; этот факт обычно отмечают записью

$$A(x) \equiv B(x)(\text{modd } F(x),p), \quad (3)$$

которая читается: полином $A(x)$ сравним с полиномом $B(x)$ по *двойному модулю* $(F(x), p)$ [4].

Все полиномы $A(x)$ над полем $GF(p)$ такие, что $A(x) \equiv R(x)$ (modd $F(x), p$) при фиксированном $R(x)$, т. е. полиномы, которые дают при делении на $F(x)$ остаток $R(x)$, образуют *класс полиномов по двойному модулю* $(F(x), p)$, который обозначают через $\{R(x)\}$ или $R(x)$ (modd $F(x), p$).

Из определения следует, что всем полиномам класса отвечает один и тот же остаток $R(x)$ и можно получить все полиномы класса, если в форме $F(x)K(x) + R(x)$ заставить $K(x)$ пробегать все полиномы с коэффициентами из $GF(p)$.

Если $F(x)$ – полином степени n над полем $GF(p)$, то всевозможные остатки $R(x)$ – полиномы степени не выше $n-1$:

$$R(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0, \qquad (4)$$

где каждое из a_0, a_1, ..., a_{n-1} может быть любым из p элементов поля $GF(p)$.

Из (4) следует, что существует точно p^n различных полиномов $R(x)$. Соответственно имеется p^n классов полиномов по двойному модулю $(F(x), p)$. Любой полином класса называется *вычетом по двойному модулю* $(F(x), p)$ по отношению ко всем полиномам этого класса.

В соответствии со свойством сравнений [1, 2], если $A(x) \equiv R(x) (\text{modd } F(x),p)$ и $B(x) \equiv P(x) (\text{modd } F(x),p)$, то $A(x)+B(x) \equiv R(x)+P(x) (\text{modd } F(x),p)$ и $A(x)B(x) \equiv R(x)P(x) (\text{modd } F(x),p)$.

Тем самым определены *сложение и умножение классов вычетов по двойному модулю* $(F(x), p)$:

$$\{R(x)\} + \{P(x)\} = \{R(x) + P(x)\} \text{ и } \{R(x)\} \cdot \{P(x)\} = \{R(x)\, P(x)\}. \qquad (5)$$

Легко проверить, что все законы поля, исключая *M5*, удовлетворяются для сложения и умножения классов вычетов, заданных посредством (5) при произвольном $F(x)$ над полем $GF(p)$. Однако так же, как это имело место при сравнении целых чисел, *M5* выполняется только в том случае, если $F(x)=f(x)$ – полином, неприводимый над $GF(p)$.

Полином $f(x)$ степени $n \geq 1$ с коэффициентами из поля $GF(p)$ неприводим над полем $GF(p)$, если он не может быть представлен в форме $f(x) = A(x)B(x)$, где $A(x)$ и $B(x)$ – полиномы над $GF(p)$ [1].

Взяв от каждого класса по одному вычету, получим полную систему вычетов. Обычно в качестве полной системы вычетов употребляют полиномы степени не выше $n-1$, т. е. полиномы вида (4).

Полная система вычетов по двойному модулю $(f(x), p)$, где $f(x)$ – полином, неприводимый над $GF(p)$, и p – простое число, удовлетворяет всем законам поля.

Таким образом, *полная система вычетов по двойному модулю* $(f(x), p)$ *образует конечное поле, содержащее* p^n *элементов, которые обозначают через* $GF(p^n)$ *и называют расширенным полем или расширением степени n простого поля* $GF(p)$ [4].

Рассмотрим, что в теории полей Галуа представляет гомоморфизм, а точнее частный случай гомоморфизма – изоморфизм.

Основополагающая теорема полей Галуа гласит [1, 2]: *Для каждого простого числа p и произвольного* $n \geq 1$ *существует конечное поле порядка* p^n*, единственное с точностью до изоморфизма* [4].

Если в двух множествах M, $\overline{M}$ определены некоторые соотношения между элементами и если элементу a из M поставлен в соответствие один и только один элемент $\overline{a}$ из $\overline{M}$ так, что

1) каждый элемент $\overline{a}$ из $\overline{M}$ является образом по меньшей мере одного элемента из M;

2) все соотношения между элементами из M выполняются и для соответствующих элементов из $\overline{M}$,

то $\overline{M}$ называется *гомоморфным образом множества M* [2]; в этом случае пишут $M \sim \overline{M}$ или $a \sim \overline{a}$.

В частности, если множество представляет собой мультипликативную группу поля $GF(p^n) - G$, то каждому ее элементу можно поставить в соответствие элемент $\psi(a)$, $a \in M$, так чтобы выполнилось условие *гомоморфизма:*

если $a \sim \psi(a)$, $b \sim \psi(b)$ и $c = ab$, (6)

то $c \sim \psi(c) = \psi(ab) = \psi(a)\,\psi(b)$, $a, b, c \in G$.

Функция ψ называется *характером мультипликативной группы* [2, 3].

Взаимно однозначное отображения элементов поля на элементы того же поля, при котором удовлетворяются все законы поля, называется *автоморфизмом поля* [1, 2].

Взаимно-однозначное отображение элементов полей заданного порядка, построенных соответственно по различным неприводимым полиномам, при котором удовлетворяются все законы поля, называются *изоморфизмом* [2].

Поле, изоморфное полю $GF(q^s)$, будем обозначать через $G\tilde{F}(q^s)$ и писать $GF(q^s)\,(q^s)\,GF(q^s) \approx G\tilde{F}(q^s)$.

Элементы поля $GF\,(q^s)$ будем по-прежнему обозначать через $a, b, c, \ldots$, а элементы поля $G\tilde{F}(q^s)$ – через $\tilde{a}, \tilde{b}, \tilde{c}, \ldots$

Если преобразование $x \to z$ переводит неприводимый над полем $GF\,(q)$ полином степени s – $\tilde{f}\,(x)$ в неприводимый над полем $GF\,(q)$ полином степени s – $\tilde{f}\,(x)$, т. е.

$$f(z) \equiv 0(\text{modd } \tilde{f}\,(x), p), \tag{7}$$

то отображение

$$a(\text{modd } f(x), p) \approx \tilde{a}(\text{modd } \tilde{f}(x), p) \tag{8}$$

где

$$a = a_{s-1}x^{s-1} + a_{s-2}x^{s-2} + ..a_1x + a_0$$
$$\tilde{a} = a_{s-1}x^{s-1} + a_{s-2}x^{s-2} + ..a_1x + a_0$$
$$a \in GF(q)$$

есть изоморфизм поля $GF(q^s)$.

Действительно, такое отображение однозначно обратимо**,** так как для каждого элемента $a \in GF(q^s)$ существует элемент $\tilde{a} \in G\tilde{F}(q^s)$ и обратно. Далее, если $a,b \in GF(q^s)$, $\tilde{a},\tilde{b} \in G\tilde{F}(q^s)$ и $a \approx \tilde{a}, b \approx \tilde{b}$, то

$$\begin{aligned} a + b &\approx \tilde{a} + \tilde{b} \\ ab &\approx \tilde{a}\tilde{b}. \end{aligned} \qquad (9)$$

Приведем технические характеристики тестируемых навигационных приемников (табл. 1) [3,5].

2. Математическое обоснование шифрования на основе гомоморфных отображений в полях Галуа

Поле $GF(q^n)$ имеет три различных представления [5]:

- степенное,
- полиноминальное,
- векторное.

Рассмотрим на простом примере, как образуются эти представления, и найдем изоморфизм между двумя полями $GF(2^4)$.

Для этого используем два неприводимых многочлена над полем $GF(2^4)$: $f_1(x) = x^4 + x + 1$, $f_2(x) = x^4 + x^3 + 1$ (табл. 2, 3).

Полиноминальное представление можно вычислить из степенного представления: $x^m (\text{modd } f(x), p) = x \cdot x^{m-1} (\text{modd } f(x), p)$.

Векторное представление представляет собой значение коэффициентов a_n из полиноминального представления

$$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0 .$$

Изоморфизм между элементами двух построенных полей составит: $x_1^m \approx (x_2^m)^{7 \bmod 15}$.

Проверим согласно (9), что

$$c_1 = a_1 + b_1 \approx c_2 = a_2 + b_2$$
$$d_1 = a_1b_1 \approx d_2 = a_2b_2$$

Для примера примем, что $a_1 = x_1^3$, $b_1 = x_1^7$, тогда

$$a_2 = (x^3)^{7 \bmod 15} = x_2^6,\ b_2 = (x^7)^{7 \bmod 15} = x_2^4 .$$

Таблица 2 – **Различные представления элементов поля *GF*(2⁴) по двойному вычету** ($f_1(x) = x^4 + x + 1$, 2)

Степенное представление	Полиноминальное представление	Векторное представление
0	0	0000
$x_1^0 = 1$	1	0001
x_1^1	x_1	0010
x_1^2	x_1^2	0100
x_1^3	x_1^3	1000
x_1^4	$x_1 + 1$	0011
x_1^5	$x_1^2 + x_1$	0110
x_1^6	$x_1^3 + x_1^2$	1100
x_1^7	$x_1^3 + x_1 + 1$	1011
x_1^8	$x_1^2 + 1$	0101
x_1^9	$x_1^3 + x_1$	1010
x_1^{10}	$x_1^2 + x_1 + 1$	0111
x_1^{11}	$x_1^3 + x_1^2 + x$	1110
x_1^{12}	$x_1^3 + x_1^2 + x + 1$	1111
x_1^{13}	$x_1^3 + x_1^2 + 1$	1101
x_1^{14}	$x_1^3 + 1$	1001

Сумму элементов удобно вычислять в полиноминальном представлении:

$$c_1 = x_1^3 + x_1^7 = ((x_1^3) + (x_1^3 + x_1 + 1)) \operatorname{modd} (x^4 + x + 1), 2 = x_1 + 1 = x_1^4,$$

или в векторном:

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = x_1^4.$$

$$c_2 = x_2^6 + x_2^4 = ((x_2^3 + x_2^2 + x_2 + 1) + (x_2^3 + 1)) \bmod (x^4 + x^3 + 1), 2 = x_2^2 + x_2 = x_2^{13}.$$

$$\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = x_1^{13}.$$

Таблица 3 – **Различные представления элементов поля *GF*(2^4) по двойному вычету** ($f_2(x) = x^4 + x^3 + 1$, 2)

Степенное представление	Полиноминальное представление	Векторное представление
0	0	0000
$x_2^0 = 1$	1	0001
x_2^1	x_2	0010
x_2^2	x_2^2	0100
x_2^3	x_2^3	1000
x_2^4	$x_2^3 + 1$	1001
x_2^5	$x_2^3 + x_2 + 1$	1011
x_2^6	$x_2^3 + x_2^2 + x_2 + 1$	1111
x_2^7	$x_2^2 + x_2 + 1$	0111
x_2^8	$x_2^3 + x_2^2 + x_2$	1110
x_2^9	$x_2^2 + 1$	0101
x_2^{10}	$x_2^3 + x_2$	1010
x_2^{11}	$x_2^3 + x_2^2 + 1$	1101
x_2^{12}	$x_2 + 1$	0011
x_2^{13}	$x_2^2 + x_2$	0110
x_2^{14}	$x_2^3 + x_2^2$	1100

Произведение элементов удобно вычислять в степенном представлении:

$$d_1 = x_1^3 x_1^7 = (x_1^{3+7})^{\mathrm{mod}15} = x_1^{10};$$

$$d_2 = x_2^6 x_2^4 = (x_2^{6+4})^{\mathrm{mod}15} = x_2^{10}.$$

Проверяем соответствие согласно найденному изоморфизму:

$$(x^4)^{7\,\mathrm{mod}15} = x^{13},\ (x^{10})^{7\,\mathrm{mod}15} = x^{10}.$$

Заключение

Шифрование на основе гомоморфных отображений в полях Галуа будет заключаться в следующем: соотношение данных одного из конечных полей, определение изоморфных отображений в другом конечном поле и передача изоморфных отображений облачному серверу.

Далее в облачном сервере будут осуществляться вычисления над зашифрованными данными в соответствии с правилами вычислений в полях Галуа, затем результаты вычислений передаваться клиенту. Клиент уже по известному ему изоморфизму определит, какой результат был получен.

Инструменты гомоморфной криптографии в ближайшем будущем смогут оказать свое влияние на рынок облачных услуг и (в той или иной степени) на облик современных информационных технологий.

Список литературы

1. Чеботарев Н. Г. Основы теории Галуа. – М.: ОНТИ, 1934. – 220 с.

2. Ван-дер-Варден Б. Л. Современная алгебра, ч. 1, 2 / пер. с нем. – М.: Изд-во технико-теоретической литературы, 1947.

3. Виноградов И. М. Основы теории чисел. – 5-е изд. – М.: Наука, 2003. – 178 с.

4. Свердлик М. Б. Оптимальные дискретные сигналы. – М.: Сов.радио, 1975. – 200 с.

5. Акритас А. Основы компьютерной алгебры / пер. с англ. – М.: Мир, 1994. – 545 с.

6. Лидл Р., Нидеррайтер Г. Конечные поля: в 2-х т. Т.1 / пер. с англ. – М.: Мир, 1988. – 430 с.

УДК 378.147.88

Лысаковская Анастасия Андреевна
направление Информационная безопасность (магистратура), гр. БИм-21

Научный руководитель
Александров Александр Петрович, доцент,
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ПЕРЕХВАТ СООБЩЕНИЙ В КАНАЛАХ СОТОВОЙ СВЯЗИ

В настоящее время мобильная связь является привычным атрибутом жизни. Данная статья посвящена угрозам и недостаткам защиты мобильной связи. В качестве основной технологии будет рассматриваться технология стандарта GSM. GSM (англ. Global System for Mobile Communications) – глобальный стандарт цифровой мобильной сотовой связи, с разделением каналов по времени (TDMA) и частоте (FDMA), разработанный в конце 80-х годов прошлого века.

1. **GSM** относится к сетям второго поколения (2 Generation) (1G – аналоговая сотовая связь, 2G – цифровая сотовая связь, 3G – широкополосная цифровая сотовая связь). Забегая вперед, необходимо отметить, что хотя перехватывать разговоры в GSM-сети можно, сделать это далеко не просто, вопреки распространенному мнению.

1.1. Архитектура GSM-сети. Особенности работы

Перед тем как приступить к рассмотрению способов перехвата, необходимо понять архитектуру сети и принципы ее работы.

Архитектура сети GSM похожа на архитектуру обычных телефонных сетей, но имеет некоторые особенности. Сеть состоит из трех основных подсистем:

– подсистема базовых станций (BSS – Base Station Subsystem);

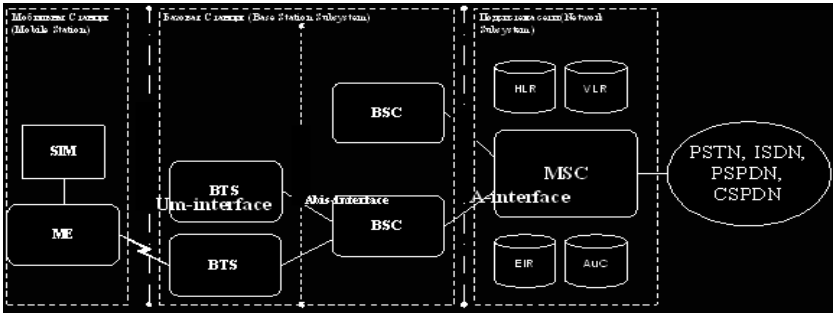
– подсистема сети и коммутации (NSS – Network Switching Subsystem), которая является «ядром» (core network) системы;

– центр технического обслуживания (OMC – Operation and Maintenance Centre).

В отдельный класс оборудования выделены мобильные (сотовые) телефоны (MS – Mobile Station).

Для обеспечения сервисов пакетной передачи существует также расширение GPRS. Это позволяет мобильным телефонам получать доступ к интернету.

Архитектура сети GSM представлена на рисунке. Для однозначности интерпретации будем использовать термины и обозначения, принятые в рекомендациях GSM.



Архитектура GSM-сети

SIM (Subscriber Identification Module) – модуль идентификации абонента.

MS (Mobile Station) – мобильная станция (мобильный (сотовый) телефон).

PSTN (Public Switched Telephone Network) – телефонная сеть общего пользования, в которой используются обычные проводные телефонные аппараты, мини-АТС и оборудование передачи данных.

BSS состоит из BTS (англ. Base Transceiver Station), т.е. самих базовых станций и контроллеров базовых станций (BSC – Base Station Controller). Область, которую покрывает одна BTS, называют сотой. Сигнал от станции имеет теоретический радиус 120 км, но на практике составляет от 400 м до 50 км.

Области покрытия соседних станций перекрываются, тем самым обеспечивается возможность передачи обслуживания MS при перемещении ее из одной соты в другую без разрыва соединения (handover). Сигнал от каждой станции распространяется, покрывая площадь в виде круга, но при пересечении с областями покрытия соседних станций получаются правильные шестиугольники.

При разработке стандарта были учтены задачи оптимального размещения станций при минимальном перекрытии зон. В итоге каждая станция имеет 6 соседей и именно поэтому при перекрытии зон получаются шестиугольники, которые похожи визуально на пчелиные соты (в разрезе). Отсюда происходит альтернативное название «сотовая» связь.

Основная задача контроллера базовых станций (BSC) заключается в контроле соединения между BTS и подсистемой коммутации. Также он управляет очередностью соединений, скоростью передачи данных, распределением радиоканалов, производит сбор статистики и контроль различных радиоизмерений, управляет процедурой handover.

Ядро (NSS) состоит из центра коммутации (MSC), домашнего (HLR) и гостевого (VLR) регистров местоположения, регистра идентификации оборудования (EIR) и центра аутентификации (AUC).

Центр коммутации (MSC – Mobile Services Switching Centre) контролирует определенную географическую зону с расположенными на ней BTS и BSC. Он осуществляет установку соединения к абоненту и от него внутри сети GSM, обеспечивает интерфейс между GSM и PSTN, другими сетями радиосвязи, сетями передачи данных (GPRS). Также выполняет функции маршрутизации вызовов, управление вызовами, эстафетной передачи обслуживания при перемещении MS из одной зоны в другую. После завершения вызова MSC обрабатывает данные по нему и передает их в центр расчетов для формирования счета за предоставленные услуги (биллинг), собирает статистические данные. MSC также постоянно следит за положением MS, используя данные из HLR и VLR, что необходимо для быстрого нахождения и установления соединения с MS в случае ее вызова.

Домашний регистр местоположения (HLR – Home Location Registry) содержит базу данных абонентов, приписанных к нему. Здесь содержится информация о предоставляемых данному абоненту услугах, информация о состоянии каждого абонента, необходимая в случае его вызова, а также Международный Идентификатор Мобильного Абонента (IMSI – International Mobile Subscriber Identity), который используется для аутентификации абонента (при помощи AUC). Каждый абонент приписан к одному HLR. К данным HLR имеют доступ все MSC и VLR в местной GSM-сети, а в случае межсетевого роуминга – и MSC других сетей.

Гостевой регистр местоположения (VLR – Visitor Location Registry) обеспечивает мониторинг передвижения MS из одной зоны в другую и содержит базу данных о перемещающихся абонентах, находящихся в данный момент в этой зоне, в том числе абонентах других систем GSM – так называемых роумерах. Данные об абоненте удаляются из VLR в том случае, если абонент переместился в другую зону. Такая схема позволяет сократить количество запросов на HLR данного абонента и, следовательно, время обслуживания вызова.

Регистр идентификации оборудования (EIR – Equipment Identification Registry) содержит базу данных, необходимую для установления подлинности MS по IMEI (International Mobile Equipment Identity, международный идентификатор мобильного абонента (индивидуальный номер абонента)). Формирует три списка: белый (допущен к использованию), серый (некоторые проблемы с идентификацией MS) и черный (MS, запрещенные к применению). У российских операторов (и большей части операторов стран СНГ) используются только белые списки, что не позволяет раз и навсегда решить проблему кражи мобильных телефонов.

Центр аутентификации (AUC – Authentification Centre). В задачи этого компонента входит обеспечение аутентификации и защиты информации в GSM-сетах.

1.2. Обновление местоположения

Важной процедурой работы в сети GSM является обновление местоположения (Location update, LU). Для того чтобы в момент звонка BSS не искала абонента на всей зоне покрытия, она должна хотя бы примерно представлять, где в настоящий момент находится каждый MS. Информация о текущем местоположении предоставляется самим MS с помощью процедуры, называемой «location update». BSS объединяются в логические группы, называемые location area (LA). Все LA пронумерованы, у каждой есть определенный числовой код – Location Area Code (LAC). Текущий «адрес» телефона в сети представляет собой пару (LAC, CellID), где CellID – числовой идентификатор «соты». Пара (LAC, CellID) уникальна в пределах всей сети.

В каждый момент времени телефон слушает до 16 широковещательных каналов (broadcast channel, BCH) от 16 сот. На основании услышанного он выбирает 6 «лучших» сот, с которыми (по мнению телефона) у него будет максимально устойчивая связь с минимальными затратами энергии. Из этих шести сот телефон выбирает одну «самую лучшую» на основании так называемых «критериев C1 и C2» (технические детали этих критериев нам здесь не важны). Именно эту соту телефон постарается использовать для получения или совершения звонка.

После включения телефон пытается зарегистрироваться в сети. В процессе телефон формирует список 6 соседних сот, выбирает из них лучшую и использует «общий канал доступа» (RACH) этой соты, чтобы сообщить о том, что его текущее местоположение – тут, в этой самой соте. Эта информация (пара LAC+CellID) попадает в контроллер базовых станций (BSC), а от него передается коммутатору (MSC), который обслуживает эту часть сети.

Коммутатор сохраняет информацию о текущем местоположении телефона в специальном кэше, называемом VLR (Visitor Location Register). В дальнейшем телефон периодически (обычно раз в час, но зависит от настроек сети) будет выполнять LU. Либо же если абонент передвигается, то телефон будет выполнять LU при переходе в зону покрытия соты из другого LA. В быту это проявляется в виде специфических звуковых наводках, если телефон находится рядом с колонками (наушниками).

1.3. Выделение каналов

В заключение рассмотрения особенностей функционирования GSM сети кратко опишем реализацию выделения каналов в радиодиапазоне. Это важно для понимания особенностей перехвата сигналов в сети GSM.

Для GSM выделен спектр определенной частоты, поэтому необходимо оптимально распределить ширину полосы между всеми возможными пользователями. Как уже упоминалось ранее, GSM использует комбинацию методов множественного доступа TDMA и FDMA (Time– and Frequency–Division Multiple Access).

Сначала полоса частот в 25 МГц делится на полосы в 200 Кгц. Каждой станции соответствует своя полоса (или несколько полос). Абоненты полосы разделены во времени, каждый из каналов делится между 8 абонентами. Каждому абоненту соответствует один кадр. Восемь кадров объединяются во фрейм (TDM – кадр). 26 фреймов, в свою очередь, образуют мультифрейм, который повторяется циклически. Длина мультифрейма – 120 миллисекунд. На один кадр приходится 1/200 мультифрейма, т.е. около 0,6 миллисекунды. Позиция 12 в мультифрейме занята для целей управления, а 25-я зарезервирована для будущих применений.

2. Безопасность GSM

В стандарте GSM следующие механизмы безопасности:

- аутентификация;
- секретность передачи данных;
- секретность абонента;
- секретность направлений соединения абонентов.

Защита сигналов управления и данных пользователя осуществляется только по радиоканалу.

2.1. Аутентификация

Как было отмечено выше в описании архитектуры, аутентификацией в GSM занимается подсистема AUC. Рассмотрим работу этого компонента подробнее.

В процессе производства SIM-карт производитель заносит в ROM каждой карты случайное число, называемое «KI» (Key for identification). Это число будет служить секретным ключом для данной SIM-карты. Когда SIM-карты доставляются мобильному оператору, с ними передаются данные о KI каждой новой SIM-карты. Эти данные (в виде пар (IMSI, KI)) заносят в «центр аутентификации» мобильной сети (AUC).

2.2. Обеспечение секретности абонента

Для исключения определения (идентификации) абонента путем перехвата сообщений, передаваемых по радиоканалу, каждому абоненту системы связи присваивается «временное удостоверение личности» – временный международный идентификационный номер пользователя (TMSI), который действителен только в пределах LA. В другой LA ему присваивается новый TMSI. Если абоненту еще не присвоен временный номер (например, при первом включении MS), идентификация проводится через международный идентификационный номер (IMSI). После окончания процедуры аутентификации и начала режима шифрования временный идентификационный номер TMSI передается на MS только в зашифрованном виде. Этот TMSI будет использоваться при всех последующих доступах к системе. Если MS переходит в новую LA, то ее TMSI должен передаваться вместе с идентификационным номером зоны (LAC), в которой TMSI был присвоен абоненту.

При входе MS в новую LAC осуществляется процедура опознавания, которая проводится по старому, зашифрованному в радиоканале TMSI, передаваемому одновременно с LAC. LAC дает информацию центру коммутации и центру управления о направлении перемещения MS и позволяет запросить прежнюю зону расположения о статусе абонента и его данные, исключив обмен этими служебными сообщениями по радиоканалам управления.

3. Перехват информации в GSM

3.1. Клонирование SIM-карты

Одной из распространенных проблем является клонирование SIM-карты. В интернете часто можно встретить объявления о легком способе клонировании карты, а также представлено множество утилит, например, SIM CardSeizure. В качестве целей клонирования обычно указывают возможность бесплатно звонить за чужой счет и возможность прослушивания разговоров владельца клонированной SIM-карты. В первом варианте использования у владельца клона будут проблемы с получением входящих звонков, а вот исходящие можно делать свободно. Основными потребителями являются люди, которые

затем у метро предлагают прохожим дешево позвонить в любую страну мира. Что касается прослушивания абонента, то этот вопрос будет рассмотрен ниже.

3.2. Перехват разговоров в сети GSM

Переходим к рассмотрению взлома GSM.

Большинство статей по взлому GSM опираются на статью Эли Баркана (2006) и исследование Карстена Нола (Karsten Noh).

В своей статье Баркан с соавторами показали, что так как в GSM коррекция ошибок идет до шифрования (а надо бы наоборот), возможно определенное уменьшение пространства поиска для подбора КС и реализация known-ciphertext атаки (при полностью пассивном прослушивании эфира) за приемлемое время с помощью предварительно вычисленных данных.

Сами авторы статьи говорят, что при приеме без помех для взлома в течение 2 минут требуется 50 терабайт предвычисленных данных. В той же статье указывается, что сигнал из эфира всегда идет с помехами, которые усложняют подбора ключа.

Переходим к инженерным проблемам. Как получить данные из эфира? Для перехвата разговоров надо иметь полноценный сканер, который должен уметь разбираться, какие базовые вещают вокруг, на каких частотах, каким операторам они принадлежат, какие телефоны с какими TMSI в настоящий момент активны. Сканер должен уметь следить за разговором с указанного телефона, корректно обрабатывать переходы на другие частоты и базовые станции.

Перехват сообщений в GSM сетях возможен. Следовательно, необходимо разрабатывать современные методы по защите информации от перехвата в GSM сетях.

Список литературы

1. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами: учебное пособие / под ред. Ю.Ф. Каторина. – СПб.: НИУ ИТМО, 2012. – 416 с.

2. Хорев А. А. Технические средства и способы промышленного шпионажа. – М.: ЗАО «Дальснаб», 1997.

3. Каторин Ю., Куренков Е., Лысов А., Остапенко А. Антишпионские штучки. Энциклопедия промышленного шпионажа. – СПб.: Полигон, 2000. – 512 с.

УДК 654.9, 004.932.72'1

Лычко Сергей Александрович
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-31

Научный руководитель
Малашкевич Василий Борисович, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ ДРОНОВ

В последние годы широкое распространение получили частные гражданские беспилотные летательные аппараты – дроны [1]. Спектр их использование очень широк: от игр и бизнес-приложений до военного применения. К сожалению, иногда дроны могут применяться злоумышленниками. Примерами такого использования являются кража конфиденциальной или коммерческой информации, проникновение на закрытую территорию и т. д.

Существующие системы защиты от вышеперечисленных рисков создаются, как правило, в военной области или частными предприятиями для внутреннего использования и являются закрытыми. Поэтому актуальны исследование и разработка открытых систем обнаружения дронов в воздушном пространстве охраняемых объектов, создание методов и алгоритмов их функционирования, а также разработка методов противодействия вторжениям дронов.

Целью исследования является разработка открытой и относительно простой аппаратно-программной системы, которая позволит производить обнаружение и распознавание дрона в полете и при необходимости выполнять действия по подавлению неправомерного функционирования дронов.

Для решения поставленной задачи необходимо разработать средства мониторинга секторов окружающего воздушного пространства с помощью видеокамер, анализ полученного потока видеоизображения в режиме реального времени, выделение из видеоизображения летящих объектов и распознавание среди них дронов. С целью повышения вероятности правильного обнаружения дронов могут быть использованы также системы ультразвуковой локации. В случае обнаружения дрона производится анализ ситуации и, при необходимости, активация модулей по подавлению неправомерного функционирования дронов.

Настоящий проект предусматривает разработку аппаратной платформы системы, состоящей из следующих частей:

1. *Сенсорный каскад*, позволяющий производить съемку в оптическом и/или инфракрасном диапазоне, а также предобработку результатов. Предобработка позволит существенно сжать видеопотоки за счет обнаружения и передачи видео только движущихся объектов. Для реализации сенсорного каскада могут использоваться IP-камеры или Web-камеры высокого разрешения совместно с одноплатными микрокомпьютерами Rapsberry Pi [2, 3].

Сжатый видеопоток передается на сервер системы с помощью проводного сетевого соединения или посредством Wi-Fi.

Дополнительным сенсором каскада является ультразвуковой локатор, обеспечивающий информацию о скорости вращения винтов дрона на основе доплеровского смещения частоты отраженного звукового сигнала. Аналогичные системы локации применяются в измерителях скорости движения автомобилей.

2. *Серверная часть*, на которой производятся обработка данных, полученных от сенсорного каскада, распознание дронов и автоматическое принятие решения о вторжении.

3. *Система сигнализации*, позволяющая активизировать систему подавления, передать сигнал о вторжении диспетчеру, а также запротоколировать и сохранить данные, необходимые для последующего анализа зафиксированной ситуации.

4. *Система подавления или перехвата управления дронами*. Перехват дронов возможен вследствие открытости протоколов управления. Например, известна система SkyJack, способная «захватить» летящего дрона. Для дронов с закрытым управляющим трафиком может использоваться «ослепление» дрона с помощью излучения множества «мусорных» управляющих пакетов, блокирующих управление дроном злоумышленников.

Значительную часть проекта составляют разработка и исследование эффективности алгоритмов обнаружения и классификации дронов. Для решения этих задач могут быть использованы алгоритмы компьютерного зрения и машинного обучения, для которых существуют открытые реализации, например библиотека OpenCV [4]. Повышения эффективности работы этих алгоритмов можно добиться с помощью их комплексирования и каскадирования с помощью методов бустинга.

Таким образом, в настоящей работе предложена концепция построения аппаратно-программной системы обнаружения и защиты от вторжения дронов на основе модульной структуры. Определены ос-

новные блоки системы и показана возможность их реализации на основе известных промышленно выпускаемых изделий. Значительных исследований потребует разработка алгоритмов обнаружения и классификации дронов. В работе определены основные направления таких исследований.

Разработка и реализация предложенной системы позволит предупредить возможные негативные последствия использования дронов. Практическая значимость предлагаемой работы определяется расширением функций систем безопасности и их способностью противостоять новым современным угрозам.

Список литературы

1. Беспилотная авиация // UAV.RU [Электронный ресурс]. – 2009. – URL: http://www.uav.ru/articles/tech_modern.pdf (дата обращения 08.11.2016).

2. Компания Axis Communications [Электронный ресурс]. – 2016. – URL: http://www.axis.com/ru/ru (дата обращения: 08.11.2016).

3. Новости информационных технологий // PVSM.RU [Электронный ресурс]. – 2010. – URL: http://www.pvsm.ru/raspberry-pi/51571/print/ (дата обращения 08.11.2016).

4. Открытая социальная сеть TechCave: Нахождение контуров объекта в OpenCV // TECHCAVE.RU [Электронный ресурс]. – 2016. – URL: techcave.ru/posts/51-nahozhdenie-konturov-obekta-v-opencv/ (дата обращения 08.11.2016).

УДК 004.056

Ляшко Елена Викторовна
направление Информационная безопасность (специалитет), гр. БИс-31

Научный руководитель
Смирнов Владимир Иванович, старший преподаватель,
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ОСОБЕННОСТИ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ И ПРИМЕНЕНИЕ ЗНАНИЙ О ФИЗИЧЕСКИХ ЭФФЕКТАХ

Введение

В данной статье раскрыты особенности каналов утечки речевой информации, а также возможность применения знаний о физических эффектах (ФЭ) при выборе акустических материалов для защиты речевой информа-

ции. Особое внимание уделено перспективной задаче по поиску новых марок веществ и материалов, применяемых для защиты речевой информации.

Защита речевой информации от утечки по техническим каналам является одной из важнейших задач в области инженерно-технической защиты информации. Способов защиты речевой информации и технических средств, реализующих эти способы, существует достаточно много, и они постоянно совершенствуются.

Особенности каналов утечки речевой информации

Как известно, в состав технических каналов утечки информации (ТКУИ) входят генератор информативного сигнала, физическая среда и приёмник. Г. А. Атаманов отмечает тот факт, что возникновение ТКУИ обусловлено «особенностями функционирования технических средств, используемых владельцем для обработки, передачи и хранения информации» [1]. Очевидно, что особенности функционирования ТСОИ и ВТСС тесно связаны с проявлением в них тех или иных физических эффектов.

В научно-технической литературе можно встретить различные классификации ТКУИ. Для большинства обобщенных классификаций характерно то, что каналы утечки речевой информации представляют собой отдельную группу ТКУИ. Это вызвано специфическими особенностями речевой формы представления защищаемой информации (табл. 1).

Характерные свойства речевой информации

Свойство	Описание	Примеры
Конфиденциальность	Устно отдаются такие распоряжения, которые не могут быть доверены никакому носителю	По показаниям двойного агента Элизабет Бентли, Лочлин Керри передавал сведения советской разведке только в устной форме [2]
Оперативность	Перехват речевой информации может осуществляться в момент её озвучивания	Долгое время благодаря подслушивающему устройству в посольстве США в Москве советское руководство имело возможность получать очень важную оперативную информацию, что давало определенные преимущества в осуществлении мировой политики в период «холодной войны» [3]
Документальность	Современные методы анализа речи по речевому сообщению позволяют однозначно идентифицировать личность того человека, который озвучил это сообщение	В 1985 г. во ВНИИ МВД СССР была разработана методика опознавания личности по лингвистическим признакам речи [4]
Виртуальность	По речи человека можно сделать заключение о его эмоциональном состоянии	Гневу соответствует увеличение частоты основного тона, диапазона основного тона, частоты первой форманты и темпа речевого сигнала [5]

Особенностью технических каналов утечки речевой информации является то, что анализ информации, перехваченной с помощью технического средства разведки (ТСР), производит человек. По этой причине «в качестве нормативного показателя оценки эффективности защиты ЗП от утечки речевой информации по техническим каналам часто (но не всегда) используется словесная разборчивость речи W» [6].

Для технических каналов утечки речевой информации типична ситуация малых отношений сигнал/шум и наличия тех или иных ТСР (датчики, микрофоны, антенны, усилители, радиопередатчики и т.п.). Появляются новые ТСР, которые могут найти применение в акустических ТКУИ [7].

Технические каналы утечки речевой информации подразделяются на прямой акустический канал и акусто-преобразовательные каналы. Их индивидуальность обусловлена проявлением тех или иных ФЭ. Встречаются ситуации, когда сложно определить тип канала утечки речевой информации из-за его смешанного характера [8]. Например, при прямом подслушивании конфиденциальных переговоров человеком с ослабленным слухом, речевой сигнал докладчиков воспринимается микрофоном, фильтруется, усиливается и излучается специальным вибратором, к которому прикасается злоумышленник с ослабленным слухом для восприятия речевых сигналов. Такой канал утечки можно отнести как к акустоэлектрическим (из-за использования аналоговых электронных технических средств), так и к акустовибрационным (из-за специального способа излучения и восприятия речевой информации).

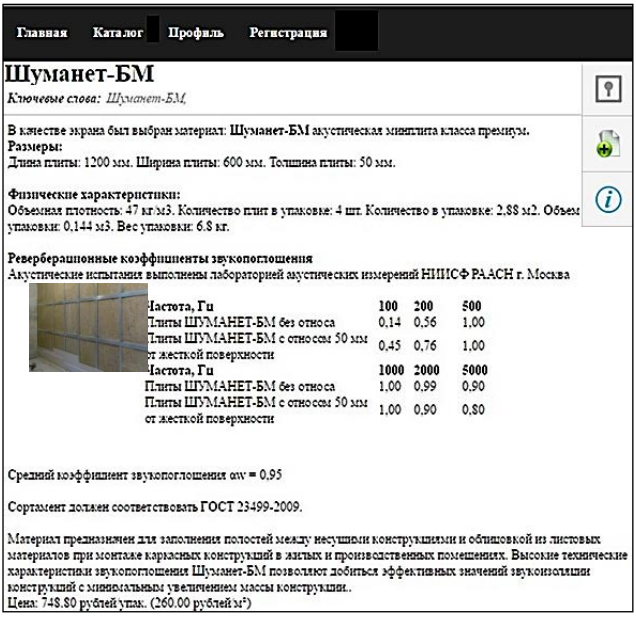
Для защиты речевой информации могут применяться активные (использование специальных генераторов, к которым подключаются излучатели различного типа, и применение специальных технических средств) и пассивные методы (звукоизоляция, звукопоглощение и глушение звука).

Применение знаний о физических эффектах (ФЭ) при выборе акустических материалов для защиты речевой информации

Экономическое потрясение отечественной промышленности в конце XX века заставило свернуть производство многих изделий, в том числе тех, которые традиционно использовались для звукоизоляции, звукопоглощения и глушения звука в помещении. Обострение геополитической обстановки, зарубежные санкции против ряда отечественных компаний и целых регионов – всё это заставляет задуматься о проблеме обеспечения технологической независимости России. Существует необходимость в рациональном выборе акустических материалов и изделий отечественного производства, используемых при проектировании, строительстве и реконструкции зданий.

Функциональные элементы ТСОИ, ВТСС, ТСР, а также свойства материалов и конструкций, применяемых в инженерно-технической защите информации, основываются на использовании различных ФЭ (совокупностей взаимосвязанных ФЭ). Сложность анализа этих элементов и свойств заключается в том, что специалисту по инженерно-технической защите приходится абстрагироваться на уровне ФЭ. Очень трудно мысленно представить и оценить их возможные комбинации, характеризующие новые потенциальные ТКУИ. Специалисту по защите информации известно только ограниченное количество ФЭ, поскольку их число постоянно увеличивается с развитием науки и техники.

Для того чтобы изменить данную ситуацию, предлагается разработка и развитие информационного ресурса в сети Интернет (см. рисунок). Это позволит собрать информацию об акустических материалах и изделиях отечественного производства, которые нашли или могут найти практическое применение в области инженерно-технической защиты информации. В дальнейшем предполагается создание экспертной системы в помощь специалисту по защите информации. При этом будет учитываться подход к выявлению ТКУИ с использованием ФЭ [9].



Информационный ресурс (прототип)

Величина результата воздействия C_i для конкретного ФЭ зависит от используемых марок веществ и материалов (точнее от кортежа параметров $<b_1, b_2, \ldots, b_n>$). Количество известных веществ и материалов, на которых проявляется тот или иной ФЭ, сильно разнится. Не все известные марки материалов и веществ, на которых проявляется тот или иной физический эффект, нашли практическое применение в области инженерно-технической защиты информации.

Заключение

В качестве пассивных средств защиты речевой информации от утечки по техническим каналам обычно используются те марки материалов и веществ, которые позволяют получить наибольший эффект и удовлетворяют нормативным, эксплуатационным и экономическим требованиям. В связи с этим поиск новых марок веществ и материалов можно считать одной из перспективных задач в области инженерно-технической защиты информации.

Список литературы

1. Атаманов Г. А. Технические каналы утечки информации: определение, сущность, классификация // Защита информации. INSIDE. – 2010. – № 1. – С. 28-33.
2. Лайнер Л. «Венона». Самая секретная операция американских спецслужб. – М.: ОЛМА-ПРЕСС Образование, 2003. – 384 с. – (Досье).
3. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами: учебное пособие / под ред. Ю.Ф. Каторина. – СПб.: НИУ ИТМО, 2012. – 416 с.
4. Женило В. Р. Компьютерная фоноскопия. – М.: Акад. МВД России, 1995. – 208 с.
5. Галунов В. И. О возможности определения эмоционального состояния говорящего по речи // Речевые технологии: научно-практический журнал. – 2008. – № 1. – С. 60-66.
6. Дураковский А. П., Куницын И. В. Оценка защищенности речевой информации. Часть 1. Выявление акустических и вибрационных каналов утечки речевой информации: учебно-методическая разработка для проведения лабораторного практикума. – М.: НИЯУ МИФИ, 2015. – 52 с. – Серия «Учебная книга факультета «Кибернетика и Информационная безопасность» НИЯУ МИФИ».
7. The Visual Microphone: Passive Recovery of Sound from Video, by Abe Davis, Michael Rubinstein, Neal Wadhwa, Gautham J. Mysore, Frédo Durand, William T. Freeman (MIT CSAIL, Microsoft Research and Adobe Research) // ACM Transactions on Graphics. – 2014. – Vol. 33, No. 4, Article 79. – Pp. 1-10.
8. Дидковский В. С., Дидковская М. В., Продеус А. Н. Акустическая экспертиза каналов речевой коммуникации: монография. – Киев: Имэкс-ЛТД, 2008. – 420 с. – Серия «Библиотека акустика. Акустическая техника. Т.9».
9. Смирнов В. И., Пекунов А. А. Защита информации от утечки по техническим каналам: системный подход и подход с использованием физических

эффектов // Инженерные кадры – будущее инновационной экономики России: материалы Всероссийской студенческой конференции (Йошкар-Ола, 23-28 ноября 2015 г.): в 8 ч. – Йошкар-Ола: ПГТУ, 2015. – Ч. 4: «Информационные технологии – основа стратегического прорыва в современной промышленности». – С. 95-99.

УДК 004.93

Маркин Кирилл Анатольевич,
Полухин Владислав Вадимович
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-21

Научный руководитель
Ипатов Юрий Аркадьевич, канд. техн. наук, доцент,
кафедра информатики
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СИНТЕЗ ХЭШ-ФУНКЦИИ С МИНИМАЛЬНЫМИ КОЛИЗИОННЫМИ СВОЙСТВАМИ

Современное общество невозможно представить без Интернета. Информационные технологии окружают нас повсюду. Человек постоянно сталкивается с необходимостью обмениваться информацией, хранить личные данные, вести переписку, нередко используя для этого пароли и логины, однако вопросы безопасности остаются при этом очень актуальными.

Хотим мы того или нет, но в мире ежедневно происходят взломы серверов и баз данных. Учитывая этот факт, каждый хочет быть уверенным в том, что его личные данные, такие как пароли пользователей, будут надежно защищены и скрыты от чужих глаз. Поэтому, чтобы понять, как обезопасить себя в будущем, нужно более детально исследовать тему хеширования.

Первоначальной функции хеширования [1] было создание уникального образа информационных последовательностей произвольной длины с целью идентификации и определения их подлинности. Постепенно с развитием технологий возможности развития и усовершенствования хеш-функций перешли на новый уровень.

Процесс хеширования превращает введенные данные в набор строковых и целочисленных элементов. Происходит это благодаря одностороннему хешированию. В итоге после произведенных вычислений вы-

полнить обратное преобразование будет очень сложно или вовсе невозможно. Когда мы получим результат, будет практически невозможно определить исходные данные, но одни и те же входные данные дают одинаковый итог. Отсюда спектр использования хеш-функций является очень большим, но чаще применяется для хранения информации, такой как логин, пароль, номер удостоверения или другой персональной информации.

Вместо сравнивания сведений, вводимых пользователем, с теми, которые хранятся в базе данных, происходит сопоставление их хешей. Все это дает гарантию, что при непреднамеренной утечке информации никто не сможет воспользоваться важными данными для личных целей. Еще одним преимуществом хеш-кода является то, что удобно проверять правильность загрузки файлов с Интернета, особенно если во время скачивания происходили перебои связи.

В 1990-х гг. были разработаны такие известные функции, как MD4 и MD5 (более надежный вариант) [2]. MD5 предназначена для преобразования входящих данных (вне зависимости от их размера) в результат фиксированной длины. Порой результат ее работы называют «отпечатком» или «дайджест сообщением». Несмотря на то, что на сегодняшний день MD5 является несколько устаревшим (был разработан еще в 1991 г.) и к использованию не рекомендуется, он до сих пор все еще в ходу, и часто вместо слова «хеш-код» на сайтах просто пишут MD5 и указывают сам код.

Если применять MD5, в итоге результатом хеширования станет строка приблизительно размером 32 символа, которые будут в шестнадцатеричном виде. В функцию MD5 можно помещать строки и числа любой длины, но на выходе всегда будем получать результат в 32 символа. Уже только этот факт – хорошее подтверждение тому, что это «односторонняя» функция. Но тут назревает вопрос: раз была придумана столь сложная система хеширования, почему с каждым днем ее пытаются усовершенствовать? Все дело в коллизиях хеш-функций. Коллизия хеш-функции – это получение одинакового результата для разных изначально введенных данных[3].

Первые попытки взлома MD5 были предприняты 1 марта 2004 г. компанией CertainKeyCryptosystems. Они запустили проект MD5CRK, целью которого являлось выявление коллизий. 24 августа 2004 г. проект завершил свою работу. Была обнаружена уязвимость, которая позволяла найти коллизии аналитическим методом. И уже в 2005 г. это было продемонстрировано на практике.

Одним из особых видов атак на хеш-функции является Chosen-Prefix. Атакующий берёт два случайных документа и может показать,

какие биты нужно изменить в одном документе, чтобы получить требуемую хеш-функцию. Такая атака была впервые проведена в 2007 г., сложность выявления коллизии составила около 250 вызовов. Функция MD5 теряет свою актуальность из-за отсутствия возможности совершенствования. Поэтому с каждым годом современные сервисы используют более новые хеш-функции для хранения данных.

Сложившаяся в последнее время ситуация говорит о том, что необходимо повышать уровень безопасности хеш-функций. Пришло время проанализировать другие стратегии для конструирования безопасных хэш-функций. Решению именно этой задачи и посвящена данная работа.

На рисунке 1 представлена блок-схема алгоритма синтеза хеш-функции, которая обладает сравнительным уровнем устойчивости к коллизиям.

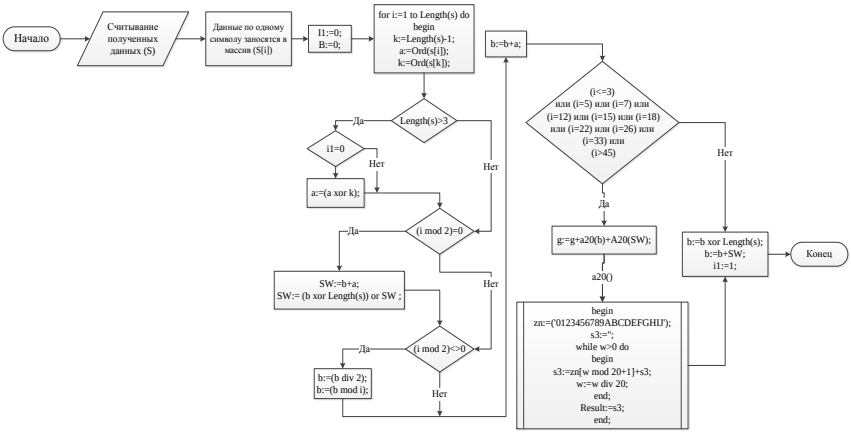


Рис. 1. Блок схема работы программы Swithcedv.3

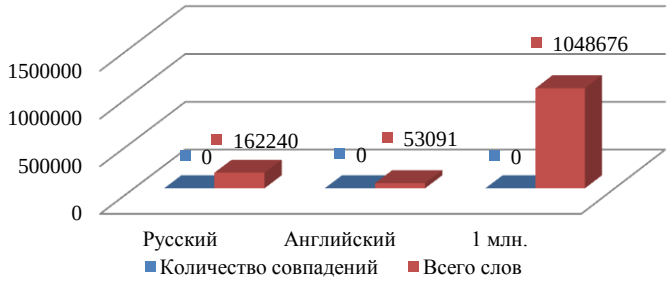


Рис. 2. Диаграмма коллизий программы Swithced

На рисунке 2 показаны результаты тестирования созданного алгоритма по уровню коллизий для русского и английского словарей. Анализ данных показывает, что реализованный алгоритм обеспечивает данный уровень возникновения коллизий.

Результаты моделирования и анализа результатов показывают, что созданный прототип решения хэш-функции не уступает по уровню коллизий функции MD5.

Список литературы

1. Hellerman H. Digital Computer System Principles. McGraw-Hill, 1967.
2. Чмора А. Современная прикладная криптография. – М.: Гелиос АРВ, 2001.
3. Фергюсон Н., Шнайер Б. Практическая криптография: пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 424 с.: ил.

УДК 004.056

Менщиков Александр Алексеевич,
Комарова Антонина Владиславовна
направление Методы и системы защиты информации, информационная безопасность (аспирантура)

Научные руководители:
Гатчин Юрий Арменакович, д-р техн. наук, профессор,
Коробейников Анатолий Григорьевич, д-р техн. наук, профессор,
кафедра проектирования и безопасности компьютерных систем
ФГАОУ ВО НИУ «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»,
г. Санкт-Петербург

ТЕНДЕНЦИИ ПАТЕНТОВАНИЯ МЕТОДОВ АУТЕНТИФИКАЦИИ НА ВЕБ-РЕСУРСАХ

Введение

Данная статья посвящена изучению методов аутентификации на веб-ресурсах. Цель проводимого исследования – рассмотрение основных существующих способов и методов в данной области, а также тенденций их патентования.

Изучаемый вопрос является актуальным, поскольку самые распространённые на сегодняшний день подходы и алгоритмы, такие как парольная аутентификация, являются устаревшими [1]. В качестве метода

исследования можно назвать сравнительный анализ различных реализаций. Также мы приводим их классификацию по особенностям использования, сложности имплементации и стойкости к атакам [2].

Было проведено патентное исследование, которое показало возрастание популярности разработок этой тематики. Мы приводим статистику и тенденции, которые существуют на сегодня в области патентования методов аутентификации в веб.

Описание исследования

Был выполнен поиск с использованием международной базы данных патентов espacenet [3]. В данную базу включены сведения от 189 государств, являющихся членами международной организации по интеллектуальной собственности WIPO [4]. В ходе поиска использовались сложные запросы по ключевым словам: «authentication» и «web» и тематикам, связанным с обработкой данных на компьютере, сетевыми протоколами и схемами, а также криптографическими методами передачи информации [5].

Результаты были сгруппированы по тематикам, правообладателям и годам, производился поиск географической принадлежности организаций и авторов, дополнительно изучалось цитирование патентов.

Результаты исследования

Были выбраны 266 основных патентов, которые наиболее полно вписывались в исследуемую тематику, данные выбирались за 1999-2016 годы. Распределение и динамика патентования по годам приведена на рисунке 1.

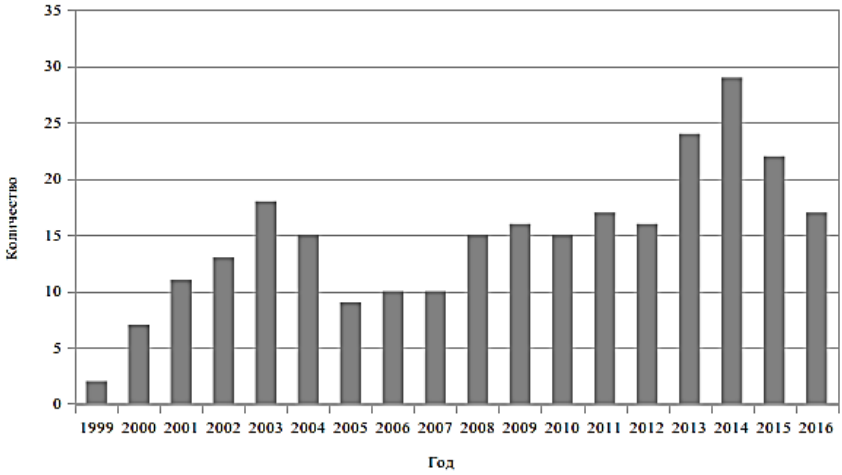


Рис. 1. Распределение количества патентов по годам

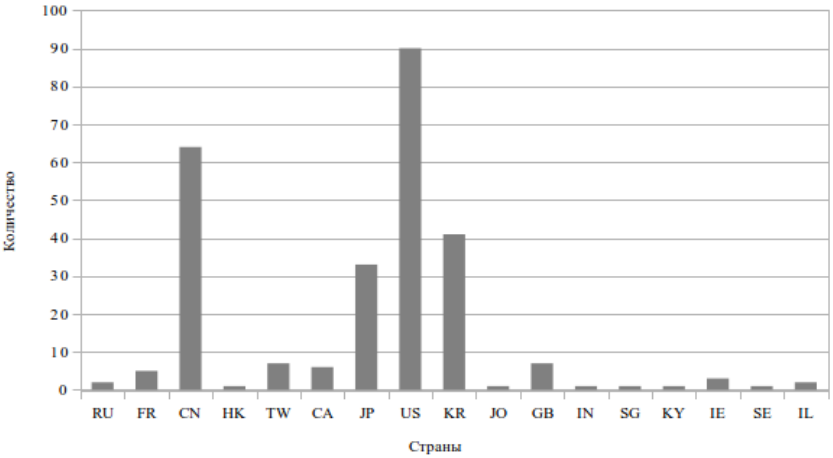


Рис. 2. Количество патентов по странам

Была проанализирована статистика тематических групп, к которым относятся изучаемые методы аутентификации, а также принадлежность компаний-заявителей патентов по странам (рис. 2). Следует отметить, что наилучшие результаты показали компании из США и Китая.

Выводы

Результаты данного исследования показали актуальность тематики, увеличение числа запатентованных методов и способов аутентификации на веб-ресурсах, а также достаточно высокую перспективность и востребованность разработки новых методов, основанных на улучшении и объединении существующих подходов, а также разработки новых оригинальных алгоритмов.

Результаты данной работы можно с успехом использовать при проведении патентного поиска в области защиты информации, а также при выборе тематики своих исследований молодыми учеными.

Список литературы

1. Bonneau Joseph, et al. // The quest to replace passwords: A framework for comparative evaluation of web authentication schemes // 2012 IEEE Symposium on Security and Privacy. IEEE, 2012.

2. Schechter S., Brush A. J. B., Egelman S. // It’s no secret: Measuring the security and reliability of authentication via “secret” questions // IEEE Symp. Security and Privacy. – 2009. – Pp. 375–390.

3. База патентов espacenet [Электронный ресурс]. – URL: http://worldwide.espacenet.com/ (дата обращения 22.11.2016).

4. Сайт международной организации по интеллектуальной собственности WIPO [Электронный ресурс]. – URL: http://www.wipo.int/pct/en/ (дата обращения 22.11.2016).
5. Международная патентная классификация [Электронный ресурс]. – URL: http://www1.fips.ru/wps/wcm/connect/content_ru/ru/inform_resources/international_classification/Inventions/ (дата обращения 22.11.2016).

УДК 004.31

Минина Татьяна Сергеевна,
Вагапова Регина Юнировна
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-31

Научный руководитель
Мясников Владимир Иванович, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА АВТОНОМНОЙ НАВИГАЦИОННОЙ СИСТЕМЫ

Введение

В настоящее время проблема нахождения потерявшихся в лесах людей достаточно актуальна. Несмотря на предупреждения специалистов, обычно люди не всегда берут с собой в лес телефон, навигатор или компас. Профессиональный навигатор достаточно дорогой, телефон бесполезен, так как в лесах плохая связь с оператором.

В том случае, когда человек понимает, что потерялся, он пытается связаться с родными или с МЧС. Для этого необходимо установить связь с ближайшей вышкой сотовой связи, на что затрачивается большое количество энергии, вследствие чего телефон полностью разряжается, и шансы на спасение этого заблудившегося малы. Исходя из этого как раз и возникает необходимость в разработке автономной энергоэффективной и недорогой навигационной системы.

Существует множество различных навигаторов. Они могут быть как отдельными устройствами, так и встроенными в телефон. Однако и те и другие обладают рядом недостатков. Эти устройства имеют GPS-модуль, что в большой степени влияет на потребление энергии, а также делает их бесполезными на местности, где отсутствует связь. Кроме того, современные навигаторы обладают огромными функциональными возможностями, в которых нет необходимости при ориентации на мест-

ности, но их наличие влияет на скорость разрядки батареи, что значительно снижает время возможного использования навигаторов. Все перечисленные особенности, безусловно, очень сильно влияют на стоимость устройств.

Целью выполнения нашей НИР является разработка и тестирование автономной навигационной системы.

Решаемые задачи:

- снижение энергопотребления навигатором,
- исключение зависимости от связи со спутником и оператором,
- снижение стоимости устройства.

Техника решения. Схема разрабатываемого устройства приведена на рисунке.

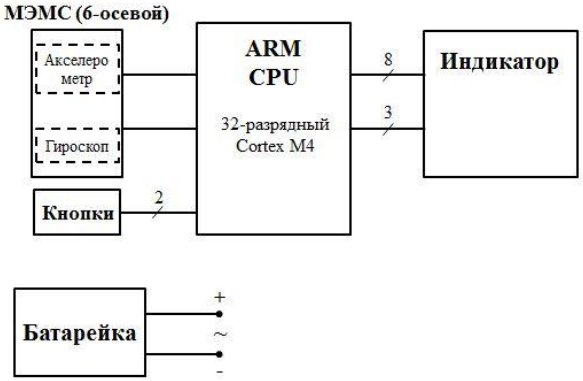


Схема разрабатываемой автономной навигационной системы

В отличие от аналогов, данное устройство для инициализации человека на местности использует акселерометр и гироскоп.

С помощью математических формул, используя направление движения и скорость, устройство вычисляет пройденный путь и направление в исходную точку. Отсутствие GPS-модуля позволяет сохранить заряд батареи на длительное время.

Устройство обладает простым интерфейсом, содержащим ЖК-дисплей, который отображает пройденный путь и направление в начальную точку, и две кнопки – включение/выключение устройства и фиксирование текущего положения.

С увеличением времени использования устройства увеличивается погрешность вычислений начального положения до 100 метров.

При приближении к исходной точке устройство отображает на экране область ее определения. Простота интерфейса делает навигатор удобным и доступным практически для любого человека, в особенности для людей пожилого возраста, что особенно важно, так как именно они чаще всего (как показывает статистика) теряются на незнакомой местности.

Выводы. Исходя из вышеперечисленных достоинств предлагаемой навигационной системы, можно утверждать, что разрабатываемое устройство будет актуальным и конкурентоспособным.

Список литературы

1. Бакмачев А. МЭМС-гироскопы и акселерометры Silicon Sensing: английские традиции, японские технологии // Компоненты и технологии. – 2014. – № 4. – С. 18–26.

2. Матвеев В. В., Распопов В. Я. Основы построения бесплатформенных инерциальных навигационных систем / под ред. В. Я. Распопова. – СПб.: ГНЦ РФ ОАО «Концерн «ЦНИИ «Электроприбор», 2009. – 280 с.

УДК 378.147.34

Морозов Иван Михайлович
направление Информационная безопасность (магистратура), гр. БИм-21

Научный руководитель
Александров Александр Петрович, доцент,
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ОТЕЧЕСТВЕННЫЕ МОДЕЛИ ОЦЕНКИ ОРГАНИЗАЦИОННОЙ ПРИВЕРЖЕННОСТИ

Большая часть современных отечественных моделей оценки надежности персонала основывается на иностранных исследованиях. Некоторые из них (как, например, модели Мейер-Аллен) представляют собой адаптацию западных работ к российским условиям, другие являются более самостоятельными исследованиями. В данной статье рассмотрены три разные, с точки зрения подхода, работы: модель В. И. Доминяка, модель С. С. Баранской и опыт апробации методики Мейер-Аллен И. А. Германова и Е. Б. Плотниковой.

➢ **В. И. Доминяк. Измерение лояльности: действующая модель**

В. И. Доминяк [1] основывался на законе теории развития систем, согласно которому развитие любой системы можно описать S-образной кривой. Развитие включает в себя четыре этапа:

- первый – этап становления;
- второй – этап интенсивного роста;
- третий – стабилизация;
- четвертый – стадия «умирания».

До поступления на работу в организацию потенциальный сотрудник сначала не владеет информацией об организации или владеет ею в минимальном объеме (некая «нулевая» точка). В процессе формирования решения о поступлении на работу он накапливает знания об организации, условиях работы, предполагаемой компенсации и т.п. Одновременно формируется и идеальная картина ожиданий потенциального сотрудника. Его лояльность к организации, которую можно назвать *потенциальной*, или *предварительной*, растет (предположительно по S-образной кривой). На стадии стабилизации он входит в организацию. С момента входа эта лояльность начинает снижаться за счет расхождений между идеальной картиной ожиданий и реальной картиной жизни организации.

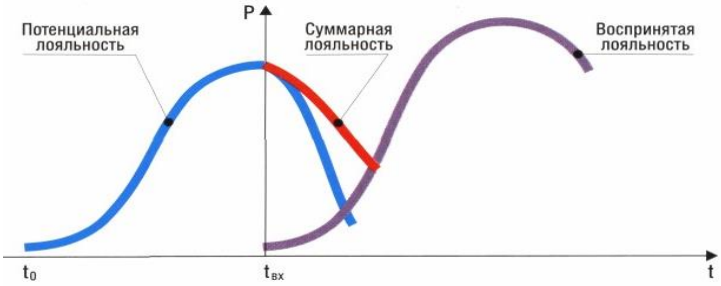
С момента входа в организацию у сотрудника начинает формироваться другая лояльность, основанная на реальном опыте пребывания в организации. Такую лояльность можно назвать *воспринятой* лояльностью. Она также должна развиваться по S-образной кривой.

Итоговая (*суммарная*) лояльность складывается из потенциальной и воспринятой лояльности. Таким образом, результирующая кривая развития лояльности может быть построена на основе двух кривых: потенциальной лояльности и воспринятой лояльности.

График (см. рисунок), построенный В. И. Доминяком, отображает предполагаемое его моделью изменение лояльности в зависимости от стажа сотрудника. На графике t_0 – момент, когда будущий сотрудник начал собирать информацию об организации, $t_{вх}$ – момент трудоустройства.

Теоретически итоговая организационная приверженность должна быть тем выше, чем ближе идеальная картина ожиданий к реальной ситуации.

В 2004 году была проведена практическая проверка модели, в ней приняли участие 235 сотрудников различных отечественных организаций, в том числе 101 мужчина и 134 женщины, в возрасте от 19 до 68 лет.



Зависимость лояльности сотрудника от стажа, В. И. Доминяк [1]

Для сбора информации был использован опросник, созданный по модели OCQ. В процессе анализа собранной информации были обнаружены статистически значимые различия (по t-критерию Стьюдента и непараметрическому критерию Манна-Уитни) между соседними группами «до 1 года» и «2-5 лет», «2-5 лет» и «5-10 лет». В то же время не было обнаружено статистически значимых различий между группами «5-10 лет» и «10-20 лет». На основании этого В. И. Доминяк сделал вывод, что на протяжении первых двух лет организационная приверженность снижается и лишь затем начинает расти, выходя на стабильное плато в районе пяти лет. Падение организационной приверженности после двадцати лет не является статистически достоверным в силу малой выборки по этой возрастной группе.

- **С. С. Баранская. Методика измерения лояльности**

С. С. Баранская [2] рассматривает лояльность трех типов: организационную лояльность, профессиональную лояльность и лояльность труду.

Организационная лояльность

Здесь можно видеть два похода. В первом случае делается акцент на нормативных компонентах лояльности, связанных с принятием, подчинением и разделением сотрудниками норм и правил организации, на отсутствии саботажа и проявлений нелояльного поведения. Во втором случае акцент делается именно на возникновении у сотрудников эмоций и чувств по отношению к организации, что представляет больший интерес для психологического исследования: сотрудники проявляют интерес и озабоченность состоянием дел организации, гордятся своей причастностью к ее команде, принимают участие в решении ее проблем и развитии.

Профессиональная лояльность

Часто причина организационной лояльности заключается не столько в возникновении привязанности к определенной организации, сколько в

возможностях профессиональной самореализации внутри нее, построении карьеры в рамках своей специализации. В данном случае речь идет о профессиональной лояльности. При этом собственно место работы (организация) имеет лишь второстепенное значение по отношению к характеру, специализации работы в ней.

Лояльность труду

Данный вид лояльности связан с восприятием трудовой деятельности, активности в целом как центрального понятия в жизни, имеющего особую ценность для сотрудника. Его рассматривают также как мотивацию к труду и вовлеченность в трудовую деятельность. В русскоязычном варианте лояльность труду соответствует понятию трудолюбия.

Разработку своей методики и модели С. С. Баранская начала с анализа существующих моделей и методик оценки лояльности. Для своей методики измерения она выбрала форму опросника, включающего сорок пунктов по трём подвидам лояльности. Основная роль была отведена организационной лояльности.

После пробного практического испытания, в котором приняли участие 130 человек, число вопросов было сокращено до двадцати. Кроме того, в опросник была добавлена вторая часть, направленная на выявление уровня идеальной лояльности как отношения сотрудника к организации, в которой он бы хотел работать. Наличие второй части позволяет сравнить уровни реальной и идеальной лояльности и тем самым повысить информативность опросника. Однако включение в опросник второй части является лишь дополнительным приемом, и решение о его необходимости зависит исключительно от целей исследования [2].

В основном исследовании приняло участие 310 человек, в том числе 149 мужчин и 152 женщины, в возрасте от 21 года до 74 лет, со стажем работы от полугода до 48 лет. Ключи для обработки методики были получены на основе суммы итоговых баллов респондентов данной выборки по шкалам организационной лояльности, лояльности профессии и труду. На основе полученного распределения баллов проводилась процедура психометрической проверки методики и определения тестовых норм.

Методика представляет собой опросник, состоящий из двух частей по двадцать пять утверждений, относящихся к трем типам лояльности: организационной лояльности, лояльности профессии и лояльности труду. В первой части респондентам предлагается оценить данные утверждения по 5-балльной шкале с точки зрения отношения сотрудников к организации, в которой они работают: от 1 – «абсолютно не согласен», до 5 – «полностью согласен»; во второй части опросника эти же утвер-

ждения оцениваются сотрудниками по отношению к организации, в которой они хотели бы работать. С целью повышения достоверности ответов респондентов и снижения процента социально одобряемых ответов утверждения опросника составлены в форме от третьего лица:

1. Организационная лояльность, которая включает в себя подгруппы: «Гордость за организацию», «Вовлеченность в дела организации» и «Нелояльное поведение».

2. Профессиональная лояльность.

3. Лояльность труду.

На первом этапе исследования С. С. Баранская проверяла концептуальную и факторную валидность методики. Теоретическая модель, положенная в основу структуры шкал опросника, является следствием анализа множества моделей лояльности с точки зрения ее основных компонентов. На основе выделенных компонентов, общих для большинства авторских моделей, С. С. Баранской были разработаны утверждения, входящие в шкалы опросника. Структурная валидность опросника и теоретической модели изучались посредством нескольких вариантов факторного анализа с использованием метода главных компонент и варимакс-вращения.

В процессе исследования рассматривалось два варианта модели: трёхфакторный, описанный выше, и пятифакторный. В пятифакторной модели группа «Организационная лояльность» была разделена на три отдельных группы: «Организационная лояльность», «Вовлеченность в дела организации» и «Нелояльное поведение».

По итогам факторного анализа С. С. Баранская пришла к выводу, что разработанная ею методика измерения лояльности обладает адекватной факторной валидностью для обоих вариантов. И выбор применяемой модели должен зависеть от специфики конкретной задачи.

Затем при помощи критерия нормальности Колмогорова-Смирнова была проведена проверка шкал на нормальность распределения и установлено отступление распределений шкал от нормального закона. Полученные данные были учтены при стандартизации методики.

В процессе стандартизации были получены интервалы для каждой из шкал соответствующие высокому, среднему и низкому уровню соответствующей составляющей лояльности.

- **И. А. Германов и Е. Б. Плотникова. Опыт апробации методики Мейер-Аллен**

В своей работе И. А. Германов и Е. Б. Плотникова [3] провели анализ результатов применения шкалы организационной лояльности промышленных предприятий к различным группам сотрудников, различа-

ющихся как занимаемыми должностями, так и образовательным уровнем. В опросе, проведённом в ходе исследовательской работы, приняли участие 1135 сотрудников пяти крупных промышленных предприятий города Перми. Выборочная совокупность строилась с использованием квотного метода. В опросе приняло участие следующее количество сотрудников из различных групп.

- По занимаемой должности:

181 чел. – 16% - руководящий состав;

274 чел. – 24% - специалисты;

680 чел. – 60% - рабочие.

- По уровню образования:

505 чел. – 45% - общее и начальное профессиональное образование;

278 чел. – 28% - среднее профессиональное образование;

352 чел. – 31% - высшее и неполное высшее образование.

Хотя эти группы и пересекаются (уровень занимаемой должности, как правило, прямо связан с уровнем образования), но рассматриваются они отдельно. Причиной этому служит то, что программы поддержания лояльности на предприятиях связаны с занимаемыми должностями, а их восприятие – с уровнем образования.

В данной исследовательской работе была использована широко распространенная методика – шкала организационной лояльности Мейер-Аллен, основывающаяся на трёхкомпонентной модели, включающей в себя: *аффективную*, *продолженную* и *нормативную лояльности*. При этом использовался измененный перевод модели, выполненный В. И. Доминяком.

Для оценки валидности модели использовался критерий Кронбаха, который показал следующие результаты:

- 0,697 – для аффективной лояльности;
- 0,705 – для продолженной лояльности;
- 0,733 – для нормативной лояльности;
- 0,862 – для модели в целом.

Учитывая, что модель считается достоверной, если альфа Кронбаха более или равна 0,700, И. А. Германов и Е. Б. Плотникова приходят к закономерному выводу, что эффективность отдельных шкал невысока. В то же время исключение из анкеты некоторых вопросов, относящихся к аффективной и нормативной лояльности, позволяет увеличить альфу Кронбаха до 0,701 и 0,785 соответственно.

Также в рамках исследования был сделан ряд интересных наблюдений:

- эффективность шкалы аффективной лояльности выше для сотрудников, занимающих более высокие должности или имеющих более высокий уровень образования;

• для шкалы нормативной лояльности характерна прямо противоположная тенденция;

• шкала продолженной лояльности демонстрирует наибольшую достоверность для сотрудников, занимающих средние должности или имеющих средний уровень образования. Наименьшую достоверность она демонстрирует для рабочих и сотрудников с низким образовательным уровнем.

Интересно, что результаты данного исследования показали, что для руководителей и сотрудников с высшим образованием наличие альтернативных возможностей по трудоустройству мало связано с лояльностью, это пересекается с выводами, сделанными Абдулкадиром Кирмизи и Орканом Дениза в их исследовании «Организационная приверженность специалистов по ИТ в частных банках».

Общий уровень согласованности велик для всех групп, при этом альфа Кронбаха тем выше, чем выше занимаемая должность и уровень образования респондента.

Выводы

Одним из важнейших выводов, сделанных в ходе данной работы, который необходимо учитывать при адаптации модели Мейер-Аллен к российской культурной и социальной специфике, является высокий уровень взаимосвязи всех трёх компонентов. Если в условиях американского общества в частности и западного общества в целом модель Мейер-Аллен демонстрировала высокий уровень взаимосвязи между аффективной и нормативной лояльностью и низкий уровень взаимосвязи между двумя другими парами, то как опыт В. И. Доминяка, так и данная исследовательская работа, показали, что при использовании модели Мейер-Аллен в России все три компонента имеют высокий уровень корреляции, причем он высок для всех групп, участвовавших в исследовании И. А. Германова и Е. Б. Плотниковой. Кроме того, уровень взаимосвязи между компонентами тем выше, чем выше занимаемая должность и уровень образования респондента. Важно также отметить, что общая лояльность имеет умеренную связь с удовлетворением от работы и желанием уволится.

Из работы И. А. Германова и Е. Б. Плотниковой следует, что:

- с одной стороны, методика Мейер-Аллен обладает достаточно высокой надежностью для применения её в России;
- с другой стороны, для получения более достоверных результатов методику необходимо корректировать и учитывать тот факт, что, в отличие от иностранной практики, с учётом российских условий она представляет собой одномерный конструкт, а не трехкомпонентную структуру.

Заключение

Рассмотренные методы оценки надежности персонала основываются на психологических и субъективных факторах. Сведения для оценки сотрудника извлекаются из заполняемого им теста, призванного оценить различные компоненты лояльности к организации и её обобщенный уровень. У такого подхода есть как преимущества, так и недостатки.

К достоинствам его можно отнести:

- продолжительный опыт применения;
- относительную достоверность получаемых результатов;
- простоту применения;

Недостатки:

- учитывается только отношение сотрудника к организации;
- не учитываются факторы, влияющие на сотрудника или характеризующие его;
- при многократном прохождении однотипных тестов сотрудники могут «обмануть» их.

Список литературы

1. Доминяк В. И. Измерение лояльности: действующая модель [Электронный ресурс]. – Владислав Доминяк. 2000-2009. – URL: http://dominiak.ru/publ/publ9.html (дата обращения 29.10.2016).

2. Баранская С. С. Методика измерения лояльности [Электронный ресурс] // Психологические исследования: электрон. науч. журн. – 2011. – № 1(15). – URL: http://psystudy.ru (дата обращения 30.10.2016).

3. Германов И. А., Плотникова Е. Б. Измерение организационной лояльности персонала (Опыт апробации методики Мейер-Аллен) // Вестник Пермского университета. – 2011. – № 3(7). – С. 106-111.

УДК 681.3

Мустафа Ахмет Бадор Мохамед
направление Системы автоматизации проектирования (аспирантура ЛЭТИ)

Научный руководитель
Лячек Юлий Теодосович, канд. техн. наук, профессор
кафедра систем автоматизированного проектирования
ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)», г. Санкт-Петербург

АЛГОРИТМ МОДИФИКАЦИИ ОБЛАСТЕЙ ШТРИХОВКИ, ЗАДАННЫХ ВЫБОРОМ ГРАФИЧЕСКИХ ПРИМИТИВОВ КОНТУРОВ

Рассматриваются особенности автоматического преобразования областей штриховки при модификации конструкторских чертежей при использовании их адаптивной сеточной параметрической модели [1, 2].

В качестве примера, поясняющего формирование сеточной параметрической модели чертежа, на рисунке 1 представлено изображение простой детали, сформированной из четырех отрезков и четырех дуг. Форма детали полностью определяется четырьмя размерными обозначениями.

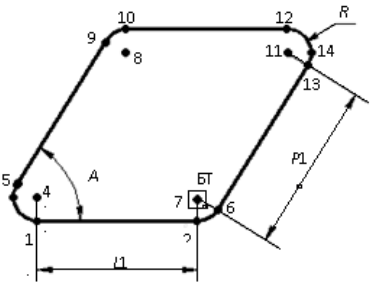


Рис. 1. Чертеж детали с указанием характерных точек его примитивов

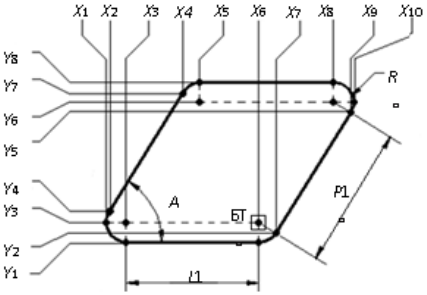


Рис. 2. Прямоугольная базовая сетка, образованная характерными точками примитивов

При изменении значений представленных размерных обозначений задача перерисовки даже такого простого образа детали может занимать у конструктора относительно длительное время. В случае же наличия для чертежа адаптивной к изменению величины размерных обозначений параметрической модели конструктору достаточно указать только новые значения одного или даже всех размеров, и система параметризации обеспечит автоматическое преобразование (модификацию) образа безошибочно и практически мгновенно. Однако для создания такой адаптивной параметрической сеточной модели необходимо:

- сформировать прямоугольную сетку по осям X и Y (рис. 2) на основе анализа всех характерных точек графических примитивов, представленной на чертеже детали, которые определяют ее форму;
- установить функциональную или численную связь между элементами сформированной сетки по обеим координатам [3] через заданные конструктором новые значения размеров, которые установлены на исходном чертеже;
- в соответствии с новыми значениями размерных обозначений определить новые координаты для элементов сеток по X и Y (перестроить базовую сетку);
- установить однозначную связь между старыми (исходными) значениями координат и соответствующими им новыми значениями координат;

- последовательно изменить значения координат характерных точек в описаниях для всех базовых графических примитивов изображения со старых значений на новые. При этом описания и изображения старых (исходных) примитивов должны стираться и изменяться на новые как в файле чертежа, так и файле регенерации изображения.

Сеточная параметрическая модель чертежа позволяет эффективно перестраивать непосредственно базовые графические примитивы, определяющие исходный образ представленной на нем детали. Однако достоинством такой модели является также то, что с ее помощью может быть обеспечена и автоматическая модификация элементов оформления чертежа (размерных обозначений, осевых линий, областей штриховки, различных технологических обозначений и даже форматов), связь которых с базовыми элементами чертежа представляется в неявном виде.

Так как описание примитива штриховки (HATCH) непосредственно не связано с примитивами, определяющими форму детали, то при модификации чертежа изображение штриховки, как правило, смещается относительно перестраиваемых контуров детали. В этой связи штриховка обычно при модификации чертежа не наносится, а просто стирается. Конструкторам приходится добавлять ее в ручном режиме, что существенно снижает эффект от автоматической модификации чертежей.

В работе рассматривается относительно простой вариант автоматической обработки примитива HATCH, все элементы контуров которого задаются непосредственно конструктором. В этом случае все вершины контуров штриховки являются базовыми точками графических примитивов, определяющих образ изображенной на чертеже детали. Поэтому эти точки-вершины автоматически полностью охватываются созданной параметрической сеточной моделью чертежа и могут быть относительно просто скорректированы в соответствии с данными сеточной модели. Сами модифицированные области заполняются штриховыми линиями в соответствии с определяющими примитив HATCH параметрами. К этим параметрам относятся общие данные о штриховке (внутреннее имя, стиль, вид, масштаб, количество образующих контуров и т.д.), и они не должны меняться при модификации. Исключением может быть только масштаб штриховки, если при модификации изображения существенно меняется площадь соответствующих контуров.

Описание штриховки, чертежа в целом и любого используемого в нем графического в dxf-формате представляется вложенными текстовыми списками, состоящими из отдельных структурных единиц – групп, выделяемых круглыми скобками. В каждой группе вначале указывается код группы (групповой код), представляющий целое число, а

затем соответствующая этому коду информация. Такое описание позволяет в файле чертежа найти нужные данные и, при необходимости, изменить их в соответствии с результатами модификации чертежа.

С учетом особенностей описания области HATCH в dxf-файле алгоритм модификации штриховки включает следующие этапы.

1. В цикле выбирается первая запись из выявленных в описании чертежа списка примитивов HATCH, и анализируется ее структура.

2. Если значение группового кода 98, который соответствует внутренней точке задания контура, равно 1, а значение координат для следующей за ней группы с кодом 10 тождественно равны нулю, то такое нулевое значение координат соответствует непосредственному заданию примитивов контуров. Такой примитив штриховки должен подвергаться обработке по предлагаемому алгоритму, иначе возвращаются к этапу 1.

3. В группе с кодом 91 определяется количество контуров, образующих анализируемую область штриховки.

4. В цикле обработки контуров (в соответствии с ранее выявленным их количеством в п. 3), для каждого контура (код группы – 91), входящего в описание, последовательно выявляются:

4.1. Количество базовых графических примитивов, образующих текущий контур (код этой группы – 93);

4.2. В цикле по базовым примитивам текущего контура для каждого графического примитива (код примитива – 72) выявляются его исходные (до модификации) параметры, а затем внутреннее, присвоенное системой, имя этого примитива (код имени – 330). В частности, по коду примитива (72) выявляются следующие параметры:

- для отрезка (значение кода отрезка равно 1) – координаты точки начала (код группы – 10) и конца (код группы – 11),
- полилинии (код примитива – 0) – координаты каждой точки (код группы – 10) и кривизну в ней для последующего сегмента (код группы – 42),
- дуги и окружности (код примитива – 2) – координаты центра (код 10), значения радиуса (код 40), начального (код группы – 50) и конечного углов (код группы – 51) в радианах и направление обхода (код группы – код 73), а значение –1 соответствует обходу против часовой, а 0 – по часовой стрелке;
- эллиптической дуги (код 3) – координаты центра (код 10), координаты точки большой полуоси (код 11), длина малой полуоси в долях от большой (код 40), значение начального (50) и конечного (51) углов в радианах, направление обхода (код 73) со значением 1 – против часовой и 0 – по часовой стрелке;

- сплайна (код примитива 4) – порядок сплайна (код 94), признак рациональности (код 73), признак периодичности (код 74), количество узлов (код 95), количество управляющих точек (код 96), а также данные узла (код 40) и координаты управляющих точек (код 10), которые повторяются в соответствии с количеством узлов.

4.3. Используя сеточную параметрическую модель, заменяют в описании рассматриваемого контура выявленные старые параметры графических примитивов на новые;

4.4. Осуществляют модификацию (перерисовку) области текущего контура в соответствии со скорректированными новыми значениями параметров графических примитивов;

4.5. Переходят на начало цикла (п. 4) для обработки следующего контура, если обработанный контур в списке не последний, иначе переходят на п.1, если не все примитивы НАТСН чертежа обработаны.

Список литературы

1. Аль-Шайх Хасан, Лячек Ю.Т. Параметризация конструкторских чертежей // Информационно-управляющие системы. – 2010. – № 1(44). – С. 18-24.

2. Лячек Ю. Т. Геометрическое моделирование. Параметризация и модификация 3D-моделей и чертежей в САПР. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2015. – 160 с.

3. Дж. Г. Алкади Лайс, Ю. Т. Лячек. Параметрическая адаптивная сеточная модель чертежа // Известия СПбГЭТУ «ЛЭТИ». – 2014. – № 6. – С. 44-50.

УДК 004.41

Никитин Петр Владимирович
направление Управление в технических системах
(магистратура), гр. УИТСм-11

Научные руководители:
Горохова Римма Иванова, канд. пед. наук, доцент,
кафедра проектирования и производства ЭВС,
Савинов Александр Николаевич, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ПРОЕКТИРОВАНИЕ ПРОЦЕССА УПРАВЛЕНИЯ WEB-ПОРТАЛОМ НА ОСНОВЕ РАЗРАБОТАННОГО БРИФА

Информационное общество характеризуется как эпоха информационных технологий, в котором нельзя представить организации (будь то

образовательные, коммерческие или государственные) без своего сайта. Наличие своего internet-ресурса в виде сайта подчеркивает успешность и солидность любого образовательного учреждения, дает ей возможность наиболее полно описать вид деятельности и услуги, которые оно предоставляет. В частности, речь идет о web-студиях: интерактивные формы обратной связи, заказ обратного звонка, web-формы – все эти аспекты делают общение между компанией и современным клиентом разнообразным по содержанию и широте контактов.

В процессе разработки web-сайта или какого-либо web-сервиса в сети Интернет обычно написание кода стоит на первом плане и подразумеваются такие технологии для разработки, как HTML, CSS, JavaScript и PHP. В работе над IT-проектом можно выделить наиболее оптимальное и целесообразное разбиение проекта разработки web-сайта на семь основных этапов разработки.

- *Цель создания сайта*. В этом пункте определяются задачи и функции, выполняемые web-сайтом, среди них можно выделить: увеличение продаж, создание сообщества, работа с клиентами, донесение информации и прочее.
- *Тип сайта*. Существует множество разновидностей сайтов: визитка, промо-сайт, портал, интернет-магазин.
- *Примеры понравившихся сайтов*. В данном пункте заказчик перечисляет наиболее понравившиеся сайты и дает комментарии.
- *Требования к дизайну сайта*. Заказчик дает свои рекомендации и пожелания относительно стилистики, цветовой гаммы сайта.
- *Структура сайта*. Одним из важных моментов при разработке web-сайта является обсуждение структуры сайта, так как после верстки изменение структуры сайта осложняется. Поэтому важно перечислить все разделы и страницы, которые планируется разместить на сайте. Необходимо перечислить все разделы меню, рубрики, баннеры, контакты, формы поиска и другие возможные элементы сайта.
- *Особенности функционала сайта*. Здесь описываются пожелания по работе сайта, задачи, которые требуют нестандартного решения.
- *Контент для сайта*. В этом разделе перечисляются все материалы, которые клиент может предоставить для наполнения сайта. К таким материалам относятся: контент для страниц, логотип, баннеры, фотографии, прайс-листы и т. д.

В последнее время широкое распространение приобретают интерактивные web-формы обратной связи, используемые для общего доступа к брифам, нередко оснащенным конструктором для создания брифов.

На сегодняшний день существует как минимум два известных сервиса-конструктора онлайн-брифов, это Briefall и Dodid. В целом оба сервиса практически не отличаются функционалом и схемой работы: создается шаблон брифа и заказчику отправляется ссылка на форму онлайн-брифа, после заполнения web-формы заказчик нажимает на кнопку «Отправить» («Готово»), и форма доступна для просмотра в личном клиенте разработчика. Со стороны заказчика различий функционала в рассмотренных сервисах нет: одинаковая процедура заполнения и отправка на согласование исполнителю (разработчику проекта). Основные отличия находятся в самом конструкторе брифов (см. таблицу).

Различия между сервисами Dodid и Briefall

Dodid	Briefall
Ориентирован на фрилансеров (программистов, дизайнеров, копирайтеров и пр.)	Больше подходит для полноценных web-студий
В сервисе присутствует дополнительная функция ToDo-листа	Сторонний функционал отсутствует
Отсутствует возможность создания шаблона брифа на основе предыдущего, отсутствует вложенность и папки	На основе шаблона создаются брифы для каждого конкретного клиента. Шаблон один, а брифов – три. Присутствуют иерархия и папки
Применимые типы полей: Строка; Текст; Один из списка; Несколько из списка	Применимые типы полей (со временем будет пополняться): Строка; Текст; Один из списка; Несколько из списка; Выпадающий список
Экспорт заполненных брифов в формат .pdf	Экспорт в файл отсутствует, просмотр только через сервис

Таким образом, можно сделать вывод, что оба сервиса нашли свою аудиторию: более простой сервис Dodid больше подходит фрилансерам, а Briefall ориентирован на полноценные web-студии. Однако у этих двух сервисов не хватает интерактивности, а именно возможности двустороннего редактирования как со стороны заказчика, так и со стороны исполнителя-разработчика.

В нашем исследовании разработана еще одна форма брифа. Она похожа на второй вариант, но включает элементы итеративности и двустороннего редактирования, что является более оптимальной формой как для заказчика, так и для разработчика.

Для реализации программного средства нами была выбрана среда программирования NetBeans. Программа позволяет редактировать сразу несколько файлов путем деления экрана на несколько частей. Поддерживаемые операционные системы: Linux, Windows и Mac OS X. В

В результате проделанной работы был выполнен логически завершенный web-конструктор брифов для совместного редактирования в

режиме online. Данный сервис имеет гибкую настройку, а для заказчика сайта сервис будет полезен в первую очередь тем, что заполнение анкеты брифа становится менее трудозатратным и длительным: бриф не требует скачивания формы на компьютер, заполнения в формате документа и дальнейшей отправки заполненного брифа разработчику. Анкета брифа всегда доступна по одной ссылке и для всех сотрудников, у кого есть ссылка, что исключает потери брифа, а также дублирования разных версий брифа в случае, если анкета заполняется несколькими отделами. Данное программное решение позволяет менеджменту компании из любого места оперировать информацией в анкете, следить за внесенными изменениями, а также проверять статус брифа (Н-р «На рассмотрении», «Утвержден» и т.д.). Разработка средства автоматизации выполнена при помощи Rational Rose.

Разработанный web-конструктор брифов имеет следующие достоинства:

1) благодаря совместному редактированию и просмотру анкеты экономится время сотрудников;

2) сокращается число действий при заполнении анкеты брифа;

3) резко сокращается число ошибок и неточностей благодаря типам полей для ответов;

4) точная информация в брифе помогает разработчику более четко понимать задачу, поставленную перед web-студией.

В статье предложен один из вариантов разработки и создания удобного и полезного в первую очередь с точки зрения разработчика сайтов приложения для совместного редактирования online-брифов. К данному приложению были предъявлены такие необходимые требования, как возможность одновременного редактирования и заполнения анкеты брифа, способствование коллективному творчеству, наблюдение за процессом заполнения в динамике и удобного конструктора брифов для различных типов сайта в соответствии со спецификой. При этом было необходимо учесть недостатки аналогичных программ.

Список литературы

1. Айверсон У. Популярные Web-сервисы: практика использования. – М.: Изд-во «Кудиц-Образ», 2014. – 258 с.

2. ISO/IEC BNF Grammar for ISO/IEC 9075-2:2003 - Database Language SQL (SQL-2003) SQL/Foundation [Online]. – ISO/IEC, 07 13, 2003. – URL: http://savage.net.au/SQL/sql-2003-2.bnf.html.

3. Купер А. Проектирование взаимодействия. – М.: Символ-плюс, 2013. – 458 с.

УДК 004.725

Паршин Егор Владимирович
направление Программная инженерия (бакалавриат), гр. ПС-41

Научный руководитель
Бородин Андрей Викторович, канд. экон. наук, профессор,
кафедра информатики и системного программирования
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПОДСИСТЕМЫ МОНИТОРИНГА СОСТОЯНИЯ СЕРВЕРОВ ВРЕМЕНИ SYMMETRICOM СЕРИИ TRUETIME NTS-100

Американская компания Microsemi является лидером на рынке разработки и производства серверов времени. Данная компания – правопреемник компании Symmetricom в части решений по эталонам времени и частоты. Сервера этой компании серии NTS-100 являются вполне доступными (на вторичном рынке) эталонами времени при весьма неплохих характеристиках. В то же время эти изделия предъявляют повышенные требования к качеству антенн в сравнении, например, с доступными решениями другой американской компании – Communication Systems Solutions (CSS). С другой стороны, сервера CSS имеют меньшие функциональные возможности и, главное, существенно уступают серверам компании Symmetricom по идеологии и реализованным механизмам безопасности. Для установки и настройки антенн компания Microsemi (ранее Symmetricom) рекомендует использовать специальное оборудование собственного производства. Стоимость простейшего (минимального) такого комплекта оборудования достигает нескольких десятков тысяч долларов. В связи с этим значительный интерес представляет задача разработки альтернативных инструментов настройки оборудования.

Таким образом, необходимо разработать набор инструментов для получения информации о качестве выбора места установки и настройки приемной антенны по совокупности косвенных признаков, программно доступных в серверах времени компании Symmetricom серии NTS-100.

Рассмотрим основные технические решения, положенные в основу предлагаемой разработки. Для доступа к параметрам состояния сервера времени был выбран стандартный протокол TELNET, поддерживаемый оборудованием сервера на Ethernet-интерфейсе управления.

Основой разработки является специальный демон, собирающий (с заданным интервалом времени) и сохраняющий в базу данных (БД) ряд параметров системы. Каждая запись БД содержит: текущее системное время, булевый признак состояния антенны, булевый признак «захвата» времени, количество «захваченных» сателлитов, признак состояния захвата сателлита и уровень принимаемого сигнала по каждому из каналов, фазу осциллятора, смещение и дневной дрейф частоты осциллятора, ошибку худшего случая отклонения времени из-за дрейфа частоты в условиях недоступности спутников.

Вторым программным продуктом является анализатор «видимости» сателлитов, который для идущих друг за другом промежутков времени заданной длины выполняет следующий алгоритм. На первом этапе для каждой записи БД происходит упорядочивание по возрастанию уровня принимаемого сигнала сателлитов. Затем среди записей БД, соответствующих данному промежутку времени, находится нижняя грань относительно лексикографического порядка на (упорядоченных) массивах уровней. На втором этапе экспертно заданный массив уровней принимаемого сигнала, упорядоченный по возрастанию, проверяется на доминирование вычисленной нижней гранью. Если доминирование обеспечивается с заданным уровнем вероятности на периодах времени не менее суток, то считается, что приемная антенна установлена и настроена правильно, иначе установка и настройка требуют корректировки. Следует отметить, что процедуру такой проверки целесообразно проводить неоднократно: для основных сезонных периодов и в разных погодных условиях.

Третий программный продукт предназначен для исследования временных рядов, представляемых базой данных. Анализ этих временных рядов может проводиться с целью исследования погодной девиации и сезонных колебаний точности эталона, зависимости точности эталона от количества «захваченных» сателлитов и т. п. Также этот программный продукт позволяет рассчитать основные характеристики эталонов для нужд имитационного моделирования систем дистрибуции точного времени в мультисервисных сетях передачи данных (МСПД). Основными рассчитываемыми характеристиками здесь являются вероятности элементарных событий в системе [1]: снижения точности ниже заданного порога, потери синхронизации, отказа системы и т. д. В дальнейшем эти параметры могут быть использованы при оценке совокупной стоимости владения подсистемой синхронизации времени при заданных параметрах [12]. Среди этих параметров могут присутствовать: требуемая дисциплина точности эталона и функция потерь при отклонении от требуе-

мой дисциплины [4]. Для соответствующих расчетов удобно использовать пакет прикладных программ «МультиМИР» [10, 11]. Примеры подобных расчетов приведены в работах [2, 8, 9].

В заключение остановимся на основных полученных результатах. Разработанное программное обеспечение позволяет не только должным образом отладить антенную подсистему эталона времени, но и организовать постоянный мониторинг состояния отдельного сервера времени, а также осуществить интеграцию с системами мониторинга окружающей среды [3, 6].

Дальнейшее развитие проекта связано с реализацией методов анализа очень длинных временных рядов с целью выявления процессов временной деградации эталона и оценки параметров этой деградации. Эффективная оценка параметров временной деградации элементов системы дистрибуции точного времени позволит оптимизировать не только топологию системы, но и график замены оборудования по критерию совокупной стоимости владения МСПД [5, 7]. Также предполагается интеграция описанного программного обеспечения с подсистемами мониторинга состояния среды серверного помещения и погодного мониторинга.

Список литературы

1. Бородин А. В. Теоретико-игровые модели процессов риска над сетями Петри // Моделирование и анализ безопасности и риска в сложных системах: труды международной научной школы МАБР-2006. – СПб.: ГОУ ВПО «СПбГУАП», 2006. – С. 305-307.

2. Бородин А. В. Технико-экономическое обоснование варианта резервирования сетевой компоненты отказоустойчивой масштабируемой вычислительной системы специального назначения // Кибернетика и программирование. – 2015. – № 6. – С. 55-70. – DOI: 10.7256/2306-4196.2015.6.17523.

3. Бородин А. В., Варламов А. С., Кораблев Д. В. Учебно-испытательный полигон отработки технологий дистрибуции точного времени // Кибернетика и программирование. – 2015. – № 3. – С. 11-23. – DOI: 10.7256/2306-4196.2015.3.15438.

4. Бородин А. В. Об импортозамещении при создании систем дистрибуции точного времени в мультисервисных сетях передачи данных // Кибернетика и программирование. – 2015. – № 2. – С. 78-97. – DOI: 10.7256/2306-4196.2015.2.14036.

5. Бородин А. В. Оптимизация стоимости владения объектно-ориентированной метасистемой в условиях заданной модели угроз // Обозрение прикладной и промышленной математики. – 2006. – Т. 13, вып. 5. – С. 843-844.

6. Бородин А. В., Варламов А. С., Кораблев Д. В. Создание учебно-испытательного полигона отработки технологий дистрибуции точного времени в сетях передачи данных // Наука и мир. – 2015. – № 6(22). – Т. 1. – С. 34-37.

7. Бородин А. В. Стоимость владения как критерий архитектуры первичного NTP-сервера на основе GPS-приемников коммерческой точности // Обозрение прикладной и промышленной математики. – 2009. – Т. 16, вып. 3. – С. 507-508.

8. Бородин А. В., Зубьяк Д. Р. Стохастическое моделирование в задачах синтеза оптимальных топологий сетей дистрибуции точного времени // Технические науки – от теории к практике. – №34. – Новосибирск: Ассоциация научных сотрудников «Сибирская академическая книга», 2014. – С. 7-15.

9. Научные ответы на вызовы современности: техника и технологии. Кн. 1 / В. В. Тарасов, Г. П. Кича, А. В. Куликов и др. – Одесса: Куприенко С. В., 2016. – 177 с.

10. Уразаева, Т. А. О функциональности пакета прикладных программ «МультиМИР» // Современные проблемы и перспективы социально-экономического развития предприятий, отраслей, регионов. – Йошкар-Ола: Поволжский государственный технологический университет, 2014. – С. 261-265.

11. Уразаева Т. А. Пакет прикладных программ «МультиМИР»: архитектура и применение // NB: Кибернетика и программирование. – 2014. – № 5. – С. 34-61. – DOI: 10.7256/2306-4196.2014.5.12962.

12. Hornby D., Pepple K. Consolidation in the data center: simplifying IT environments to reduce total cost of ownership. – Santa Clara, CA: Sun Microsystems, 2003. – 205 p.

УДК 004.31

Подоплелов Дмитрий Сергеевич,
Фёдоров Ян Владимирович
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Васяева Елена Семеновна, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

АВТОНОМНЫЙ РОБОТ ДЛЯ ПОДВОДНОГО МОНИТОРИНГА

В последнее время робототехника становится наиболее важным технологическим этапом современного производства. Роботы успешно заменяют тяжелый, утомительный и однообразный труд человека, особенно при работе в условиях вредной или опасной для здоровья среды. Это связано с тем, что робототехническим системам присущи такие

особенности, как высокая точность, отсутствие усталости, беспрерывность цикла работы, возможность применения во вредных и опасных зонах.

Подводная среда относится к таким зонам. Подводные роботы обеспечивают безопасность для человека и простоту при проведении различных исследований в воде. На практике подобные робототехнические системы применяются для исследования океанов, морской флоры и фауны, подводной геологии, поисково-спасательных работ, участия в обследовании и прокладке подводных кабелей, 3D-съемки подводного рельефа.

Для организации подводных исследований существуют следующие решения:

- исследование аквалангистом;
- применение технических систем типа подводных лодок для безопасного перемещения человека под водой;
- использование подводных роботов, управляемых по кабелю или на радиоуправлении.

У каждого из решений имеются свои недостатки: у первого – невозможность применения метода в опасных для человека местах, у второго – высокая стоимость системы, у третьего – необходимость управления и постоянного контроля человеком. Поэтому возникла идея создать подводного робота, не требующего человеческого контроля во время работы.

Целью проекта стало создание автономной системы ориентирования и передвижения в подводных условиях посредством обработки и анализа изображения с камеры и вспомогательных датчиков (давления, инфракрасные и ультразвуковые дальномеры, акселерометр, гироскоп, цифровой компас).

При анализе целей и задач проекта было выяснено, что всю процедуру построения системы можно разделить на несколько частей:

- Конструирование герметичного корпуса и герметизации всей системы.
- Определение метода перемещения системы в подводной среде, подбор подходящих элементов и выбор их расположения.
- Разработка системы погружения и всплытия.
- Разработка системы подводного ориентирования, выбор необходимых контроллеров и прочих элементов для ее реализации.
- Разработка системы передвижения, связывающая систему ориентирования с механической базой, основанной на ПИД-регуляторе, акселерометре, гироскопе и других вспомогательных датчиках.

Основой для разработки робота послужила структура квадрокоптера (рис. 1). В центре системы находится герметичный корпус, в котором установлены все управляющие системы, и другие необходимые объекты, а с четырех сторон находятся роторы, вращающиеся диагонально в противоположных направлениях. Большая популярность квадрокоптеров позволяет с легкостью найти уже готовую платформу, на которой будут расположены все части системы, а их структура упрощает некоторые проблемы: перемещение, балансировка, повороты. Также в Интернете существует большое количество готовых программ для управления подобными системами в открытом доступе, изучение которых способствует быстрой и безошибочной разработке своего решения для управления системой.

Рис. 1. Фото конструкции подводного робота

Первым делом было решено разработать систему движения по линии. Для ее тестирования был построен четырехколесный робот, поскольку сразу в воде тестировать систему будет затруднительно.

В настоящее время реализовано следующее:

- выбраны аппаратные и технические средства для разработки прототипа;
- реализован прототип встраиваемой системы на двух микроконтроллерах Raspberry Pi и ArduinoMega и камеры RaspberryPiCameraBoard (рис. 2);
- разработан программный код для микроконтроллера, реализующий движение системы по линии;
- проведена серия испытаний систем.

Основным контроллером системы является RaspberryPi, который получает и обрабатывает данные с видеокамеры. В результате обработки формируются управляющие сигналы, передаваемые другому кон-

троллеру ArduinoUno. Основная функция этого контроллера заключается в управлении платформой. Для точного движения робота используются алгоритмы ПИД-регулятора, а для обработки изображения – открытая библиотека OpenCV.

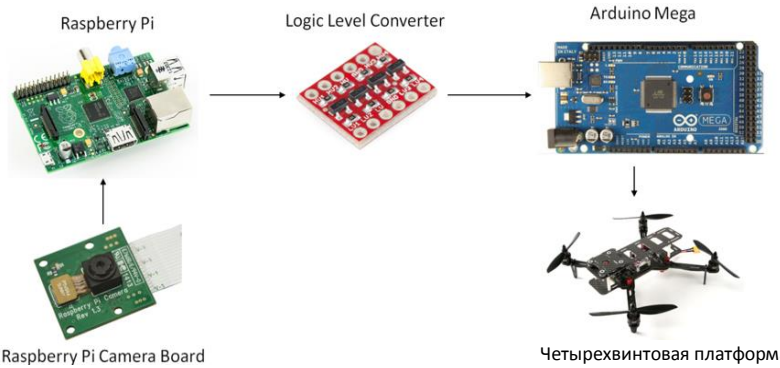


Рис. 2. Структура прототипа системы

Но на этом разработка подводного робота не останавливается, следующим этапом на пути его развития станут разработка алгоритма для обнаружения препятствий и принятия решений в соответствии с текущей обстановкой, алгоритма ориентирования на местности для точного перемещения в необходимую координату и возврата в стартовую позицию. Ведутся также работы по проектировке герметичного корпуса для сохранения и стабильного функционирования всех электронных компонентов системы.

Предложенная разработка может быть использована в опасных для человека местах, имеет небольшую себестоимость, и каждый может внести свой вклад в ее усовершенствование для минимизации человеческого вмешательства в процесс ее работы.

Список литературы

1. Скаскевич А. А., Струк В. А. Основы герметологии: тексты лекций. – Гродно: ГрГУ, 2010. – 140 с.

2. Теория цифровой обработки видеоизображения [Электронный ресурс]. – URL: http://www.malbred.com/obrabotka-video/teoriya-tsifrovoy-obrabotki-videoizobrazheniya/all-pages.html

3. Техническое зрение [Электронный ресурс]. – URL: http://controleng.ru/apparatnye-sredstva/tekhnicheskoe-zrenie/

УДК 004.31

Подоплелов Дмитрий Сергеевич
Федоров Ян Владимирович
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Васяева Наталья Семеновна, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

КОНСТРУКЦИЯ ПОДВОДНОГО АВТОНОМНОГО РОБОТА

Развитие IT-технологий и робототехники все больше и больше внедряется во все сферы производственной и бытовой деятельности человека. Машины, не знающие усталости, заменяют однообразный, тяжелый или опасный труд человека, а их алгоритмы порой позволяют достигать очень высокой, недоступной способности человека точности при выполнении каких-либо заданий. Довольно сложные когда-то задачи теперь с легкостью решаются «умными» роботами.

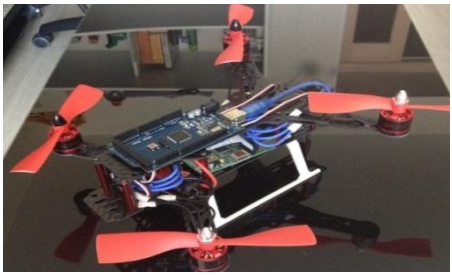
Данная задача была рассмотрена студентами направления информатики и вычислительной техники. Было принято решение о создании подводного автономного робота. Такой робот смог бы помогать человеку при исследовании океанов, морской флоры и фауны, при прокладке подводных кабелей и поиске проблем при их неисправности.

Эта задача не является тривиальной, и поэтому она была разбита на несколько частей. Одна из подзадач – создание конструкции робота. Основная проблема в проектировании подводных систем – это ее герметичность. Все электропроводящие элементы должны быть надежно изолированы от жидкой среды, в которой будут находиться вся конструкция.

Данная конструкция должна состоять из нескольких частей, а именно:

- модульной базы для расположения на ней всех компонентов конструкции;
- основного герметичного корпуса, содержащего блок управления системой и элементы питания;
- вспомогательных герметичных корпусов, содержащих различные датчики, камеры и осветительные приборы;
- роторов и винтов для передвижения системы;
- соединительных элементов, связывающих все части системы, не нарушающих герметичность конструкции.

Основой всей конструкции была выбрана платформа для квадрокоптера (см. рисунок), поскольку имеются уже готовые модульные базы, выбор данного элемента существенно облегчает работы по проектировке топологии робота. Также на самой базе расположена система из четырех специально подготовленных к условиям подводного использования роторов на основе бесколлекторных двигателей с большим крутящим моментом и лопастей с достаточным углом их заклинивания.



Базовая конструкция робота

Для защиты блока управления системами робота и элементов питания от внешних физических факторов (таких как влага и давление воды на глубине) спроектирован основной герметичный корпус, создана ее модель в программе трехмерного моделирования SketchUp для последующей печати на 3D-принтере.

На данном этапе проводятся исследования по разработке соединительных элементов для соединения всех узлов робота, находящихся как внутри герметичных корпусов, так и непосредственно контактирующих элементов с внешними воздействиями среды.

Таким образом, данная конструкция дает возможность упросить изучение и решение проблем в подводной среде без непосредственной человеческой помощи. Главными достоинствами разработки являются доступность материалов и относительно несложная, всем знакомая конструкция.

Список литературы

1. Скаскевич А. А., Струк В. А. Основы герметологии: тексты лекций. – Гродно: ГрГУ, 2010. – 140 с.

2. Теория цифровой обработки видеоизображения [Электронный ресурс]. – URL: http://www.malbred.com/obrabotka-video/teoriya-tsifrovoy-obrabotki-videoizobrazheniya/all-pages.html

3. Техническое зрение [Электронный ресурс]. – URL: http://controleng.ru/apparatnye-sredstva/tekhnicheskoe-zrenie/

УДК 159.9.078

Порядин Антон Евгеньевич
направление Информатика и вычислительная техника (аспирантура)

Научный руководитель:
Сидоркина Ирина Геннадьевна, д-р техн. наук, профессор,
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

КОМПЬЮТЕРНЫЙ МЕТОД ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ АСИММЕТРИИ ВОСПРИЯТИЯ РАЗНОНАПРАВЛЕННОГО ДВИЖЕНИЯ ОБЪЕКТОВ В ДВУМЕРНОМ ПРОСТРАНСТВЕ

Введение

Исследование асимметрии зрительного восприятия – одна из важнейших задач для таких научных областей, как физиология, психология, медицина и многих других. Механизмы, лежащие в основе межполушарной асимметрии головного мозга, до сих пор плохо изучены, их понимание позволит сделать существенный шаг в понимании принципов парной деятельности отделов ЦНС. Проблема получения наиболее объективной и полной информации об асимметрии зрительного восприятия конкретного человека при использовании минимального количества оборудования и в кратчайший промежуток времени возникает во многих областях деятельности человека, будь то профессиональный отбор или профориентация.

Психодиагностика – это один из видов деятельности, определяющий успешность протекания других видов деятельности: коррекции, профилактики и прогноза. Она представляет собой процесс распознавания психологических особенностей отдельного человека или группы людей. Возможность моделирования и оценки зрительной асимметрии (ЗА) позволяет расширить круг использования решения психодиагностических задач для профессионального отбора.

Особенность задач психодиагностики [4] заключается в том, что она включает в себя две составляющие: эмпирическую и априорную. Эмпирическая составляющая представляет собой результат отображения фактов, полученных в процессе решения задач, и может существенно изменяться в ходе диагностического поиска. В самом начале работы она задана неопределенно и не в полном объеме, таким образом относится к области NP-задач и формулируется в ходе исследования. Априорную составляющую психодиагностической задачи образуют знания, имею-

щиеся у эксперта до проведения тестирования, которые требуется реализовать в методе.

Рассмотрим известные методы оценки зрительной асимметрии.

Метод диоптической экспозиции. Суть данного метода заключается в раздельном предъявлении каждому глазу слайда с отличающимся изображением. Обычно используются простые, цветные изображения сюжетного содержания. Для демонстрации слайдов используется стереоскоп, который испытуемый подносит к закрытым глазам, а затем по команде смотрит на изображения. За одну сессию предъявляется до 10 пар слайдов, различающихся между собой по сюжету, контрастности, яркости и цветовой гамме. После просмотра очередной пары слайдов испытуемый должен максимально подробно описать увиденные изображения, уделяя как можно больше внимания пространственному расположению объектов и их цвету. Данный метод предоставляет возможность количественной оценки зрительной асимметрии наряду с качественным анализом. Восприятие всех показанных объектов принимается за 100%. Преобладание в процентном отношении (50% и более) восприятия изображений, предъявляемых правому глазу, является признаком правосторонней асимметрии. Аналогичное утверждение действует и для левого глаза. Слитное восприятие сразу двух слайдов обоими глазами (наложение одного изображения на другое) рассматривается как симметрия монокулярного зрения. Данный метод не реализован в каком-либо программном продукте из-за ряда сложностей в реализации и недостатков:

1) невозможность объективного сопоставления изображения и описания, предоставленного испытуемым без участия специалиста;
2) низкая точность количественной оценки.

Метод определения ведущего глаза при бификсации объекта в пространстве (проба Розенбаха). Этот прием, широко используемый в офтальмологии, является основным методическим приемом для определения ведущего по прицеливанию глаза. Испытуемому предлагается, держа перед глазами карандаш в вытянутой руке и фиксируя его, взором совместить с вертикальным объектом, находящимся на расстоянии 3-5 м. Сначала требуется бинокулярная фиксация этой точки, затем монокулярно левым глазом, затем снова бинокулярно и, наконец, монокулярно – правым глазом. Отмечается, в каком случае монокулярная фиксация совпадает с бинокулярной (карандаш точно накладывается на объект), а в каком – «отходит в сторону» на некоторое расстояние. По совпадению монокулярного показания с бинокулярным можно судить о том, какой глаз является «ведущим». Метод позволяет установить нали-

чие ЗА, но не позволяет произвести количественную оценку. Программная реализация данного метода не требуется из-за простоты его использования. Также недостатком метода является возможность испытуемого исказить результаты эксперимента.

Метод измерения монокулярных полей зрения при помощи периметра Ферстера. Положение головы обследуемого фиксируют на подбородник, в качестве ближнего предмета используют вертикально расположенный стержень на горизонтальной, жестко зафиксированной полуокружности, в качестве дальнего предмета используют вертикальную черту на экране, расположенную за полуокружностью, затем добиваются центральной бинокулярной фиксации объектов, а асимметрию зрения определяют как угловой стереоскопический параллакс моно- и бинокулярного зрения, расстояние от центра средней линии между глазами до ближнего объекта составляет 33 см, до черты на экране 3 м, а размер ближнего объекта 15 см, внешнюю сторону полуокружности для точной фиксации асимметрии зрения градуируют от центра влево и вправо от 0 до 90°, через каждые 5°. Данный метод не реализован в виде программного обеспечения, ввиду использования измерительного оборудования и простого процесса обработки результатов.

Все перечисленные выше методы обладают рядом недостатков:

1) отсутствие реализации в виде программного обеспечения;
2) отсутствие или низкая точность количественной оценки ЗА;
3) субъективность оценки, испытуемый может исказить результаты диагностики (например, заявить о более выгодном для него значении ЗА при профессиональном отборе).

Компьютерные технологии получили широкое распространение и способны упростить процесс диагностики. Учитывая перечисленные недостатки, был предложен метод оценки ЗА, который отличается от перечисленных методов условиями реализации и не имеет указанных недостатков.

Метод оценки функциональной асимметрии через восприятие разнонаправленного движения объектов в двумерном пространстве.

Новизна предлагаемого психофизиологического метода состоит в возможности количественной оценки точности восприятия разнонаправленного движения объектов в двумерном пространстве с возможностью программного моделирования процессов тестирования личности.

Метод реализован в виде программного обеспечения [3]. На данный момент в системе реализованы тесты, основанные на применении различных вариаций направления движения объекта и метки. Обследуемому предъявляют в центре экрана метку и движущиеся слева-направо или

справа-налево с заданной скоростью вертикальные линии, отстоящие друг от друга на заданном расстоянии. Обследуемый, наблюдая за объектами, в момент предполагаемого совпадения положения линий с меткой, нажимает кнопку «Стоп». На момент нажатия кнопки «Стоп» вычисляется ошибка несовпадения положения движущейся линии и метки. После окончания серии вычисляется среднеарифметическое и среднеквадратическое значение несовпадения движущихся линий и метки.

Сопоставление среднеарифметических значений ошибок несовпадения положений движущихся линий и метки при движении линий слева-направо и справа-налево позволяет судить о наличии и величине асимметрии зрительного восприятия движущихся в противоположном направлении линий.

Сопоставление среднеквадратических отклонений ошибок несовпадения положений движущихся линий и метки при движении линий слева-направо и справа-налево позволяет судить о точности реакции на движущиеся линии при противоположном направлении их движения.

В основу априорной составляющей решения данной задачи заложен тот факт, что субъективные ощущения, возникающие у наблюдателя при восприятии набегающего и убегающего движений, имеют принципиальные отличия. Движущийся объект слева-направо или справа-налево для правшей и левшей, у которых естественное движение взгляда противоположно, будет субъективно ощущаться по-разному, так как для одних движущийся объект относительно движения взгляда будет набегающим, а для других – убегающим.

Реализуется модель психосемантики с ограниченной логикой для интерпретации семантики, отличающаяся использованием элементов информационных структур представления измерителей психофизиологических характеристик, используемых для оценки функциональной асимметрии через восприятие разнонаправленного движения объектов в двумерном пространстве.

В результате теоретических и экспериментальных исследований психофизиологических методов и способов оценки функциональной асимметрии центральной нервной системы человека (ЦНС) будут сформулированы основные принципы построения профессиональной интеллектуальной системы [5, 6] для тестирования определенных свойств нервной системы личности, диагностики функциональной асимметрии, обработки результатов для реализации профотбора.

Выводы

Популярные методы оценки ЗА обладают рядом существенных недостатков, таких как субъективность и необходимость в использовании

дополнительного инструментария, а специалисты, в свою очередь, не могут конкурировать с существующими компьютерными технологиями в скорости и точности обработки результатов. Предложенный программный метод, реализованный в среде системы искусственного интеллекта, будет лишен описанных недостатков. Его использование позволит сделать возможным проведение диагностики в удаленных регионах и организациях. Новизна предложенного метода состоит в возможности количественной оценки точности восприятия разнонаправленного движения объектов в двумерном пространстве с возможностью программного моделирования процессов тестирования личности. Использование предложенного метода для профессионального отбора и профориентации позволит быстрее раскрыть индивидуальные технические особенности человека и совершенствовать их на любом этапе профессиональной карьеры.

Список литературы

1. Бердичевская Е. М. Функциональная межполушарная асимметрия и спорт // Функциональная межполушарная асимметрия: хрестоматия. – М.: Научный мир, 2004. – Глава 32. – С. 636-671.

2. Галюк Н. А. Феномен асимметрии зрительного восприятия у человека // Вестник ТГПУ. 2006. №2 – С.5-9.

3. Порядин А. Е. Инструментальные средства оценки психофизиологического состояния человека // Инженерные кадры – будущее инновационной экономики России: материалы Всероссийской студенческой конференции (Йошкар-Ола, 23-28 ноября 2015 года): в 8 ч. Часть 4. Информационные технологии – основа стратегического прорыва в современной промышленности. – Йошкар-Ола: Поволжский государственный технологический университет, 2015. – С. 79–82.

4. Психологическая диагностика: проблемы и исследования / под ред. К. М. Гуревича. – М., 1986.

5. Порядин А. Е. Разработка системы поддержки принятия решений для оценки психологического и психофизиологического состояния человека // Интеллектуальная собственность и современные техника и технологии для развития экономики: материалы III республиканской молодежной научно-практической конференции в рамках Всероссийского студенческого форума «Инженерные кадры – будущее инновационной экономики России» (Йошкар-Ола, 23-28 ноября 2015 года). – Йошкар-Ола: Поволжский государственный технологический университет, 2015. – С. 15–18.

6. Порядин А. Е., Сидоркина И. Г. Комплекс инструментальных средств, реализующих логику оценки психофизиологического состояния человека // Открытые семантические технологии проектирования интеллектуальных систем (OSTIS-2016): материалы VI международной научно-технической конференции (Минск, 18-20 февраля 2016 года). – Минск: БГУИР, 2016. – С. 367-370.

УДК 004.31

Решетников Михаил Андреевич,
Сорокин Андрей Дмитриевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Васяева Наталья Семеновна, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СИСТЕМА ПОГРУЖЕНИЯ АВТОНОМНОГО ПОДВОДНОГО РОБОТА

В данной статье рассматриваются различные системы погружения для автономных подводных роботов.

Отметим три метода погружения классических подводных лодок, адаптируем их для применения в нашем проекте и сделаем выводы об оптимальном решении.

Статический метод погружения

Статический метод погружения робота аналогичен принципу, который используется в настоящих подводных лодках. Этот принцип основан на законе Архимеда и условии плавания тела в жидкости. Для того чтобы лодке погрузиться, необходимо уменьшить ее объем или увеличить массу.

Рис. 1

Динамическое погружение

Динамический погружение – это простой и безопасный способ погрузить подводный робот. Чтобы погрузиться, робот должен поддерживать оптимальную скорость вращения винтов. На лопастях возникает динамическая сила, и, если эта сила больше, чем выталкивающая сила, – робот погружается.

Движение под водой должно происходить за счет изменения скоростей вращения четырех лопастей: движение вперед происходит при увеличении скорости вращения на двух задних винтах, движение назад – на двух передних, движение вправо – при увеличении скорости вращения на двух левых, влево – на двух правых. При уменьшении скорости вращения лопастей робот всплывает на поверхность под действием выталкивающей силы.

Комбинированный метод

Эта система работает вместе с помпой, который заполняет балластный отсек, чтобы частично погрузить робот, и освобождает резервуар для всплытия. Эта система требует, чтобы дрон был на поверхности, когда балластный отсек начнет освобождаться.

Робот должен быть отрегулирован так, чтобы он имел слегка положительную плавучесть, когда балластный отсек заполнен. Принцип погружения точно такой же, как в случае динамического погружения, за исключением того, что эта система позволяет дрону погрузиться намного глубже.

Заполненный отсек уменьшает плавучесть, и это позволяет погрузиться при меньшей скорости вращения лопастей, поэтому такое погружение выглядит более реалистичным. Эта система – гибридный метод между динамическим и статическим погружением.

Рис. 2

Для роботов, предназначенных для соревнований, оптимальным выбором можно считать динамическое погружение, благодаря тому, что это дешевле, и структура робота, выполненная в виде квадрокоптера, делает нецелесообразным использование помпы и балластного отсека. Однако в полевых условиях необходимо использовать балластную систему, обеспечивающую погружение на большую глубину.

Список литературы

1. Блум Дж., Изучаем Arduino: инструменты и методы технического волшебства; пер. с англ. – СПб.: БХВ-Петербург, 2015. – 336 с.

2. Бачинин А., Панкратов В., Накоряков В. Основы программирования микроконтроллеров. – М.: ООО «Амперка», 2013. – 207 с.

3. Васяева Е. С., Васяева Н. С. Специфика обучения школьников основам робототехники // Ресурсы робототехнических конструкций как инструмента воспитания и образования детей и юношества: сборник статей по материалам круглого стола в рамках XIX Вавиловских чтений – международной междисциплинарной научной конференции. – Йошкар-Ола: Поволжский государственный технологический университет, 2016. – С. 88-94.
4. http://ubootmodell.ru/

УДК 004.4

Семенов Владимир Васильевич
направление Информатика и вычислительная техника
(магистратура), гр. ИВТм-22

Научный руководитель
Малашкевич Василий Борисович, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАСПРЕДЕЛЕННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА МОНИТОРИНГА ЛЕСА

Лесные пожары являются мощным природным и антропогенным фактором, существенно изменяющим функционирование и состояние лесов. Лесные пожары наносят урон экологии, экономике, а часто и человеческие жизни оказываются под угрозой. Для стран, где леса занимают большую территорию, лесные пожары являются национальной проблемой, а ущерб, наносимый реальному сектору экономики, исчисляется десятками и сотнями миллионов долларов в год.

Традиционно функции обнаружения лесных пожаров возлагались на сотрудников предприятий лесного хозяйства. Риски человеческого фактора и значительные экономические затраты выявили несовершенство и неэффективность такого подхода к проблеме защиты лесов от пожара.

Системы авиационного наблюдения за лесом оказываются дорогими в эксплуатации и не способны обеспечить постоянный мониторинг больших лесных массивов.

Современные космические системы оптического и теплового видеонаблюдения эффективно обнаруживают развитые очаги горения леса. Недостатком таких систем является сложность раннего обнаружения очагов пожара.

В связи с этим разработка и внедрение современных автоматизированных систем раннего обнаружения очагов возгорания, регистрации пожароопасных ситуаций и реагирования на пожары является актуальной задачей.

Разрабатываемая информационная система – это система наблюдения за лесными массивами, анализа и регистрации лесных пожаров на территории Республики Марий Эл.

Основными задачами системы является автоматическое раннее обнаружение лесных пожаров, определение координат очагов пожара и их привязка к электронной географической карте Республики Марий Эл. Принцип действия системы основан на многопозиционной оптической локации охраняемых территорий, анализе получаемых в процессе локации видеопотоков с целью автоматического обнаружения, регистрации и извещения об очагах пожара.

Основанием для разработки информационной системы является недостаточная эффективность эксплуатируемой в Республике Марий Эл системы мониторинга лесных пожаров «Лесной дозор», права собственности, на которую принадлежат разработчику системы ООО «ДиСи-Кон», г. Нижний Новгород.

К недостаткам имеющейся системы можно отнести следующие:

- система находится в собственности разработчиков, и предоставляется на условиях аренды. При этом заказчик не имеет средств для управления камерами;
- высокая вероятность ложных тревог. Требуется постоянное участие человека-оператора;
- отсутствие интеграции с системами погоды – невозможность предусмотреть развитие пожаров;
- отсутствие интерфейсов для интеграции и внедрения дополнительных сервисов, которые могут предоставить видеонаблюдение;
- отсутствие планирования ресурсов по тушению пожаров.

Разрабатываемая система состоит из программного и аппаратного обеспечения, а также средств связи. В состав системы входит сеть управляемых видеокамер, подключенных к серверам, связанным с компьютерами операторов системы, а также программное обеспечение.

Система имеет клиент-серверную архитектуру. Серверы системы образуют процессинговый центр и решают задачи по сбору, обработке и хранению информации. Основными источниками информации в системе являются потоки видеоданных, поступающие с удаленных точек мониторинга леса по широкополосной сети передачи данных. Клиентами системы являются рабочие места операторов ПК.

Аппаратное обеспечение системы включает оборудование и технические средства, необходимые для видеонаблюдения, организации каналов связи и технического обеспечения системы (видеокамеры, сетевое оборудование, средства вычислительной техники и связи).

Средства видеонаблюдения развертываются над лесными массивами территории Республики Марий Эл. Для их стационарной установки могут использоваться любые высотные сооружения (существующие вышки лесной охраны, вышки операторов связи), обеспечивающие необходимую минимальную высоту установки.

Средства вычислительной техники, входящие в состав системы (серверы) размещаются в серверных помещениях Министерства лесного хозяйства, отвечающих соответствующим требованиям, предъявляемым к подобным помещениям. Рабочие станции, экраны и мониторы отображения информации размещаются на рабочих местах сотрудников Министерства лесного хозяйства.

Программное обеспечение включает в себя операционные системы серверного оборудования и рабочих станций, а также программные модули, реализующие основные функции системы.

Средства связи обеспечивают трансляцию видеопотока, генерируемого удаленными устройствами видеонаблюдения, в центр обработки данных. Каналы связи должны поддерживать стек протоколов TCP/IP и могут арендоваться у провайдеров сетевых услуг – операторов сотовой связи, а также компаний – владельцев линий связи.

К показателям эффективности функционирования системы видеомониторинга возгораний лесных массивов относятся:

- надежность обнаружения очагов возгорания леса при заданном уровне их ложных обнаружений;
- минимальное время формирования и представления оперативной информации;
- минимальное время принятия решения по факту обнаруженных возгораний;
- программное управление маршрутами патрулирования видеокамер и их адаптации по месту расположения, времени суток, календарной дате и условиям освещения;
- возможность автоматического изменения маршрутов патрулирования видеокамер по командам системы автоматического обнаружения очагов возгорания;
- возможность ручного управления маршрутами патрулирования видеокамер по командам оператора;

- точность определения географических координат очагов возгораний;
- сведение к минимуму «человеческого» фактора при патрулировании и видеомониторинге возгораний лесных массивов;
- экономическая эффективность, достигаемая при внедрении разрабатываемой системы за счет снижения потерь от лесных и природных пожаров.

Основные функции разрабатываемой системы:

- автоматический видеомониторинг лесных массивов;
- автоматическое раннее обнаружение очагов возгорания;
- автоматическое управление маршрутом оптической локации каждой видеокамеры;
- определение координат возгораний с привязкой их к электронным картам местности;
- автоматическое ведение архива видеозаписей и протоколирование событий, возникающих в системе, с целью электронного документирования потенциально опасных явлений;
- создание детальных и сводных отчетов о работе системы за указанный период в форме твердых бумажных документов, фотокопий и файлов видеозаписей;
- обеспечение доступа пользователей к функциям системы в соответствии с назначенными правами;
- планирование ресурсов для тушения обнаруженного пожара;
- интеграции со службой погоды для предсказания развития пожара.

Основными потребителями системы выступают: лесопользователи, администрации населённых пунктов, МЧС, заповедники, предприятия (нефтегазовые компании), объекты которых проходят через лес, расположенные вблизи лесов военные объекты, атомные станции, исследовательские центры; госпредприятия, на которые возложена охрана леса, в том числе от лесных пожаров.

Список литературы

1. Шестаков М. Ю., Созданов А. И. Система мониторинга состояния территориально-распределенных объектов контроля [Электронный ресурс]. – URL: http://bankpatentov.ru/node/51509

2. Горяченков М. С. Задача дистанционного мониторинга и управления группой распределенных аппаратных объектов [Электронный ресурс]. – URL: http://bolid.ru/support/articles/articles_13.html

3. Макаров О. В. Теория и практика разработки систем мониторинга [Электронный ресурс]. – URL: http://idp-cs.net/article11.php?num=11#z00

УДК 004.93

Семенов Дмитрий Альбертович
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-21

Научный руководитель
Ипатов Юрий Аркадьевич, канд. техн. наук, доцент,
кафедра информатики
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИССЛЕДОВАНИЕ И МОДЕЛИРОВАНИЕ ЗАДАЧИ О РЮКЗАКЕ

Задача о рюкзаке является хорошо изученной и исследованной NP-полной задачей с множеством прикладных применений [1]. Так, существуют алгоритмы решения этой задачи, которые для большинства входных данных эффективно находят приемлемый ответ в зависимости от заданного критерия оптимальности [2]. Существует несколько модификаций задачи:

1) каждый предмет можно брать только один раз;
2) каждый предмет можно брать сколько угодно раз;
3) каждый предмет можно брать определенное количество раз;
4) на размер рюкзака имеется несколько ограничений;
5) некоторые вещи имею больший приоритет, чем другие.

Для исследования рассмотрим классическую постановку задачи [3]. Имеется набор из N предметов, каждый предмет имеет массу Wi и полезность Vi, i = (1,2..N). Требуется собрать набор с максимальной полезностью таким образом, чтобы он имел вес не больше W, где W – вместимость ранца. Традиционно полагают, что W_i , V_i , W, P – целые неотрицательные числа.

Существуют точные и приближенные методы решения этой задачи. К точным методам относятся: полный перебор, метод ветвей и границ, динамическое программирование. К приближенным: жадные алгоритмы. Полный перебор – перебор всех вариантов (всех состояний) – малоэффективный, но точный метод. Метод ветвей и границ – по сути сокращение полного перебора с отсечением заведомо «плохих» решений. Динамическое программирование – алгоритм, основанный на принципе оптимальности Беллмана. Жадный алгоритм – основан на нахождении относительно хорошего и «дешевого» решения.

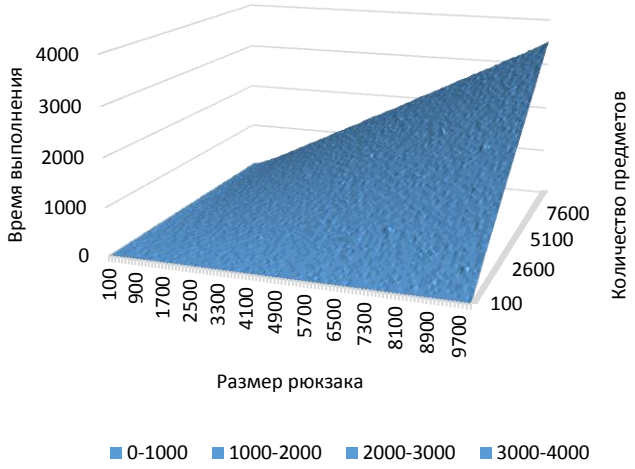


Рис. 1. Тестовая конфигурация ПК-1

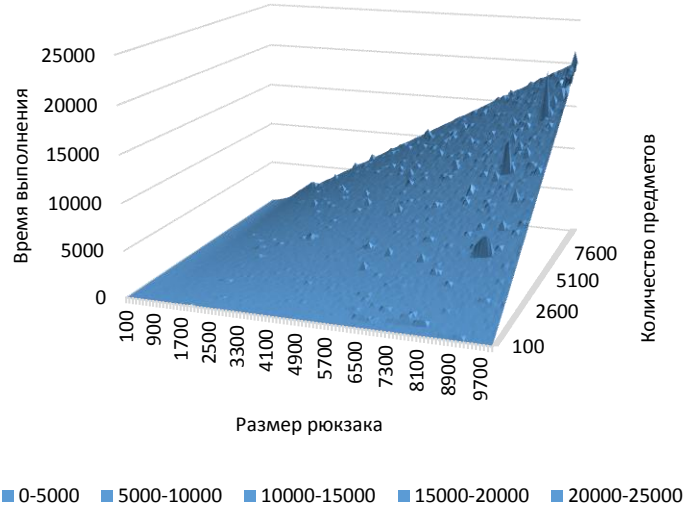


Рис. 2. Тестовая конфигурация ПК-2

Для исследования временной сложности и вычислительной эффективности был реализован алгоритм с использованием метода динамического программирования [4]. При этом для анализа скорости работы были построены трехмерные графики, которые отражают эффективность программной реализации алгоритма. На рисунках 1 и 2 представлены зависимости – размера рюкзака (кг), количества предметов (шт.) и времени расчёта оптимального набора.

В таблице представлены аппаратные характеристики вычислителей на которых проводились эксперименты. Можно сделать вывод, что первая конфигурация (ПК-1) в пять раз большей вычислительной эффективностью для этого класса задач по сравнению с ПК-2. При этом можно заметить, что тактовая частота процессора отличается незначительно. Главными отличительными особенностями высокой производительности ПК-1 являются её архитектура [5], скорость работы оперативной памяти, а также увеличенный кэш второго уровня.

Конфигурация ПК-1	Конфигурация ПК-2
Intel(R) Celeron(R) CPU 1000M @ 1.80GHz	Intel(R) Atom(TM) CPU N450 @ 1.66GHz
Ядра: 2	Ядра: 1
L1 - 128 КБ	L1 - 56 КБ
L2 - 512 КБ	L2 - 512 КБ
L3 - 2,0 МБ	-
RAM - 2,0 ГБ DDR3	RAM - 2,0 ГБ DDR2
Частота RAM - 1600 МГц	Частота RAM - 667 МГц

В целом можно сделать такой вывод: рассмотренный метод эффективно решает поставленную задачу и может быть использован в широком классе прикладных областей.

Список литературы

1. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. – М.: Мир, 1982.

2. Pisinger D. Algorithms for Knapsack Problems // PhD thesis. University of Copenhagen, 1995.

3. Окулов С. М., Пестов А. А., Пестов О. А. Информатика в задачах. – Киров: Изд-во ВГПУ, 1998. – 343 с.

4. Окулов С. М., Пестов О. А. Динамическое программирование // Развитие интеллекта школьников. – М.: БИНОМ. Лаборатория знаний, 2012. – 296 с.

5. Scott Mueller Upgrading and Repairing PCs, 22 Edition – Que Publishing, 2015. – 1428 p.

УДК 003.26

Сивачев Алексей Вячеславович,
аспирант

Научный руководитель
Прохожев Николай Николаевич, канд. техн. наук, доцент,
кафедра проектирования и безопасности компьютерных систем
ФГАОУ ВО НИУ «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»,
г. Санкт-Петербург

ПРИМЕНЕНИЕ СТАТИСТИЧЕСКИХ МЕТОДОВ ПРОСТРАНСТВЕННОЙ ОБЛАСТИ СТЕГАНОАНАЛИЗА ДЛЯ ОБНАРУЖЕНИЯ ВСТРАИВАНИЯ ИНФОРМАЦИИ В ОБЛАСТЬ ДВП ИЗОБРАЖЕНИЯ

На сегодняшний день одним из наиболее динамично развивающихся направлений стеганографии является встраивание информации в область дискретного вейвлет-преобразования (ДВП) изображения, что вызвано использованием данного преобразования в основе стандарта JPEG2000. Разработка средств стеганоанализа для ДВП области несколько отстает, и к настоящему времени ощущается острый дефицит эффективных средств в этой области. При этом модель низкочастотной области ДВП (LL) имеет значительную корреляцию с пространственной областью цифрового изображения.

В данной статье рассматривается возможность использования существующих методов статистического стеганоанализа [1], разработанных для обнаружения стеганографического воздействия на пространственную область и показавших для нее хорошие результаты [7], для обнаружения факта встраивания в область коэффициентов ДВП.

В общем случае встраивания информации в область ДВП, заключается в модификации коэффициентов ДВП одной или нескольких плоскостей таких коэффициентов, получаемых в результате одно- или многоуровневого двумерного ДВП [2].

В данной работе для моделирования стеганографического воздействия использовались плоскости коэффициентов, получаемых при одноуровневом ДВП. Воздействию подвергалась только одна из плоскостей коэффициентов (LL, HL, LH или HH). Моделирование стеганографического воздействия производилось путем изменения значений младших значащих бит (МЗБ) в коэффициентах.

Для экспериментов была использована коллекция [3], состоящая из 10000 изображений разрешением 512x512. Оценка эффективности методов производилась посредством анализа статистики результатов применения пространственных методов количественного стеганоанализа при различных значениях полезной нагрузки стеганоконтейнера. Для исследований были выбраны наиболее эффективные из современных методов статистического количественного стеганоалализа:

- RS-analysis [4];
- Sample pair analysis [5];
- Triplesanalysis [6].

Результатом работы данных статистических методов является оценка количества пикселей изображения, подвергшихся стеганографическому воздействию в области МЗБв процентах от объема контейнера. В данной работе вместо значений пикселей использовались значения коэффициентов ДВП. Полезная нагрузка составляла 0 % (оригинальное изображение), 5 % и 10 % от общего количества коэффициентов ДВП. Значения среднего арифметического и среднеквадратичного отклонений приведены в таблице.

Таблица 1 – **Значения среднеарифметического и среднеквадратичного отклонений при анализе различных областей изображения с помощью методов статистического стеганоанализа при полезной нагрузке 10 %**

Тип изображения, анализ. область	Среднеарифметическое			Среднеквадратическое		
	RS	SPA	TR	RS	SPA	TR
Ориг., LL область	0.85	0.32	-5.10	2.89	1.80	14.04
Стего., LL область	10.84	8.66	3.34	2.79	1.21	16.04
Ориг., LH область	72.25	19.99	9.91	11.42	2.14	23.89
Стего., LH область	73.89	21.57	7.98	8.71	1.24	27.93
Ориг., HL область	62.11	21.16	-17.13	10.16	2.09	34.53
Стего., HL область	64.55	22.50	-17.45	8.31	1.23	36.88
Ориг., HH область	73.55	20.66	4.43	10.83	2.04	26.74
Стего., HH область	74.54	22.07	2.21	8.56	1.19	30.74
Ориг., изображения	-0.10	-0.21	-1.09	1.44	1.60	5.60
Стего., изображения (встр.во все области)	1.05	0.67	-0.32	1.58	1.16	4.78

Результаты показывают, что алгоритмы стеганоанализа пространственной области имеют неприемлемую погрешность для плоскостей высокочастотных коэффициентов ДВПLH, HL и HH. Для плоскости низкочастотных коэффициентов ДВП (LL) погрешность ожидаемо меньше.

Рассматривая количественные результаты методов стеганоанализа как входные данные для бинарного классификатора и изменяя порог

срабатывания, можно получить представление об эффективности обнаружения факта стеганографического воздействия в ДВП области цифровых изображений. Для более детальной оценки эффективности рассматриваемых методов для LL плоскости воспользуемся построенным на основе экспериментальных данных графиком доверительных областей (ROCcurve) для полезной нагрузки в 5 % и 10 %, приведенным на рисунке.

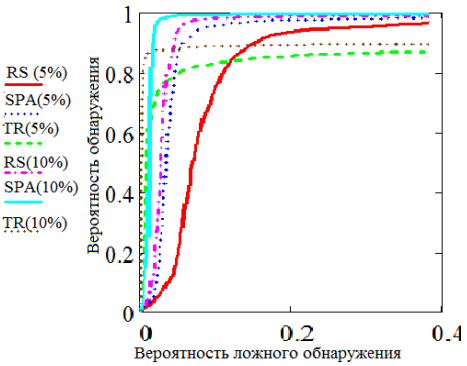


График доверительных областей для детектирования встраивания в LL плоскость

График доверительных областей (см. рисунок) демонстрирует, что при анализе LL области возможно добиться высокой вероятности обнаружения факта стеганографического воздействия (более 95 %) при относительно низкой вероятности ложного обнаружения (менее 5 %).

Таким образом, применение статистических методов стеганоанализа, разработанных для пространственной области, имеет смысл только для обнаружения факта встраивания в LL плоскость области ДВП. Для обнаружения факта встраивания в высокочастотные области LH, HL и HH статистические методы количественного стеганоанализа пространственных областей не пригодны.

Список литературы

1. Nissar A., Mir A. H. Classification of steganalysis techniques: A study // Digital Signal Processing. – 2010. – Vol. 20. – Pp. 1758–1770.

2. Gayathri C., Kalpana V. Study on image steganography techniques // International Journal of Engineering and Technology (IJET). – 2013. – Vol. 5. – Pp. 572-577.

3. BOWS2 the 10 000 original images [Electronic resource] / Break our watermarking system. – 2-nd edition. – URL: http://bows2.ec-lille.fr/ (date of access 17.07.2016).

4. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images // IEEE Multimedia. – 2001. – Vol. 8. – Pp. 22-28.

5. Lu P., X. Luo et. al. An improved sample pairs method for detection of LSB embedding // Proc. of the 6th Information Hiding Workshop, Springer LNCS. – 2004. – Vol. 3200. – Pp. 116-128.

6. Ker A. D. A general framework for structural steganalysis of LSB Replacement // Proc. of the Information Hiding. – 2005. – Pp. 296-311.

7. Исследование эффективности применения статистических алгоритмов количественного стеганоанализа в задаче детектирования скрытых каналов передачи информации / Н. Н. Прохожев, О. В. Михайличенко, Д. А. Башмаков, А. В. Сивачев, А. Г. Коробейников // Программные системы и вычислительные методы. – 2015. – № 3. – С. 281-292.

УДК 004.056.55

Скворцова Наталья Олеговна
направление Информатика и вычислительная техника
(магистратура), гр. ИВТм-11

Научный руководитель
Чекулаева Елена Николаевна, канд. экон. наук, доцент,
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ЗАЩИТА ИНФОРМАЦИОННЫХ ПОТОКОВ НА ПРЕДПРИЯТИИ

Целью исследования является анализ основных методов защиты информации на предприятии, а также возможностей учесть различные варианты защиты данных и обеспечить полную их конфиденциальность на любом предприятии.

Информационными потоками называют физические перемещения информации от одного сотрудника предприятия к другому или от одного подразделения к другому.

Система информационных потоков – это совокупность всех физических перемещений информации. Такая система дает возможность осуществить какой-либо процесс и реализовать какое-либо решение. Наиболее общая система информационных потоков – это сумма потоков информации, которая позволяет вести предприятию финансово-хозяйственную деятельность. Информационные потоки

обеспечивают нормальную работу организации (рис. 1). Цель работы с информационными потоками – максимальная оптимизация работы предприятия [5].

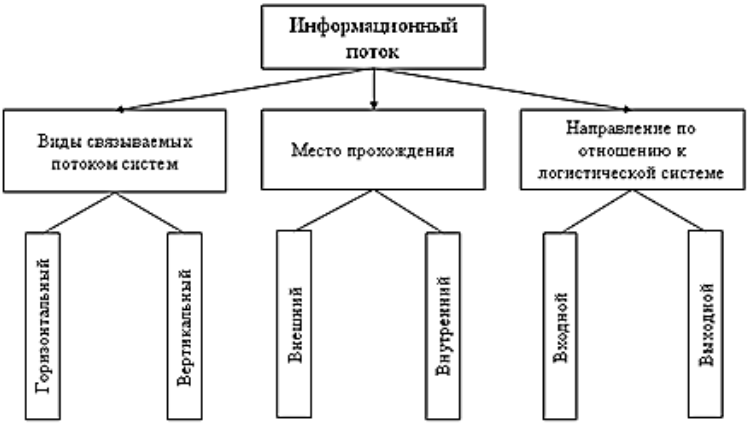


Рис. 1. Внутренние информационные потоки

Внутри ИС выделяются следующие информационные потоки:

- передача файлов между файловыми серверами и пользовательскими рабочими станциями по протоколу SMB (протокол открытого обмена информацией между АРМ пользователей и серверами на основе стека TCP/IP);
- передача сообщений электронной почты посредством использования хешированного соединения программного обеспечения Lotus Notes;
- передача юридической и справочной информации между серверами БД и пользовательскими рабочими станциями;
- деловая переписка;
- передача отчетной информации;
- передача бухгалтерской информации между пользовательскими рабочими станциями и сервером БД в рамках автоматизированных систем «1С Бухгалтерия», «1С Зарплата и Кадры», «Оперативный учет».

При использовании модели нарушителя для анализа возможных угроз информационной безопасности необходимо учитывать возможность сговора между внутренними и внешними нарушителями.

Среди всего набора методов защиты информации выделяют следующие (рис. 2):

Рис 2. Классификация методов защиты информации

К методам и средствам организационной защиты информации относятся *организационно-технические* и *организационно-правовые* мероприятия, используемые в процессе создания и эксплуатации КС для обеспечения защиты информации. Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будут размещаться компьютеры; проектировании системы, монтаже и наладке ее технических и программных средств; испытаниях и проверке работоспособности компьютерной системы.

Инженерно-техническая защита (ИТЗ) – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

Многообразие целей, задач, объектов защиты и проводимых мероприятий предполагает рассмотрение некоторой системы классификации средств по виду, ориентации и другим характеристикам.

Физические средства защиты – это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников. К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

К аппаратным средствам защиты информации относятся самые различные по принципу действия, устройству и возможностям технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации.

В программной защите информации можно выделить следующие направления использования программ для обеспечения безопасности конфиденциальной информации, в частности такие:

1) защита информации от несанкционированной доступа;

2) защита информации от копирования;

3) защита программ от копирования;

4) защита программ от вирусов;

5) защита информации от вирусов;

6) программная защита каналов связи.

Криптографический метод защиты должен обеспечить такую защиту секретной (или любой другой) информации, что даже в случае ее перехвата посторонними лицами и обработки любыми способами с использованием самых быстродействующих ЭВМ и последних достижений науки и техники она не должна быть дешифрована в течение нескольких десятков лет. Для такого преобразования информации используются различные шифровальные средства – такие, как средства шифрования документов, в том числе и портативного исполнения, средства шифрования речи (телефонных и радиопереговоров), телеграфных сообщений и передачи данных [6].

В заключение хочется отметить, что для обеспечения безопасности данных информационного ресурса предприятия необходимо учесть все возможные варианты защиты данных и обеспечить полную конфиденциальность данных на предприятии. Тем самым защита информационных потоков – это комплекс мероприятий, направленных на обеспечение информационной безопасности, которая в свою очередь обеспечит предприятию необходимый аспект ведения бизнеса в условиях агрессивной рыночной экономики.

Список литературы

1. Биячуев Т. А. Безопасность корпоративных сетей. – СПб.: СПб ГУ ИТМО, 2008. – 161 с.

2. Мельников В. Защита информации в компьютерных системах. – М.: Финансы и статистика, Электронинформ, 2007. – 400 с.

3. http://bbcont.ru/business/informacionnye-potoki-predpriyatii-i-metody-ih-issledovaniya.html

4. http://www.plam.ru/compinet/osnovy_informatiki_uchebnik_dlja_vuzov/p12.php

УДК 681.3.06

Соколов Михаил Владимирович
направление Информационная безопасность (магистратура), гр. БИм-21

Научный руководитель
Леухин Анатолий Николаевич, д-р физ.-мат. наук, профессор,
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ТЕСТЫ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, РАЗРАБОТАННОЕ ДЛЯ ОЦЕНКИ ИХ СТАТИСТИЧЕСКИХ СВОЙСТВ

Введение

Псевдослучайная последовательность – последовательность чисел, которая была вычислена по некоторому определенному арифметическому правилу, но имеет все свойства случайной последовательности чисел в рамках решаемой задачи. Генераторы псевдослучайных последовательностей являются важнейшими элементами любой системы защиты, надежность последовательностей в значительной степени зависит от свойств используемых генераторов. Качественные псевдослучайные последовательности, являясь по своей сути детерминированными, имеют практически все свойства реализаций истинно случайных процессов и успешно заменяют их, так как истинно случайные последовательности чрезвычайно сложно формировать.

Тестирование генераторов случайных и псевдослучайных чисел, используемых в криптографических алгоритмах, является актуальной задачей как в практическом, так и в теоретическом плане. Несмотря на значительные наработки в этой области, разработчики все же нуждаются в функциональном инструментарии, способном дать оптимальный результат, который позволит достаточно четко исследовать степень случайности последовательностей, полученных с помощью генераторов псевдослучайных последовательностей, и представить аналитикам весь объем данных, необходимых для оценки «качества» генератора.

На сегодняшний день разработано значительное количество генераторов псевдослучайных последовательностей. Для оценки их статистических свойств применялись различные методы статистического тестирования. Чаще всего набор и методику тестирования предлагал сам разработчик генератора. В результате сложилась ситуация, характеризую-

щаяся тем, что довольно проблематично объективно оценить разные генераторы в рамках единых стандартов. Выходом из этой проблемы является применение единой стандартной подборки статистических тестов, объединенных методом расчета необходимых свойств генераторов псевдослучайных последовательностей и принятия решения о случайности генерируемых последовательностей.

Разнообразие методов оценки псевдослучайных последовательностей, применяемых при шифровании, довольно велико. Подходы к анализу последовательностей можно разделить на две группы.

Первая группа опирается на нахождение закономерностей, позволяющих повторить шифрующую последовательность на основе малого количества информации. Главные требования сводятся к отсутствию в псевдослучайной последовательности простых межзнаковых зависимостей.

Вторая группа опирается на оценку статистических свойств последовательности: есть ли в анализируемой последовательности частотный дисбаланс, позволяющий аналитику предугадать значение следующего бита с вероятностью, большей 0,5. При этом свойства псевдослучайной последовательности должны быть приближены к свойствам истинно случайной последовательности, например в псевдослучайной последовательности равномерно распределены не только отдельные знаки, но и m-граммы, т.е. набор m соседних знаков, m = 1,2,… .

Обе эти группы методов анализа последовательностей составляют системный подход к разработке поточных шифров и тестов, предназначенных для выявления различного рода дефектов в исследуемых псевдослучайных последовательностях.

Обзор существующих методик тестирования

В настоящее время для тестирования псевдослучайной последовательности разработаны программные продукты, которые содержат наборы тестов для оценки статистических свойств. В США был стандартизирован набор статистических тестов путем принятия в 1994 г. национального стандарта «Требования безопасности к криптографическим модулям». Они призваны для решения задачи статистического контроля используемых в криптографических алгоритмах псевдослучайных последовательностей и в общем случае не подходят для решения задач анализа статистических свойств генераторов псевдослучайных последовательностей. Тесты Diehard – это набор статистических тестов для анализа качества набора случайных чисел. Вместе они рассматриваются как один из наиболее строгих существующих наборов тестов.

В 1999 г. специалистами Национального института стандартов и технологий (НИСТ США), в рамках проекта AES (Advanced Encryption Standard) был разработан набор статистических тестов «НИСТ STS» (НИСТ Statistical Test Suite) и предложена методика проведения статистического тестирования ГСЧ (ГПСЧ), нацеленных на использование в задачах криптографической защиты информации, которая в настоящее время наилучшим образом отвечает требованиям всех заинтересованных сторон.

Пакет НИСТ STS включает в себя 15 статистических тестов, разработанных для проверки гипотезы о случайности двоичных последовательностей произвольной длины, получаемых в генераторах псевдослучайных последовательностей. Основной принцип тестирования – проверка нулевой гипотезы H0, заключающейся в том, что тестируемая последовательность является случайной. Альтернативной гипотезой На служит гипотеза о том, что тестируемая последовательность не случайна. По результатам применения каждого теста нулевая гипотеза либо подтверждается, либо нет. Решение о том, будет ли заданная последовательность нулей и единиц случайной или нет, принимается по совокупности результатов всех тестов.

Описание разработанного программного средства

Для исследования статистической безопасности алгоритмов генерации псевдослучайных последовательностей и криптоалгоритмов разработано программное средство, написанное на языке высокого уровня Python. Разработанное ПО представляет универсальную систему оценки качества статистических свойств бинарных последовательностей в симметричных системах шифрования. ПО является кросс-платформенным способном работать на ОС семейства Windows и GNU Linux, а также многих других.

Разработанное программное средство легко интегрируется во многие современные операционные системы, позволяет провести оценку статистической безопасности наиболее известных и используемых в симметричных криптосистемах генераторов псевдослучайных последовательностей. ПО может использоваться как библиотека и встраиваться непосредственно в криптоалгоритмы для проведения самотестирования.

С помощью разработанного ПО было проведено сравнение времени выполнения тестов на сгенерированной последовательности, которое выявило уменьшение времени, затраченного на обработку, по сравнению с взятым за основу программным средством НИСТ (см. таблицу).

В ходе проведенных исследований и тестирований бинарных последовательностей было выявлено, что практически каждый отдельно взятый оценочный тест можно «обмануть», т. е. заставить признать слу-

чайной заведомо некачественную последовательность, поэтому данный набор тестов используется в комплексе и негативное прохождение одного из текстов бракует последовательность вне зависимости от того, что остальные тесты могли быть пройдены положительно.

Тест	Время, затраченное на обработку	
	Разработанное ПО	Программа НИСТ
Частотный тест	0,35	0,54
Проверка кумулятивных сумм	0,48	0,65
Проверка «дырок в последовательностях	2,03	2,47
Проверка «дырок»	0,99	1,44
Проверка рангов матриц	14,53	18,87
Спектральный тест	97,67	146,53
Проверка непересекающихся шаблонов	345,11	430,49
Прверка пересекающихся шаблонов	12,5	14,60
Универсальный статистический тест Маурера	546,32	651,27
Проверка случайных отклонений	76,50	85,60
Разновидность проверки случайных отклонений	30,97	36,15
Проверка аппроксимированной энтропии	1,59	1,87
Проверка серий	8,95	10,39
Сжатие при помощи алгоритма Лемпела-Зива	2,25	2,41

Заключение

Ввиду увеличивающейся информатизации во всех сферах жизнедеятельности проблема обеспечения защиты информации будет продолжать играть главенствующую роль в этом процессе. Криптография как часть системы защиты информации развивается, разрабатываются и внедряются новые методы шифрования данных, но неизменным остаётся то, что в криптоалгоритмах используются генераторы псевдослучайных последовательностей. Поэтому и тестирование псевдослучайных последовательностей в частности, и генераторов последовательностей в целом, и оценка их статистических свойств будут оставаться актуальными вопросами для специалистов, работающих в данной области.

Список литературы

1. Коробейников А. Г., Гатчин Ю. А. Математические основы криптологии: учебное пособие. – СПб.: СПб ГУ ИТМО, 2004. – 106 с. илл.
2. Recommendation for Random Number Generation Using
3. Deterministic Random Bit Generators (англ.) NIST SP 800-90.
4. Statistical Testing of Random Number Generators (англ.)
5. Proceedings of the 22nd National Information Systems Security.
6. Conference, 10/99.
7. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (англ.) NIST SP 800-22.

УДК 004.056.55

Сокольников Алексей Михайлович
аспирант кафедры информационной безопасности

Научный руководитель
Сидоркина Ирина Геннадьевна, д-р техн. наук, профессор
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

АНАЛИЗ И СРАВНЕНИЕ СИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ ДЛЯ ЗАЩИТЫ E-LEARNING КУРСОВ В ХРАНИЛИЩЕ ДАННЫХ СИСТЕМЫ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Введение

Проблема защиты информации от несанкционированного доступа была актуальна во все времена [2]. Популяризация протокола передачи данных HTTPS, поддерживающего шифрование, значительно снизила вероятность атак, основанных на прослушивании сетевого трафика, однако помимо безопасной передачи данных при разработке современной системы хранения данных для СДО стоит брать во внимание безопасность хранения файлов на сервере.

Задача обеспечения безопасности хранения данных для системы дистанционного обучения имеет крайне высокий приоритет, так как, по результатам опросов разработчиков курсов E-Learning, профессионально сделанный обучающий курс продолжительностью в 1 час обходится конечному клиенту в $10, 000 [3].

Одним из вариантов обеспечения безопасного хранения данных на сервере является шифрование файлов. Выбор алгоритма шифрования коррелирует со временем выполнения операции и стойкостью подбора ключа. Следует брать во внимание тот факт, что шифрование не гарантирует полную недоступность содержимого для третьих лиц, поскольку ключ шифрования может быть подобран, к примеру, методом полного перебора [4].

Обоснование выбора вида криптосистемы для шифрования курсов в СДО iSpringLearn

Алгоритмы шифрования и расшифровывания данных используются для сокрытия конфиденциальной информации от третьих лиц. Главным принципом в них является условие, что передатчиком и реципиентом

заранее определены алгоритм шифрования и ключ, без знания которых информация будет предоставлять из себя лишь набор символов, не имеющий смысла.

В настоящее время выделяют два наиболее популярных вида криптосистем: симметричные и асимметричные криптосистемы.

Ключевой особенностью *симметричных криптосистем* является использование одного и того же ключа для шифрования и расшифровывания данных.

Асимметричные криптосистемы, в отличие от симметричных, имеют 2 ключа: публичный и приватный. Публичный ключ передается по открытому для третьих лиц каналу и используется для проверки цифровой подписи и шифрования сообщений. Для генерации цифровой подписи и расшифровывания сообщений используется приватный ключ. Данный подход широко применяется в сетевых протоколах, к примеру, HTTPS.

По сравнению с асимметричными криптосистемами, симметричные имеют ряд преимуществ:

- во-первых, благодаря простоте операций, выполняемых при шифровании, достигается большая скорость и упрощается реализация алгоритмов;
- во-вторых, при сопоставимой стойкости требуется меньшая длина ключа;
- в-третьих, за счет того, что симметричные алгоритмы появились раньше асимметричных, они более изучены.

Основным недостатком симметричных систем является сложность передачи ключей, поскольку каждый участник для расшифровки должен обладать одинаковым ключом. В рамках задачи организации хранения обучающих курсов для СДО, вышеописанный недостаток не станет играть значительной роли, поскольку ключ не будет передаваться по каналам.

СДО при загрузке обучающего курса на сервер пересылает данные через микросервис [5] шифрования, находящийся на отдельной машине, далее происходит его шифрование, и уже зашифрованный курс переправляется в файловое хранилище, как это показано на рисунке 1. Таким образом, благодаря использованию микросервисной архитектуры удаётся избежать главного недостатка симметричных криптосистем – открытой передачи ключа, поскольку ключ никуда не передается, а хранится лишь на стороне микросервиса шифрования файлов.

Вынесение процесса шифрования в микросервис на отдельном сервере делает взлом хранилища файлов бессмысленным, поскольку ника-

кой информации о содержимом исходного файла хранилище иметь не будет. На вход оно получает лишь некий зашифрованный набор данных, не имеющий ценности без знания ключа и алгоритма шифрования.

Помимо этого, микросервис шифрования файлов исключает из обработки запросы, пришедшие с непроверенных источников (не от СДО), что повышает устойчивость системы ко внешним взломам.

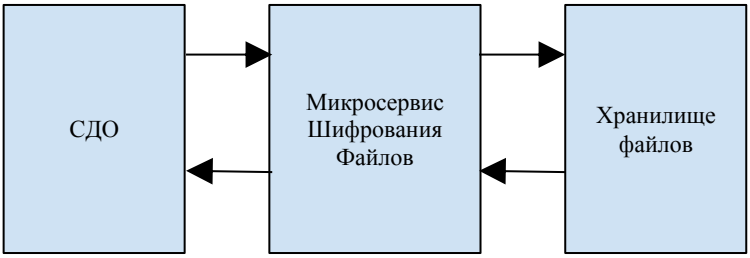


Рис. 1. Схематическое изображение структуры СДО, отвечающей за шифрование и хранение файла

Исходя из вышеописанных доводов, при использовании микросервисной архитектуры для шифрования обучающих курсов в СДО выгоднее использовать симметричные алгоритмы шифрования. Выгода в данном случае достигается за счет увеличения скорости работы и простоты реализации алгоритмов.

Алгоритм симметричного шифрования AES

AdvancedEncryptionStandart (AES) – алгоритм симметричного блочного шифрования. Размер блока равен 128 бит, длина ключа варьируется от 128 до 256 бит. Алгоритм принят как стандарт шифрования Соединенных Штатов Америки. По состоянию на 2009 год AES – наиболее распространенный алгоритм симметричного шифрования [6]. AES использует подстановочно-перестановочную сеть, являющуюся альтернативой сети Фейстеля.

Для AES длина input (блока входных данных) и State (состояния) постоянна и равна 128 бит, а длина шифроключа **K** составляет 128, 192, или 256 бит. При этом исходный алгоритм допускает длину ключа и размер блока от 128 до 256 бит с шагом в 32 бита. Для обозначения выбранных длин input, State и CipherKey в 32-битных словах используется нотация Nb = 4 для input и State, Nk = 4, 6, 8 для CipherKey соответственно для разных длин ключей.

В начале шифрования input копируется в массив State по правилу $\mathrm{state}[r, c] = \mathrm{input}[r + 4c]$, для $0 \leq r < 4$ и $0 \leq c < Nb$.

В итоге, после завершения последнего раунда трансформации, State копируется в output по правилу $\mathrm{output}[r + 4c] = \mathrm{state}[r, c]$, для $0 \leq r < 4$ и $0 \leq c < Nb$.

Алгоритм симметричного шифрования ГОСТ Р 34.12-2015 (Кузнечик)

ГОСТ Р 34.12-2015 – алгоритм симметричного блочного шифрования. Размер блока равен 128 бит, и длина ключа равна 256 бит, для генерации используется сеть Фейстеля, состоящая из ячеек, на вход которым поступают ключ и данные для шифрования. На выходе из каждой ячейки получаются измененные данные и измененный ключ. Данный шифр утвержден в качестве стандарта в 2015 году.

Алгоритм генерации ключа использует итерационные константы $C_i = H(Bin_{128}(i))$, i=1,2,…32. Задается общий ключ $K = k_{255}||\ldots||k_0$.

Вычисляются итерационные ключи:

$K_1 = k_{255}||\ldots||k_{128}$

$K_2 = k_{127}||\ldots||k_0$

$(K_{2i+1}, K_{2i+2}) = F[C_{8(i-1)+8}]\ldots$

$F[C_{8(i-1)+1}](K_{2i+1}, K_{2i}), i = 1, 2, 3, 4.$

Алгоритм шифрования:

$E(a) = Add_2[K_{10}]HNAdd_2[K_9]\ldots$

$HNAdd_2[K_2]HNAdd_2[K_1](a)$, где *a* – строка размером 128 бит.

Алгоритм дешифрования:

$D(a) = Add_2[K_1]H^{-1}N^{-1}Add_2[K_2]\ldots$

$H^{-1}N^{-1}Add_2[K_9]H^{-1}N^{-1}Add_2[K_{10}](a).$

Сравнение алгоритмов ГОСТ Р 34.12-2015 и AES

Сравнение по скорости шифрования 128-битных строк

Сравнение алгоритмов шифрования производилось в несколько этапов.

На 1 этапе происходило сравнение скорости шифрования сообщения размером в 16 байт (128 бит) при длине ключа шифрования в 32 байта (256 бит) для алгоритмов AES и ГОСТ Р 34.12-2015. Для исключения статистических ошибок каждый алгоритм запускался 50 итераций на разных случайных строках одинаковой длины.

Пример функции шифрования и дешифрования случайного сообщения для алгоритма AES представлен в листинге 1:

deftest_aes_dec():

message= Random.get_random_bytes(16)

key= Random.get_random_bytes(32)

```
iv= Random.get_random_bytes(16)
encryptor= AES.new(key, AES.MODE_CBC, iv)

crypt_start= time.time()
crypted_message= encryptor.encrypt(message)
crypt_dif= time.time() - crypt_start
print("crypted ", crypt_dif)

encrypt_start= time.time()
encryptor.decrypt(crypted_message)
encrypt_dif= time.time() - encrypt_start
print("encrypted ", encrypt_dif)
```

Листинг 1. Генерация, шифрование и расшифровка сообщения длиной 16 байт

По результатам замеров минимальная скорость шифрования 16-байтного сообщения для алгоритма ГОСТ Р 34.12-2015 составляет 0,0009496 секунд. Для алгоритма AES эта метрика составляет 0,0000012.

Общую картину измерений скорости шифрования можно увидеть на рисунке 2.

Рис. 2. Время шифрования сообщения длиной 16 байт
для алгоритмов AES и ГОСТ Р 34.12-2015

Сравнение скорости шифрования файлов популярных в СДО форматов

Для проведения второго этапа сравнения алгоритмов шифрования был проведен анализ использования, применяющий анонимные данные

клиентов СДО iSpringLearn, и выявлены популярные типы файлов, используемые для обучения. По результатам данного анализа для участия в сравнении были выбраны: презентации PowerPoint, видео в формате mp4, аудио в формате mp3.

Был реализован прототип сервиса шифрования, принимающего на вход файл и выдающего его зашифрованную версию. В целях избегания порчи информации по завершении операций шифрования и расшифровки вычислялись и сравнивались контрольные суммы для исходного и расшифрованного файлов.

Пример функции шифрования файла алгоритмом ГОСТ Р 34.12-2015 представлен в листинге 2:

```
@classmethod
defencrypt(self, key, in_filename, out_filename):
chunk_size= self.get_block_size()
if not out_filename:
out_filename= in_filename+ '.enc'

encryptor= gost2015(list(key))
file_size= os.path.getsize(in_filename)

withopen(in_filename, 'rb') as infile:
withopen(out_filename, 'wb') as outfile:
outfile.write(struct.pack('<Q', file_size))

while True:
chunk= infile.read(chunk_size)
iflen(chunk) == 0:
break
eliflen(chunk) % chunk_size!= 0:
chunk+= b' '* (chunk_size- len(chunk) % chunk_size)

outfile.write(bytes(encryptor.encryption(list(chunk))))
```

Листинг 2. Функция шифрования файла алгоритмом ГОСТ Р 34.12-2015

Чтение файла происходит в бинарном режиме, на каждой итерации цикла читаются блоки фиксированного размера (блока для шифрования), происходит их шифрование и запись в итоговый файл. Данный подход экономит ресурсы вычислительной машины, поскольку файл читается не целиком, а частями.

Исходные данные файлов:

- Изображение jpg – 2.4 мб
- Презентация pptx – 1.7 мб
- Видео mp4 – 20.7 мб
- Аудио mp3 – 8.9 мб

Результаты времени работы по шифрованию файлов алгоритмами ГОСТ Р 34.12-2015 и AES в секундах представлены в таблице 1.

Таблица 1 – **Время шифрования файлов в секундах**

Алгоритм	jpg	pptx	mp4	mp3
AES шифрование	0,257	0,181	2,214	0,941
AES расшифровка	0,206	0,148	1,784	0,784
ГОСТ Р 34.12-2015 шифрование	148,653	176,311	2000,040	547,329
ГОСТ Р 34.12-2015 расшифровка	156,599	178,817	2104,815	584,848

Из результатов видно, что с увеличением объема файла расхождение в скорости шифрования между рассматриваемыми алгоритмами наблюдается более выражено.

Влияние предварительной архивации файла на скорость шифрования

Один из вариантов увеличения скорости шифрования файла – уменьшение его размера. Выигрыш в скорости будет достигнут лишь в том случае, когда время на архивацию файла в сумме с шифрованием будет меньше времени шифрования исходного файла. В целях проверки был реализовано сжатие файлов методом zip перед их шифрованием.

Результаты времени шифрования архивированных файлов представлены в таблице 2.

Таблица 2 – **Время шифрования архивированных файлов в секундах**

Алгоритм	jpg(архив)	pptx(архив)	mp4(архив)	mp3(архив)
AES шифрование	0,255	0,173	2,179	0,943
AES расшифровка	0,205	0,143	1,760	0,749
ГОСТ Р 34.12-2015 шифрование	149,5	162,582	1982,088	562,692
ГОСТ Р 34.12-2015 расшифровка	155,080	154,141	2084,584	601,084

Время, потраченное на создание zip-архива, представлено в таблице 3.

Таблица 3 – **Время создания zip-файла из архива**

Тип файла	Время (секунды)
jpg	0,082
pptx	0,124
mp4	0,681
mp3	0,321

Анализ результатов

Основываясь на данных из таблиц 1-3, можно сказать, что архивация файлов перед шифрованием не дает весомого прироста в скорости шифрования. Данные, полученные экспериментальным путем, говорят о том, что в большинстве случаев сумма времени архивации и последующего шифрования архива превышает время шифрования исходного файла.

Опираясь на данные, представленные в таблицах 1, 2, можно утверждать, что скорость работы алгоритма AES значительно превышает ГОСТ Р 34.12-2015.

Во-первых, это может быть связано со сложностью работы библиотек Python 3 с сетями Фейстеля, т.к. на выходе каждой ячейки сети получаются изменённые данные и изменённый ключ. Все ячейки однотипны, и сеть представляет собой определённую итерированную структуру. Ключ меняется при переходе от одной ячейки к другой.

Во-вторых, ГОСТ Р 34.12-2015 – относительно новый стандарт шифрования и не поддерживается стандартными библиотеками, в отличие от AES. Для его использования приходится разрабатывать собственную реализацию алгоритма либо пользоваться решениями с открытым исходным кодом, однако правильность и оптимальность таких решений не гарантируется. В отличие от ГОСТ Р 34.12-2015, принятого как стандарт в 2015 году, AES был объявлен стандартом шифрования в 2002 году. За это время AES стал одним из самых популярных алгоритмов симметричного шифрования. В 2007 году компанией Intel была введена его поддержка на аппаратном уровне, что значительно увеличивает его скорость работы при использовании соответствующих библиотек.

Автор не исключает, что при должной популяризации и поддержке алгоритма ГОСТ Р 34.12-2015 можно добиться более качественной реализации, а следовательно, и увеличения скорости его работы и потребления ресурсов. На текущий момент найти открытую для использования реализацию алгоритма ГОСТ Р 34.12-2015, способную конкурировать с AES по скорости работы и качеству реализации, не представляется возможным, а значит использование его для шифрования обучающих курсов на сегодняшний день не даст никакого преимущества, по сравнению с AES.

Список литературы

1. Сокольников А. М., Сидоркина И. Г. Решение задачи прогнозирования возрастания нагрузки в системе дистанционного обучения «ISPRING LEARN» // Открытые семантические технологии проектирования интеллектуальных систем = OpenSemanticTechnologiesforIntelligentSystems (OSTIS-2015): материалы V

междунар. науч.-техн. конф. (Минск, 19-21 февраля 2015 года) / редкол.: В. В. Голенков (отв. ред.) [и др.]. – Минск: БГУИР, 2015. – С. 593-596.

2. Скубилин М. Д. О программной диверсификации/репликации информации [Электронный ресурс] // Известия ЮФУ. Технические науки. – 2000. – № 1. – URL: http://cyberleninka.ru/article/n/o-programmnoy-diversifikatsii-replikatsii-informatsii (дата обращения 22.05.2016)

3. http://www.tagoras.com/cost-to-create-e-learning/

4. Christof Paarэ Understanding Cryptography / 2010, Jan Pelzl.

5. Сокольников А. М. Сравнительный анализ подходов к разработке архитектуры и систем управления базами данных для высоконагруженных WEB-сервисов // NB: Кибернетика и программирование. – 2014. – № 4. – С. 1-13. – DOI: 10.7256/2306-4196.2014.4.12800. – URL: http://e-notabene.ru/kp/article_12800.html

6. Biryukov A., Khovratovich D. Related-key Cryptanalysis of the Full AES-192 and AES-256 // Advances in Cryptology – ASIACRYPT 2009. – Springer Berlin / Heidelberg, 2009. – Vol. 5912. – P. 1-18. – DOI:10.1007/978-3-642-10366-7_1

УДК 004.7

Сорокин Андрей Дмитриевич,
Решетников Михаил Андреевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Малашкевич Василий Борисович, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИНДИВИДУАЛЬНАЯ СИСТЕМА КОНТРОЛЯ КАЧЕСТВА ТОВАРОВ

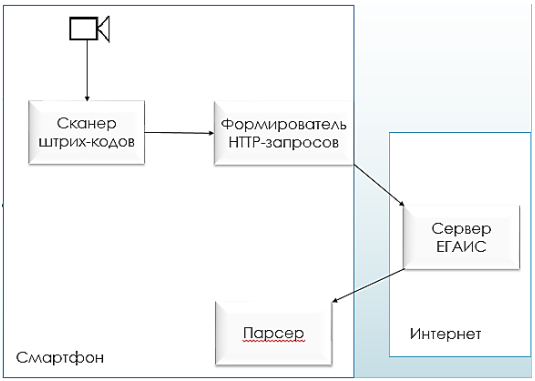
Одной из серьезных проблем потребительского рынка России является подделка и фальсификация товаров. Например, доля контрафактной алкогольной продукции на российском рынке оценивается в 40 %. Сложная ситуация складывается также с торговлей меховыми изделиями и лекарствами. Для борьбы с этой проблемой создана и запущена в эксплуатацию Единая государственная автоматизированная информационная система (ЕГАИС) [1], обеспечивающая идентификацию каждой легально выпущенной емкости с алкоголем. Аналогичные системы планируются к запуску для контроля рынка шубных изделий и дорогостоящих лекарств. Однако для использования этих систем рядовым потре-

бителям необходим выход в Интернет и ручной ввод данных о контролируемой продукции.

Для контроля рынка алкоголя в России создано приложение «Анти-Контрафакт Алко» [2] для мобильных устройств. Это приложение выполняет контроль покупки на основе QR-кода, считанного с чека оплаты покупки. Такой подход позволяет провести контроль товара только после оплаты покупки. Другие подобные приложения [3] выполняют только считывание и расшифровку штрих-кодов акцизных марок, не обеспечивая контроля их достоверности. Таким образом, остается актуальной задача независимого индивидуального контроля алкогольной продукции непосредственно на полке магазина.

Разрабатываемая система автоматизирует процесс контроля алкогольной продукции, обеспечивает проведение контроля до факта оплаты покупки, а также обеспечивает ряд дополнительных сервисов.

Разрабатываемая система контроля реализуется на аппаратной платформе смартфона. Современные смартфоны имеют в составе оборудования видеокамеры с высоким разрешением изображения, а также могут использовать мобильные подключения к Интернету. Таким образом, аппаратура смартфона имеет все необходимое для работы разрабатываемого приложения. Структурная схема системы представлена на рисунке.



Структурная схема системы контроля качества

Считывание данных о товаре выполняется с помощью встроенной камеры смартфона. Полученное изображение акцизной марки и штрих-кода дешифрируется программным сканером штрих-кода.

Данные о товаре, извлеченные сканером, преобразуются в HTTP-запрос к серверу ЕГАИС в соответствии с форматом, требуемым серве-

ром. Сервер ЕГАИС в своем HTTP-ответе сообщает результаты контроля товара, которые остается только отобразить на экране смартфона. Пользователю остается только принять решение о соответствии выбранного товара наклеенной акцизной марке законности продажи выбранного товара.

Приложение также способно предложить ряд дополнительных функций:

- возможность отправить жалобу на товар в государственные органы;
- рассылка предупреждений списку друзей, если вы наткнулись на контрафакт;
- оценка опьянения в зависимости от физиологических особенностей организма, количества выпитого алкоголя и съеденной закуски;
- расчет примерного времени отрезвления, основанный на гендерном признаке, массе тела, росте, количестве выпитого и скорости выведения алкоголя из организма;
- мини-игры по тематике (данная функция поможет весело провести время на корпоративах и праздниках).

Продукт реализуется в среде программирования Intel XDK по технологии HTML5/JS, которая обеспечивает кроссплатформенность приложения. Поэтому разрабатываемое приложение готово к установке на любой смартфон, операционная система которого имеет компонент WebView.

Данный продукт будет интересен значительной части населения России, а реализация на основных мобильных операционных системах предоставит возможность пользоваться приложением каждому обладателю смартфона, которых в России более 50 млн человек.

Прямые продажи приложения представляются малоперспективными, вследствие неготовности российских пользователей оплачивать программы. Наиболее эффективный способ монетизации – получение оплаты за размещение рекламы в составе приложения [4]. Поэтому в России лучше распространять приложение по условно-бесплатной схеме, зарабатывая на размещении рекламы в приложении и обновления списка особенностей программы (мини-игр и прочего). Платная версия программы будет активироваться через ежемесячную покупку премиум-аккаунта, в такой пакет будет также входить и отключение рекламы.

Список литературы

1. В России заработало приложение для определения контрафактного алкоголя [Электронный ресурс]. – 2016. – URL: http://yamobi.ru/posts/v_rossii_ zarabotalo_prilojenie_dlya_opredeleniya_kontrafaktnogo_.html (дата обращения 28.10.2016).

2. АнтиКонтрафакт Алко [Электронный ресурс]. – 2016. – URL: https://play.google.com/store/apps/details?id=ru.fsrar.anticontrafact (дата обращения 28.10.2016).
3. Алкоголь Сканер [Электронный ресурс]. – 2016. – URL: https://play.google.com/store/apps/details?id=ru.guesswho.egaisqr (дата обращения 28.10.2016).
4. Маркетинг → Монетизация приложения [Электронный ресурс]. – 2015. – URL: https://habrahabr.ru/company/appodeal/blog/294682/ (дата обращения 28.11.2016).

УДК 004*422

Сорокин Олег Леонидович
направление Информатика и вычислительная техника,
направленность Системы автоматизации проектирования (аспирантура)

Научный руководитель
Сидоркина Ирина Геннадьевна, д-р техн. наук, профессор,
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СИСТЕМА ОПРЕДЕЛЕНИЯ ВЕЛИЧИНЫ ПОГРЕШНОСТИ ФАКТИЧЕСКИХ ТЕМПЕРАТУРНЫХ ЗНАЧЕНИЙ В ОГРАЖДАЮЩИХ КОНСТРУКЦИЯХ

Рассматривается проблема определения величины погрешности температурных значений в ограждающих конструкциях стен зданий и сооружений с целью их корректировки. Определение данной погрешности без использования системы особенно затруднено при резких изменениях температурных условий, так как при аналитических расчетах учитываются только фактические данные о состоянии ограждающих конструкций без учета прогнозов. Внедрение разработанной системы в составе средств систем автоматизированного проектирования (САПР) позволит избежать проблемы некорректного определения температуры в конструкции, а также при применении ее на стадии проектирования здания поможет наиболее точно подобрать тепловые узлы и нагреватели для поддержания оптимальных климатических условий в помещении, а также повысить энергоэффективность работы тепловых пунктов.

Актуальность разработанной системы обусловлена значительным повышением требований к уровню теплозащиты зданий, согласно изменениям строительных норм и правил (СНиП 2-3-79).

Согласно данным требованиям температура на поверхности ограждающей конструкции $t_{в,}$ должна быть выше температуры точки росы, но

не менее чем на 2-3 °С. В ходе анализа данных с лабораторных установок по сбору температурных значений [1] были обнаружены расхождения между аналитическими расчетами и реальными температурными значениями в толще ограждения.

В дальнейшем при расчете данной ошибки на различных сечениях конструкции были обнаружены ряд закономерностей, связанных с типовыми значениями ошибок, и возможности их прогнозирования, требующие также дополнительного формализованного описания. Таким формализованным описанием в системе являются значения величины ошибок аналитических расчетов в сравнении с практическими значениями с установок по сбору температурных данных.

Одно из наиболее важных практических значений разработанной системы заключается в соблюдении микроклимата и санитарно-гигиенических требований [2], предъявляемых к ограждающим конструкциям. Нарушение таких требований зачастую происходит при резком изменении внешних воздействий, так как аналитические расчеты с физической точки зрения их не учитывают, другими словами – отсутствует элемент прогнозирования таких резких скачков, что в результате приводит к нарушению описанных выше норм [2].

Модули, направленные на расчет данных аналитических значений [3], также выдают результаты с большой величиной погрешности, что не является допустимым и может привести к снижению термосопротивления конструкции с течением времени.

Характер распределения температуры на границе условных слоев τ_{xi} представлен на рисунке 1.

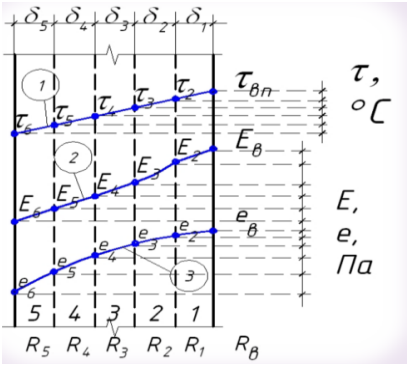


Рис. 1. Значения распределения температурных значений, рассчитанные аналитическим способом

Рассмотрим значения данных с лабораторной установки на 1.11.2014 (рис. 2) и 1.06.2015 (рис. 3), детектированные практическим методом, и сравним с аналитическими расчетами.

Рис. 2. Демонстрация работы системы определения величины погрешности фактических температурных значений в ограждающих конструкциях, характер распределения температуры на 1.11.2014, детектированный с лабораторной установки № 1

Рис. 3. Демонстрация системы определения величины погрешности фактических температурных значений в ограждающих конструкциях, характер распределения температуры на 1.06.2015, детектированный с лабораторной установки №1

Исходя из построенных графиков температурных значений, можно сделать вывод о нелинейном распределении температур в определенные дни. Характер распределения величины ошибки по слоям между практическими значениями и аналитическими расчетами представлен на рисунке 4.

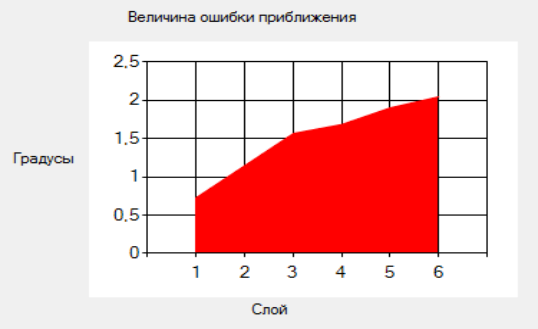


Рис. 4. Демонстрация работы системы определения величины погрешности фактических температурных значений в ограждающих конструкциях, характер распределения величины ошибки между практическими значениями и аналитическими расчетами по выбранным слоям на 1.11.2014

Таким образом, доказано нарушение норм в 2-3°С [1], что может привести к выпадению конденсата, нарушению санитарных норм, снижению срока службы конструкции и ее теплофизических свойств.

Разработанная система определения величины погрешности фактических температурных значений в ограждающих конструкциях в составе САПР решает ряд проблем, связанных с обеспечением необходимого уровня теплозащиты зданий, позволяет избежать нарушения санитарных норм, обеспечивает более длительный срок службы конструкции и сохранение его теплофизических свойств. Эффективность и необходимость внедрения данного типа систем на различных этапах проектирования зданий и сооружений, а также как надстройку к современным типам автоматизированных систем обусловлена сокращением времени на расчеты, более высокой точностью, автоматизацией сопутствующих параметров, связанных с утеплителями конструкции, а также возможностью учесть взаимосвязь и влияние последних на итоговый поправочный коэффициент.

Список литературы

1. Сорокин О. Л., Сидоркина И. Г. Анализ представления пользовательской информации в приборе «терем-4» для измерителя температуры ограждающих

конструкций // Кибернетика и программирование. – 2015. – № 5. – С. 193-198. – DOI: 10.7256/2306-4196.2015.5.16950. – URL: http://e-notabene.ru/kp/article_16950.html

2. Строительные нормы и правила Российской Федерации. Свод правил «Проектирование тепловой защиты зданий»: СП 23-101-2004. – М.: Технорматив, 2013.

3. Сорокин О. Л., Сидоркина И. Г. Модуль определения стационарного режима в САПР наружных инженерных сетей // «IS&IT–Интеллектуальные САПР 2015»: труды конгресса по интеллектуальным системам и информационным технологиям. – Таганрог: Изд-во ЮФУ, 2015. – Т. 1. – С. 70-75.

УДК 004*422

Сорокин Олег Леонидович
направление Информатика и вычислительная техника (аспирантура),
направленность Системы автоматизации проектирования.

Научный руководитель
Сидоркина Ирина Геннадьевна, д-р техн. наук, профессор,
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ЭЛЕМЕНТЫ ТЕХНОЛОГИИ УТОЧНЕНИЯ ВИЗУАЛИЗАЦИИ РАСПРЕДЕЛЕНИЯ ТЕПЛОВЫХ ПОТОКОВ В ОГРАЖДАЮЩИХ КОНСТРУКЦИЯХ

Введение

Рассмотрим элементы технологии визуализации распределения тепловых потоков с целью их уточнения и изучения влияния типа конструкции на характер распределения температуры. Исследование распределения тепловых потоков необходимо при резких изменениях температурных условий, так как при аналитических расчетах учитываются только фактические данные о состоянии ограждающих конструкций без учета прогнозов. Внедрение элементов технологии в составе средств систем автоматизированного проектирования (САПР) позволит избежать проблемы некорректного определения температуры в самой конструкции, а также при применении их на стадии проектирования здания позволит наиболее точно подобрать тепловые узлы и нагреватели для поддержания оптимальных климатических условий в помещении и повысить энергоэффективность работы тепловых пунктов.

1. Уточнение характера распределения тепловых потоков в ограждающих конструкциях

В ходе исследования влияния типа конструкции и резких температурных скачков при расчете значения поправки для уточнения характера распределения тепловых потоков на различных сечениях конструкции были обнаружены ряд закономерностей, связанных с типовыми значениями ошибок, и возможности их прогнозирования, требующих также дополнительного описания [1]. Нарушение таких требований зачастую происходит при резком изменении внешних воздействий, так как аналитические расчеты с физической точки зрения их не учитывают, то есть отсутствует элемент прогнозирования таких резких скачков, что в результате приводит к нарушению этих норм.

Рассмотрим пример, когда температура наружного воздуха изменяется на восемь и более градусов в течение нескольких суток. Сопоставляя результаты аналитических расчетов, без прогнозирования и без учета внешних изменяющихся температурных условий (рис. 1), а также с использованием элементов технологии на их основе для уточнения характера тепловых потоков (рис. 2), можно сделать вывод о накоплении недопустимых значений ошибки. Значение каждой из волн от обогревателя к ограждающей конструкции соответствует понижению температуры воздуха на пять градусов.

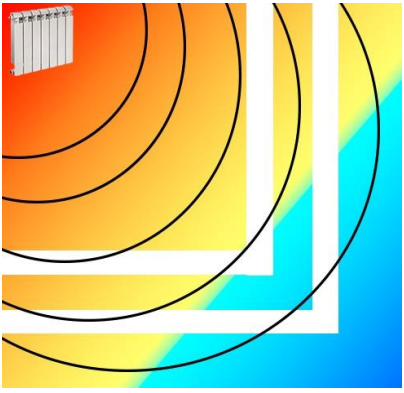


Рис. 1. Распределение тепловых потоков в ограждающих конструкциях и помещении без использования уточнения визуализации

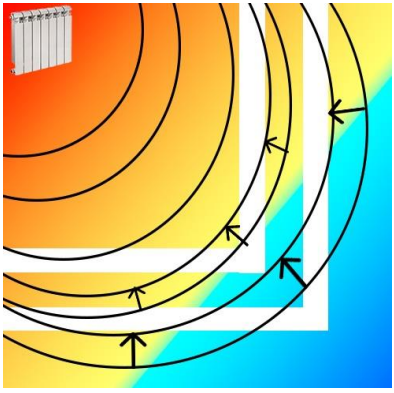


Рис. 2. Распределение тепловых потоков в ограждающих конструкциях и помещении с использованием уточнения визуализации

2. Внедрение интеллектуального прогнозирования как компоненты технологии уточнения визуализации тепловых потоков

На основе проведенных расчетов было предложено решение данной проблемы, заключающееся во внедрении поправочных коэффициентов для каждого выделенного слоя. Значения коэффициентов не фиксированы и напрямую зависят от температурных условий, температурного пояса, прогнозов о скачках температуры на основе накопленных статистических данных [1], а также зависят от конкретного слоя, который требуется рассмотреть, поскольку аналитический метод расчета подразумевает накопление ошибки по слоям.

На рисунке 3 показана основная составляющая элементов технологии уточнения визуализации тепловых потоков различного типа с внедрением интеллектуального прогнозирования при неполноте данных об изменении внешней среды с использованием баз знаний и правил [2].

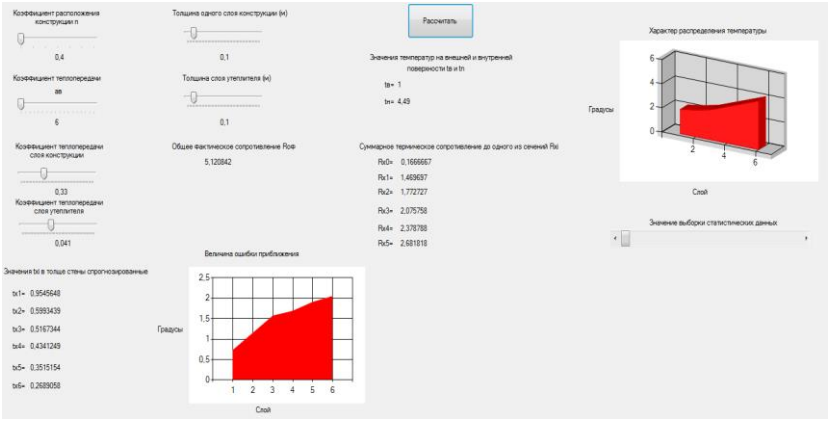


Рис. 3. Внедрение прогнозирования для определения характера распределения тепловых потоков по слоям в случае введения неполных или неточных данных

Использование прогнозирования при недостатке информации о характере распределения тепловых потоков в ограждающих конструкциях позволит подобрать уточнения для каждого из слоев с максимальной точностью, что дает возможность наиболее точно подобрать тип ограждающей конструкции и ее свойства для каждой конкретной инженерной сети.

Вывод

Включение в состав технологии интеллектуального прогнозирования позволит провести визуализацию тепловых потоков в ограждающих

конструкциях даже при недостаточном количестве статистической информации, что может быть использовано в инженерных сетях для снижения общего времени на проектирование.

Список литературы

1. Сорокин О. Л., Сидоркина И. Г. Анализ представления пользовательской информации в приборе «Терем-4» для измерителя температуры ограждающих конструкций // Кибернетика и программирование. – 2015. – № 5. – С. 193-198.

2. Сорокин О. Л., Сидоркина И. Г. Алгоритмы обработки информации в адаптивном реконфигурируемом модуле САПР ОК для визуализации контуров тепловых потоков // «OSTIS-2016» Открытые семантические технологии проектирования интеллектуальных систем. – Минск: БГУИР, 2016. – С. 431-435.

УДК 621.396.7

Сунгуров Александр Анатольевич
направление Информатика и вычислительная техника
(магистратура), гр. ИВТм-21

Научный руководитель
Смирнов Алексей Владимирович, канд. техн. наук, доцент,
кафедра информационно вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ (RFID) НАПРАВЛЕННОГО ДЕЙСТВИЯ С ПРИМЕНЕНИЕМ УСОВЕРШЕНСТВОВАННОЙ ТЕХНОЛОГИИ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ ДЛЯ ПАССИВНЫХ РАДИОМЕТОК

Рассматривается разработка программно-аппаратного комплекса радиочастотной идентификации с применением усовершенствованной технологии радиочастотной идентификации для пассивных радиометок.

Технология RFID (RadioFrequencyIdentification – радиочастотная идентификация) – это технология, основанная на использовании радиочастотного электромагнитного излучения.

RFID-метка представляет собой миниатюрное запоминающее устройство. Она состоит из микрочипа, который хранит информацию, и

антенны, с помощью которой метка эти данные передает и получает. Иногда RFID-метка имеет собственный источник питания (такие метки называют активными), но большинство меток его лишены (эти метки называют пассивными). В памяти RFID-метки хранятся уникальный номер и пользовательская информация. Когда метка попадает в зону регистрации, эта информация принимается считывателем, специальным прибором, способным читать и записывать информацию в метках. Максимальная дистанция, которую способны обеспечивать современные пассивные RFID-комплексы, составляет до 10 м.

В настоящее время антенные характеристики оборудования радиочастотной идентификации выполняются максимально всенаправленными. Если нужна большая дальность идентификации, то применяют активные радиометки, что существенно сказывается на стоимости приобретения и последующего обслуживания. В ряде случаев является целесообразным увеличение дальности работы оборудования радиочастотной идентификации за счет совершенствования алгоритма работы и увеличения коэффициента направленного действия антенн комплексов радиочастотной идентификации.

Для снижения требований к объему передаваемой информации и к масса-габаритным показателям пассивной радиометки предлагается:

1) усовершенствовать алгоритм работы программно-аппаратного комплекса радиочастотной идентификации в части обеспечения вариативности размера идентификационного номера;

2) увеличить активную площадь антенны, что, в свою очередь, позволит увеличить количество передаваемой энергии;

3) увеличить коэффициент направленного действия антенн как пассивной радиометки, так и приемо-передающего модуля считывания информации.

Основными областями применения улучшенной технологии являются промышленность, транспортная и складская логистика, системы контроля и управления доступом и распознавания объектов. Предлагаемая технология актуальна для идентификации объектов, имеющих в конструкции металлическое незаземленное основание размером не менее 20-30 см в диаметре, где целесообразна идентификация направленного действия с максимально возможной дальностью срабатывания и минимальным временем идентификации.

Одним из перспективных примеров использования является идентификация дорожных знаков. Внесение незначительных изменений в технологию изготовления дорожных знаков позволит обеспечить их

идентификацию, что в свою очередь дает возможность обеспечить большую информативность водителя о дорожной обстановке в условиях недостаточной видимости, а также обеспечить поступление оперативной информации о дорожной ситуации в систему ЭРА ГЛОНАСС.

По результатам работы планируется создать инвестиционный проект, в котором будут определены источники финансирования для организации производства программно-аппаратных комплексов.

Одним из предполагаемых источников финансирования проекта являются финансовые средства организаций, осуществляющих полномочия при определении стандартов безопасности дорожного движения и стандартов работы оборудования ЭРА ГЛОНАСС.

На момент публикации в достаточной степени проработаны алгоритм работы программно-аппаратного комплекса радиочастотной идентификации в части обеспечения вариативности размера идентификационного номера, а также математический аппарат, позволяющий определить правила установки пассивной радиометки на объект идентификации.

Выводы

Таким образом, предлагаемый аппаратно-программный комплекс радиочастотной идентификации (RFID) направленного действия с применением усовершенствованной технологии радиочастотной идентификации для пассивных радиометок позволяет увеличить дальность идентификации пассивных радиометок, а также коэффициент направленного действия антенн комплексов радиочастотной идентификации.

Основными областями применения улучшенной технологии являются промышленность, транспортная и складская логистика, системы контроля и управления доступом и распознавания объектов.

Список литературы

1. Власов Максим. RFID: 1 технология – 1000 решений: практические примеры использования RFID в различных областях. – М.: Альпина Паблишер, 2014. – 218 с.

2. Лахири Сандип. RFID. Руководство по внедрению. – М.: Кудиц-Пресс, 2007. – 312 с.

3. Бхуптани Маниш, Морадпур Шахрам. RFID-технологии на службе вашего бизнеса. – М.: Альпина Паблишер, 2007. – 290 с.

4. Финкенцеллер Клаус. Справочник по RFID. – М.: Издательский дом «Додэка-XXI», 2008. – 496 с.

УДК 004.31

Сунгуров Александр Анатольевич
направление Информатика и вычислительная техника
(магистратура), гр. ИВТм-21
Асланов Антон Сергеевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Мясников Владимир Иванович, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА МОДЕЛИ КАТЕРА ДЛЯ МОНИТОРИНГА ВОДНЫХ ОБЪЕКТОВ

Основной целью работы является изучение принципов натурного моделирования и управления плавательными средствами. В статье рассматривается задача проектирования управляемого роботизированного плавательного средства для мониторинга водных объектов с функцией забора проб воды для использования в местах, где присутствие людей является нежелательным (водные массивы заповедников, сточные воды предприятий и т.п.).

Робот предназначен для мониторинга водных объектов, в том числе и видеомониторинга, определения в воде нетипичных для исследуемого водоёма примесей, определения температуры воды и взятия проб воды.

Плавательное средство содержит на своём борту датчик кислотности жидкости и датчик температуры, цифровую видеокамеру, с которой на пульт управления (планшет, сотовый телефон или ноутбук) передаётся видеопоток. Катер снабжён подъёмным механизмом для забора проб воды.

Робот управляется по беспроводному интерфейсу Wi-Fi, по которому в обратную сторону передаётся видеопоток. По сигналу с пульта управления робот передаёт показания датчиков кислотности жидкости и температуры, а также набирает пробы воды в два небольших резервуара ёмкостью 20 мл. Подъём каждого из них осуществляется в отдельности.

Технические и эксплуатационные характеристики

- Максимальная скорость – 7 км/ч (3,78 узлов).
- Время непрерывной работы без подзарядки – 30 мин.
- Дальность действия Wi-Fi – 100 м.

• Диапазон измеряемой температуры: 0–50 °C.

• Погрешность температуры: ±2 °C.

• Диапазон измерений кислотности воды: 0–14 pH.

• Температурные пределы работы датчика кислотности: 0−60 °C.

• Точность измерений кислотности: ±0,1 pH (при 25 °C).

• Время отклика датчика кислотности жидкости: ≤ 1 мин.

Реализуемые функции

• видеонаблюдение в бассейне исследуемого водного объекта (передача на пульт управления данных с видеокамеры);

• управление (маневрирование) катером с пульта управления в зависимости от данных с видеокамеры;

• измерение температуры воды на водном объекте и передача показаний на пульт управления;

• определение кислотности воды и интерпретация показаний датчика (присутствуют ли нежелательные примеси в воде, обнаружение реакции воды: среда ближе к щелочной или к кислотной);

• забор проб воды и доставка их на берег.

Описание структуры и принципа действия робота

Принцип действия управляемого роботизированного плавательного средства с двумя двигателями основан на использовании данных с видеокамеры и со специальных датчиков и интерпретации их показаний.

Катер получает команды о поворотах с пульта управления (телефона, планшета или ноутбука) по беспроводному интерфейсу Wi-Fi. Для реализации этой функции были использованы следующие библиотеки: CyberLib.h и Onewire.h. Данные об окружении катера человек (оператор) получает по Wi-Fi с видеокамеры.

Определив по видео попадание катера в нужную точку водного объекта, оператор подаёт по Wi-Fi команду о снятии показаний с датчиков температуры и кислотности воды. Принимаемые данные отображаются на экране пульта управления. Показания датчика кислотности воды интерпретируются программой для определения реакции воды (щёлочной или кислотной).

Оператор также может подать команду о заборе проб воды. Для реализации этой функции на борту катера содержится подъёмный механизм с прикреплёнными к нему двумя резервуарами ёмкостью 20 мл. Таким образом, можно взять пробы воды в двух контрольных точках.

Робот состоит из следующих блоков.

Ходовая часть состоит из платформы с понтонами, выполненной из пластиковых бутылок с двумя моторами. Ходовую часть питает акку-

мулятор. Управление моторами происходит через специальную плату расширения – адаптер Motor Shield.

Функции *командного блока* выполняет контроллер ArduinoNano. Он монтируется на макетную плату и служит для загрузки и исполнения кода микропрограммы и сопряжения с платами расширения.

Блок связи состоит изWi-FiRouter-a (маршрутизатора), подсоединённого через USB-hub, и антенны.

Блок мониторинга содержит датчик температуры и датчик кислотности жидкости, подключённые непосредственно к макетной плате.

Блок забора проб воды состоит из подъёмного механизма, собранного из деталей робоконструктора MakeblockUltimateRobotKit, к которому подсоединены два резервуара по 20 мл. Механизм приводится в движение двумя независимыми моторами 20 мм.

При создании робота использовалось следующее оборудование:

- контроллера ArduinoNano – 1 шт.;
- контроллер ArduinoUno – 1 шт.;
- плата расширения Motor Shield – 2 шт.;
- макетная плата Breadboard Mini – 1 шт.;
- Wi-Fi маршрутизаторTPLink TL-MR3020 – 1 шт.;
- USB-hub – 1 шт.;
- антенна ASUS – 1 шт.;
- термистор B57164-K 103-J – 1 шт.;
- датчик кислотности жидкости SEV0161 – 1 шт.;
- текстовый ЖК-экран 16×2 – 1 шт.;
- видеокамера Logitech – 1 шт.;
- мотор 20 мм AMP-F018 – 2 шт.;
- моторы 12 мм AMP-F010 – 2 шт.;
- аккумулятор 1215V 3800 Mah – 1 шт.;
- детали робоконструктора MakeblockUltimateRobotKit.

Катер для мониторинга водных объектов принимал участие во всероссийской робототехнической олимпиаде (RRO-2015), международном фестивале робототехники «Робофинист-2015»и на республиканских робототехнических соревнованиях «Роботехник-2016».

Список литературы

1. Бачинин А., Панкратов В., Накоряков В. Основы программирования микроконтроллеров. – М.: ООО «Амперка», 2013. – 207 с.

2. Уэйт М., Прата С., Мартин Д. Язык СИ. Руководство для начинающих / пер. с англ. – М.: Мир, 1988. – 512 с., ил.

3. Проекты и чертежи яхт, катеров и лодок [Электронный ресурс]. – URL: http://www.vodnyimir.ru/proekty-lodok-dlya-samostoyatelnoi-postroiki-8.html.

УДК 004.056

Тимофеев Иван Алексеевич
направление Информатика и вычислительная техника
(магистратура), гр. ИВТм-11

Научный руководитель
Малашкевич Василий Борисович, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

КОМПЛЕКСНАЯ СИСТЕМА БЕЗОПАСНОСТИ ПОМЕЩЕНИЯ

Проблема обеспечения безопасности помещений остается актуальной и в наши дни. Несанкционированные вторжения в помещения, проникновения посторонних лиц, возгорания и затопления, а также кражи документов и ценностей представляют реальную угрозу деятельности предприятий.

Для решения данной проблемы необходимо рассматривать комплекс мер безопасности как единую систему безопасности. Такой подход является наиболее эффективным в сравнении с набором мер, блокирующих каждую отдельную угрозу безопасности. Современные комплексы безопасности обеспечивают защиту помещения практически от всех угроз. Комплексные системы безопасности не только исключают или снижают возможность возникновения опасных ситуаций, но и создают благоприятные условия для работы сотрудников организации.

Комплексный подход определяет систему безопасности помещения как комплекс технико-аппаратных средств, способных обнаружить и предотвратить потенциально опасную ситуацию, а также своевременно оповестить членов персонала или руководителей о её возникновении.

В комплексную систему безопасности включены такие технические средства, как:

- блок контроля освещения;
- блок контроля электропитания;
- блок контроля вентиляции;
- блок контроля охранной сигнализации;
- блок контроля пожарной сигнализации;
- система идентификации личности;
- блок оповещения;
- система управления.

Все подсистемы и блоки обладают технической, информационной и эксплуатационной совместимостью, а также управляются из единого центра (одной программой), на котором осуществляются сбор и обработка соответствующей информации.

Организация комплексного обеспечения безопасности основывается на анализе возможных негативных последствий. Угрозы безопасности могут быть как внешними, так и внутренними, например:

- попытка хищения имущества или коммерческой тайны;
- перехват управления;
- возникновение пожара, аварии и другие опасные для жизни и здоровья людей ситуаций.

Поэтому важно организовать защиту и контроль на всех уровнях: как внешнего периметра охраняемого помещения, так и всей площади помещения.

Контроль над электроэнергией здания осуществляется системой Instabus GIRA, позволяющей управлять системами электропитания здания как локально (в конкретном помещении), так и централизованно (с диспетчерского пульта или компьютера), и удаленно. Использование программируемых таймеров, датчиков освещенности, температуры, движения и т.п. делает возможным полностью автоматическое функционирование электросистем здания в зависимости от времени года, дня недели (рабочий день/выходной) и конкретных внешних условий. Это минимизирует расход электроэнергии и создает комфортные условия в помещениях.

Система управления электропитанием строится вокруг шины EIB, которая объединяет все электрические устройства здания и системы управления. При этом упрощаются кабельные системы здания, существенно снижаются затраты на их проектирование и прокладку, сокращается время монтажа, уменьшается риск возникновения пожара.

Основу для оценки состояния помещения в системе Instabus GIRA составляют разнообразные датчики. При срабатывании датчиков система выдает сообщение об угрозе и при задымлениях, и при протечке воды, сообщая блоку управления, где и что случилось. В случае возникновения угрозы центр управления даст команду соответствующему исполнительному устройству, задача которого – блокировка и устранение обнаруженной угрозы. К числу дополнительных функций системы относится протоколирование всех событий и оповещение сотрудников о возникших событиях.

Интерфейсы системы Instabus GIRA позволяют использовать широкий круг разнообразных промышленно выпускаемых датчиков. Напри-

мер, бесконтактные датчики движения, которые в обычном режиме служат для включения света, могут использоваться также и как датчики сигнализации несанкционированного вскрытия помещения. Блок оповещения способен включать освещение, звуковую сигнализацию, а при отсутствии в помещении людей – выполнять отправку сообщений в службы охраны, а также владельцу помещения.

В составе системы предусмотрен информационный дисплей, который позволит контролировать текущее состояние системы. Основной режим работы системы – автоматическое, компьютерное управление системой. Компьютер воспринимается центральной шиной системы не как командная надстройка, а как обычный (рядовой) контроллер, принимающий все сигналы системы и передающий сообщения-команды другим контроллерам системы.

Для облегчения ручного управления системой на экране компьютера отображается мнемосхема, отображающая геометрию помещения и размещение основных контролируемых узлов. Такой подход обеспечивает индикацию состояния всего помещения, а также быстрый выбор и управление параметрами отдельных узлов системы с помощью манипулятора «мышь».

Для удаленного управления системой предполагается разработка клиентского мобильного приложения для установки на смартфонах и планшетных компьютерах.

Основные особенности помещений, оснащенных системой комплексного контроля:

- способность оптимально реагировать на изменения в процессах, происходящих в здании;
- сочетание децентрализованных (распределенных) принципов построения систем с централизацией функции мониторинга и управления;
- структурированный подход к построению инженерных систем здания;
- интеграция систем контроля с минимальными затратами;
- обслуживание систем организовано оптимальным образом;
- возможность наращивания и видоизменения конфигурации инсталлированных систем;
- центральное диспетчерское управление обеспечивает как контроль, так и управление функциями здания;
- мобильное удаленное управление функциями здания.

Таким образом, данная система может быть использована во многих зданиях различных типов. Невысокая стоимость и широкий спектр

функций обеспечивает системе конкурентные преимущества в сравнении с аналогами.

Список литературы

1. http://www.slavyane-nsk.ru/kompleksnie-sistemi-bezopastnosti.html
2. http://www.gaw.ru/html.cgi/txt/doc/micros/arm/arh_7dtmi/survey.htm
3. http://www.cbsr.ia.ac.cn/IrisDatabase.htm - база данных CASIA-IrisV3-2011
4. http://biometrics.idealtest.org/dbDetailForUser.do?id=1
5. http://www.rusobschina.ru/2010-11-08-08-17-41/2010-11-11-11-45-20/674-2010-11-26-09-49-10

УДК 004.93

Тоцкий Алексей Андреевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-31

Научный руководитель
Ипатов Юрий Аркадьевич, канд. техн. наук, доцент,
кафедра информатики
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

БИБЛИОТЕКИ ПАРАЛЛЕЛЬНОГО ПРОГРАММИРОВАНИЯ ДЛЯ ЗАДАЧ ЦИФРОВОЙ ОБРАБОТКИ ИЗОБРАЖЕНИЙ

Эволюционное развитие средств программирования уже давно стало локомотивом развития информационных технологий в комплексе с алгоритмической и аппаратной составляющей. С появлением современных операционных систем возникла необходимость выполнения инструкций, в параллельном режиме поступающих от разных приложений. В эволюции аппаратных средств вычислительного процесса стало невозможным увеличивать тактовую частоту процессора, поэтому было принято решение идти по пути наращивания количества вычислительных ядер. Все эти предпосылки делают актуальным вопрос развития технологий параллельного программирования на аппаратном и программных уровнях вычислительного процесса [1].

На сегодняшний день функционирование систем технического зрения, интеллектуальных методов обработки и анализа изображений, распознавания образов и их классификации обуславливается широким спектром научно-технических исследований. Очевидно, что для обеспе-

чения эффективной работы в этом направлении процедуры и функции обработки изображений должны удовлетворять временным ограничениям (реальному времени) [2]. Следовательно, для этого возникает необходимость параллельной обработки данных.

Одним из наиболее распространенных стандартов в области параллельного программирования является OpenMultiprocessing. OpenMP служит простым и гибким инструментарием для создания многопоточных программ обработки изображений. Большинство современных компиляторов для языков программирования Fortran и C/C++ имеют встроенную поддержку OpenMP. За развитие стандарта OpenMP отвечает некоммерческая организация, в состав которой входят ведущие разработчики аппаратного и программного обеспечения [3]. Для обработки изображений, данные которых допускают матричное представление, в последнее время широко применяются графические процессоры общего назначения (GPU).

Одной из распространенных технологий программирования GPU является Nvidia CUDA [4]. Обработку данных с использованием технологии CUDA в общем виде можно представить как поточно-параллельный конвейер:

1) поток данных разбивается на множество одинаковых по размеру блоков данных с формованием обрабатываемого потока блоков;

2) GPU содержит фиксированный набор ядер.

Каждое ядро является мультипроцессорным вычислителем.

Характерной особенностью функционирования современных систем обработки изображений являются большие объемы обрабатываемой информации. Поэтому возникает задача автоматического распараллеливания процесса обработки с учетом специфических особенностей функционирования. В таблице приведены сравнительные характеристики технологий параллельного программирования [5].

Таблица 1 – **Сравнительные технологии параллельной обработки**

Название	MPI	OpenMP	MapReduce
Автоматическое распараллеливание	Нет	Да	Да
Архитектура оборудования	SMP, MPP, Кластер	SMP	SMP, Кластер
DFS	Нет	Нет	Да
Механизмы востановления при отказе оборудования	Нет	Нет	Да
Программа функционирования	Произвольная	Произвольная	MapReduce

Анализ библиотек обработки изображений с возможностью параллельного вычисления приведен в таблице 2.

Таблица 2 – **Библиотеки параллельной обработки изображений**

Название	ОС	Технологии	Языки	Функции
Matrox Imaging Library	Linux/ Windows	multi-core CPU, multi-CPU, GPU, FPGA	C, C++, C#, CPyhton, VBA	>300
Intel® Integrated Performance Primitives	Windows/ Linux/ OS X/ Android	multi-core CPU, multi-CPU	C, C++	>500
Sapera Vision Software	Windows	multi-core CPU, FPGA	C++	~400
Open eVision Libraries	Windows	multi-core CPU	C++, C#, VBA, Delphi	>100
Matrix Vision Impact	Windows	multi-coreCPU	C, C++, C#, VBA	>150

Из анализа данных рассмотренной таблицы можно сделать промежуточный вывод, что базовый набор функций, включающий в себя точечную обработку, фильтрацию изображения, логические и арифметические преобразования, у большинства библиотек сходны, однако различаются по производительности.

Таким образом, для создания эффективного алгоритма обработки изображений необходимо определиться с технологией параллельной обработки в случае большого массива данных или использовать готовые библиотеки параллельной обработки на отдельных вычислителях.

Разработка ведется в рамках гранта Президента Российской Федерации для государственной поддержки молодых ученых МК-7290.2015.9.

Список литературы

1. Лин К., Снайдер Л. Принципы параллельного программирования. – М.: Издательство МГУ, 2013. – 407 с.

2. Системы машинного зрения мобильных роботов [Электронный ресурс] / В. А. Беликов, В. В. Жога, В. Н. Скакунов и др. // Известия ВолгГТУ. – 2014. – № 25 (152). – URL: http://cyberleninka.ru/article/n/sistemy-mashinnogo-zreniya-mobilnyh-robotov (дата обращения 02.04.2016).

3. Лёвин М. П. Параллельное программирование с использованием OpenMP. – М.: Интернет-Университет Информационных Технологий; Бином. Лаборатория знаний, 2012. – 118 с.

4. Параллельные вычисления на GPU. Архитектура и программная модель CUDA / А. В. Боресков, А. А. Харламов, Н. Д. Марковский и др. – М.: МГУ, 2012. – 978 с.

5. Созыкин А. В., Гольдштейн М. Л. Архитектура системы обработки больших объемов изображений с автоматическим распараллеливанием [Электронный ресурс]. – URL: http://agora.guru.ru/abrau2012/pdf/58.pdf (дата обращения 02.04.2016).

УДК 004.7

Тоцкий Алексей Андреевич,
Асланов Антон Сергеевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель:
Морохин Дмитрий Витальевич, канд. техн. наук, доцент
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

УЛЬТРАЗВУКОВАЯ СИСТЕМА ПОЗИЦИОНИРОВАНИЯ

Рассматривается разработка локальной системы позиционирования высокоточной точности для применения в закрытых помещениях с использованием ультразвука для определения положения объекта в пространстве.

Система позиционирования (определения координат) является системой, которая может определять положение некоего объекта в пространстве относительно известной точки отсчёта.

Все системы позиционирования условно можно разделить на системы глобального и локального позиционирования. *Системы глобального позиционирования* могут определить положение объекта в любой точке земного шара. Примерами таких систем являются GPS и её российский аналог – ГЛОНАСС. Однако точность позиционирования (около 10-15 м, правда, в настоящее время разработаны алгоритмы, реализованные программно, позволяющие увеличить точность до 2-3 м) может оказаться недостаточной в некоторых случаях. Ещё одним весомым недостатком систем такого типа является неработоспособность в помещениях. Примером, когда такая система позиционирования не будет удовлетворять требованиям в этих случаях, может быть навигация по складам автономных роботов.

Системы локального позиционирования, в свою очередь, осуществляют позиционирование «локально», т.е. в пределах ограниченного за-

крытого пространства, например, комнаты. Такие системы, как правило, точнее глобальных систем, но главное их преимущество перед последними – работоспособность в отдельных помещениях.

Целью выполнения данной работы является исследование, разработка и тестирование локальной системы позиционирования. В качестве основы системы служит ультразвуковой способ измерения расстояния. Кроме управления отслеживаемым устройством вручную, предполагается реализовать автономный режим управления при помощи обмена информацией объектом с системой.

На данном этапе решались задачи синхронизации составных частей системы и визуализация положения объекта в двухмерной системе координат при помощи взаимодействия системы с ПК.

Полученное на данный момент решение состоит из нескольких модулей, структура одного из которых указана на рисунке 1. Система состоит из одного главного модуля, одного модуля излучения ультразвука и множества модулей улавливания излучаемого ультразвука. Главный модуль управляет всеми остальными модулями, для обмена информацией между ними используется радиоканал. По его команде модуль излучения ультразвука посылает ультразвуковые импульсы, а модули приёма замеряют время от объявления модулем излучения по радиоканалу о начале излучения ультразвука до (непосредственно) его приёма и передают свои замеры по радиоканалу на главный модуль, который будет отправлять эти замеры на ПК для визуализации.

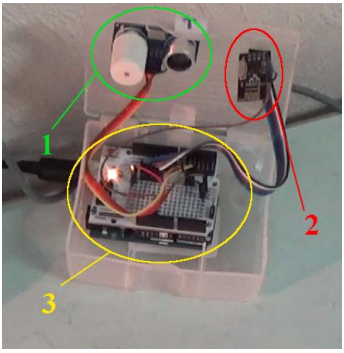


Рис. 1. Структура модуля: 1 – ультразвуковой модуль, 2 – радиомодуль, 3 – плата Arduino Uno + Troyka Shield

Для определения положения отслеживаемого объекта используется алгоритм трилатерации. С геометрической точки зрения задача трилате-

рации сводится к нахождению точки пересечения трех или четырех сфер, координаты центра которых известны, а радиусом которых является расстояние от центра каждой из сфер до отслеживаемого объекта.

В текущий момент построен прототип системы с двумя модулями приёма ультразвука (один из которых выполняет функции и главного модуля) и модулем излучения ультразвука. Налажено их взаимодействие между собой и взаимодействие с ПК для визуализации положения отслеживаемого объекта в двухмерном пространстве.

Блок-схема одного из модулей (модуля приёма ультразвука) приведена на рисунке 2.

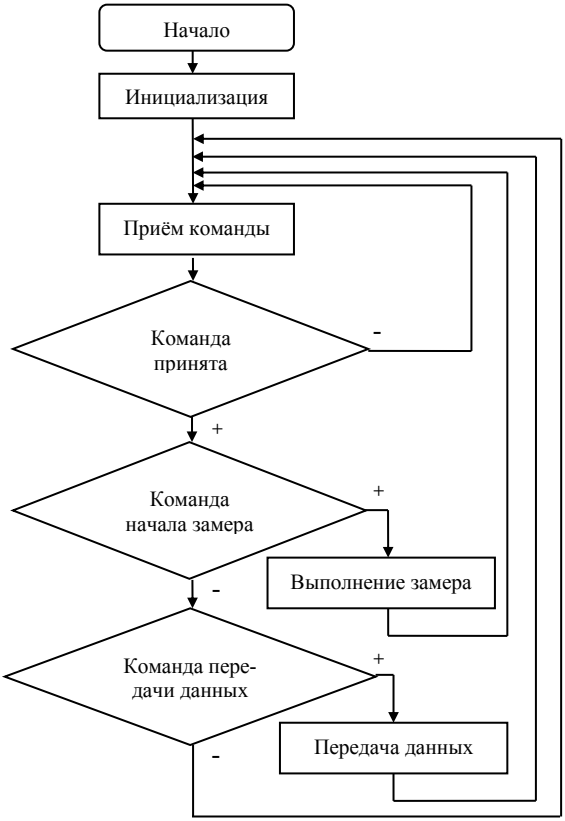


Рис. 2. Блок-схема модуля приёма ультразвука

Данная структура, почти без изменений, также применима и к модулю излучения ультразвука. Как видно на рисунке, сначала происходит инициализация системы (настройка параметров радиомодуля, открытие необходимых радиоканалов, настройка ультразвукового датчика и т. д.), а затем в бесконечном цикле происходит попытка приёма команды за отведённое время.

Каждая команда кодируется неким числом, и это число посылается в радиоканал. Если за это время команда не была получена или полученное число, интерпретируемое как команда, не соответствует ни одной команде, которую может выполнить модуль, то осуществляется непосредственный переход к получению новой команды, иначе выполняется указанная команда, и после этого происходит переход к попытке получения новой команды.

Блок-схема модуля излучения ультразвука отличается от данной схемы лишь тем, что он умеет распознавать только одну команду: запрос на излучение ультразвука, и в случае её получения он посылает команду начала замера и собственно излучает ультразвук, после чего начинает бесконечный цикл заново.

В будущем планируется усовершенствовать прототип в следующих направлениях:

- улучшить алгоритм управления системой главным модулем,
- увеличить количество модулей приёма в системе,
- улучшить точность замера расстояния,
- ввести отслеживание положения объекта в трёхмерном пространстве.

Список литературы

1. Блум Джереми. Изучаем Arduino: инструменты и методы технического волшебства / пер. с англ. – СПб.: БХВ-Петербург, 2015. – 336 с.

2. Processing: a programming handbook for visual designers and artists / Casey Reas and Ben Fry. – Second Edition, 2014. – 642 с.

3. GPS [Электронный ресурс] // Википедия – свободная энциклопедия. – URL: https://ru.wikipedia.org/wiki/GPS

4. Создание ультразвуковой локальной системы позиционирования [Электронный ресурс]. – URL: https://ru.wikiversity.org/wiki/Создание_ ультразвуковой_локальной_системы_позиционирования

5. Pozyx datasheet [Электронный ресурс]. – URL: https://www.pozyx.io/ Documentation/Datasheet

УДК 372.862

Файзуллин Ранис Марсельевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-11

Научный руководитель
Старыгин Сергей Витальевич, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ФОРМИРОВАНИЕ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ ОБУЧАЮЩИХСЯ В ПРОЦЕССЕ КУРСОВОГО ПРОЕКТИРОВАНИЯ
(УЧЕБНАЯ ДИСЦИПЛИНА «ЭЛЕКТРОТЕХНИКА, ЭЛЕКТРОНИКА И СХЕМОТЕХНИКА»)

В соответствии с требованиями ФГОС 3+ к результатам обучения по направлению подготовки бакалавров «Информатика и вычислительная техника» освоение учебной дисциплины «Электротехника, электроника и схемотехника» направлено на формирование у обучающихся (студентов третьего курса факультета информатики и вычислительной техники) общепрофессиональной компетенции ОПК-4 («способность участвовать в настройке и наладке программно-аппаратных комплексов»).

Важнейшей целью дисциплины является накопление студентами необходимого опыта деятельности по разработке и анализу схем и устройств, выбору элементной базы, по проектированию функциональных узлов ЭВМ и разработке оптимальных алгоритмов их функционирования, по созданию программ автоматизированного моделирования устройств ЭВМ и др. Прежде всего данные умения и навыки формируются и отрабатываются на лабораторных занятиях. Вместе с тем существенную роль для достижения указанной цели играет курсовое проектирование, задача которого – закрепление теоретических знаний и практического опыта профессиональной деятельности.

Курсовое проектирование решает комплекс обучающих задач:

- проработка методов синтеза логических устройств ЭВМ;
- разработка схемотехнических модулей, представление их функциональных и принципиальных схем;
- выполнение электрических расчетов, подтверждающих правильность разработанных схем;
- оформление схемотехнической документации в соответствии с нормативными требованиями.

Отметим, что содержание тем для курсового проектирования строго соответствует сформулированным цели и задачам. Студентам предлагаются темы, ориентирующие их на осмысление теории и применение практических умений и навыков. Например, разработка многоканального АЦП, цифрового генератора синусоидальных сигналов, преобразователя последовательного цифрового кода в параллельный и наоборот.

Эффективность курсового проектирования во многом зависит от организации самостоятельной работы студентов и соблюдения всех необходимых этапов процесса проектирования.

Самостоятельная работа студентов организована достаточно традиционно: распределение тем, консультирование в течение семестра, мониторинг выполнения курсового проекта.

Привычные способы организации самостоятельной работы студентов разнообразятся благодаря использованию активных и интерактивных методов обучения. Так, консультации проводятся в формате обсуждения разделов курсового проекта не только с преподавателем, но и с другими студентами (организуется работа парами или предлагается представить содержание раздела проекта (например, вступление) всей группе с целью совместного выявления недостатков и определения достоинств раздела). На завершающем этапе работы над проектом обязательно проводится апробация процедуры защиты основных результатов проектирования, включающая обсуждение сделанного сообщения с точки зрения его соответствия учебной ситуации (структура, логика, стиль), а также анализ полученных результатов.

Курсовое проектирование завершается процедурой защиты проекта. Она включает, помимо традиционного представления полученных результатов, проверку этих результатов с помощью компьютерного моделирования в электронной лаборатории EWB. Разработанная по заданию схема реализуется в системе EWB 5.12 и проводится анализ ее работы: временные диаграммы, формы управляющих и информационных сигналов, временные задержки и др. Далее осуществляется сравнение результатов проектирования и электронного моделирования, по результатам которого определяется оценка проекта.

Моделирование профессиональной (инженерной) ситуации внедрения результатов проектирования в технологический процесс оказывается эффективным приемом оценивания результатов обучения. Он позволяет определить уровень освоения общепрофессиональной компетенции (ОПК-4) студентами (пороговый, продвинутый или высокий), выявить пробелы в теоретических знаниях, определить наличие или отсутствие необходимых умений и навыков.

Однако самым существенным является то, что моделирование профессиональной ситуации в электронной лаборатории EWB наглядно демонстрирует каждому студенту реальный результат его проектировочной деятельности (положительный или отрицательный).

Таким образом, решается одна из важнейших задач обучения: реализуется этап рефлексии собственной деятельности, содержащий критический анализ всех этапов работы над проектом, качества и уровня знаний, учебного, исследовательского и профессионального опыта и, конечно, полученных результатов.

Хочется подчеркнуть, что в учебной ситуации, построенной на моделировании профессиональной ситуации, формируются не только общепрофессиональная или профессиональные компетенции, но и общекультурные компетенции (например, способность работать в коллективе), а также личные качества человека (ответственность, серьезное отношение к делу, самокритичность и др.). В совокупности все это обеспечит выпускнику быструю адаптацию в профессиональном коллективе и успешную социализацию.

Список литературы

1. Новости информационных технологий // PVSM.RU [Электронный ресурс]. – 2010. – URL: http://www.pvsm.ru/raspberry-pi/51571/print/ (дата обращения 08.11.2016).

2. Открытая социальная сеть TechCave: Нахождение контуров объекта в OpenCV // TECHCAVE.RU [Электронный ресурс]. – 2016. – URL: techcave.ru/posts/51-nahozhdenie-konturov-obekta-v-opencv/ (дата обращения 08.11.2016).

УДК 004.91

Файзуллин Ранис Марсельевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-11

Научный руководитель
Савинов Александр Николаевич, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИЗВЛЕЧЕНИЕ ИЗОБРАЖЕНИЙ ИЗ ПАМЯТИ ПРОЦЕССА БРАУЗЕРА КАК ПРИМЕР RAM-АТАКИ

На сегодняшний день ценность информации не вызывает сомнения. В связи с этим важная и секретная информация организаций и компаний

всегда находится под угрозой. Существует множество вариантов атак с целью нарушения конфиденциальности информации. В первую очередь атаки направлены на кражу данных с дисков, на которых хранится информация, и из сетей, по которой информация передается, – то есть на информационные процессы передачи и хранения информации.

Соответственно средства защиты, применяемые в организациях и предприятиях, направлены в основном на предотвращение несанкционированного чтения файлов с устройств их хранения и на предотвращение перехвата файлов, передаваемых по сети.

В основном это достигается установкой различных средств предотвращения доступа злоумышленника или распространяемых им троянских программ к важной информации. Активно используется шифрование хранимой или передаваемой информации.

Однако существует группа атак, направленных на кражу информации, обрабатываемой на ЭВМ, то есть атака направлена на информационный процесс обработки информации. К таким атакам относятся атаки по оперативной памяти компьютера, когда читается оперативная память с целью нарушения конфиденциальности информации.

Дело в том, что информация, помещенная в оперативную память ЭВМ для обработки, находится там в открытом незашифрованном виде. Средств разграничения доступа к оперативной памяти, помимо привилегированного и пользовательского режима работы, предоставляемых операционной системой, не существует. Как правило, в режиме супервизора или вообще не действуют ограничения защиты памяти, или же они могут быть произвольным образом изменены, поэтому код, работающий в данном режиме, как правило, имеет полный доступ ко всем системным ресурсам. При этом большинство приложений обработки информации работают в пользовательском режиме. Таким образом, информация, находящаяся в оперативной памяти может быть прочитана в обход методов шифрования и разграничения доступа, применяемых для защиты на данной ЭВМ.

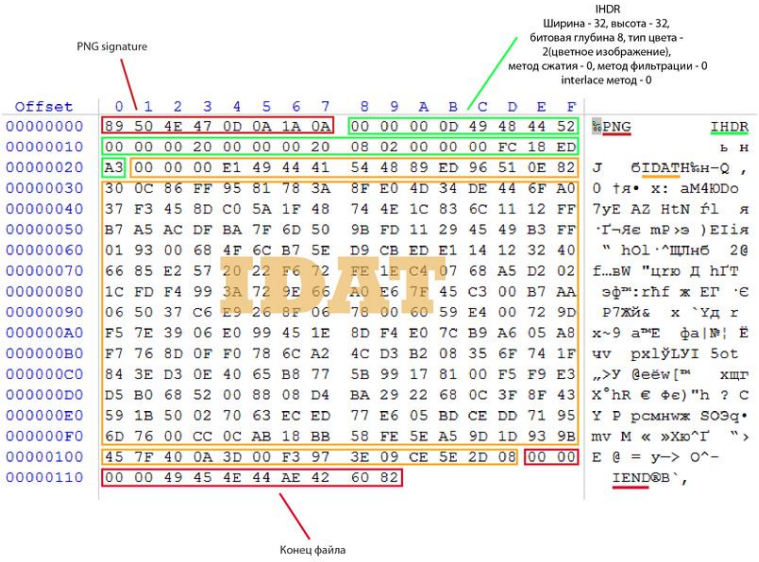
Существует несколько вариантов реализации атак по оперативной памяти. Легкореализуемый с технической стороны – атака специальным вирусным программным обеспечением, работающим в режиме ядра. Самый сложно реализуемый вариант – атака методом холодной перезагрузки, когда при охлаждении жидким азотом модули оперативной памяти изымаются из компьютера-жертвы и устанавливаются для чтения в другой компьютер.

Несмотря на множество известных атак по оперативной памяти, основным применяемым и самым действенным средством защиты от них

является предотвращение проникновения злоумышленника к ЭВМ. Однако в связи с возросшим количеством инсайдерских угроз, реализуемых в последнее время во всем мире, судя по статистике, данный способ защиты вызывает сомнения в надёжности.

Целью исследования является разработка инструмента для тестирования возможностей атак по оперативной памяти программного обеспечения, который продемонстрирует, какая информация может быть прочитана, если злоумышленнику удастся реализовать атаку по оперативной памяти. Разработано программное обеспечение, позволяющее подключиться к программному обеспечению в режиме отладчика и получить дамп памяти. Разработанный инструмент включает в себя идеи таких известных программ, как ArtMoney, ResourceHacker, WinHex.

Инструмент позволяет обеспечить привилегированный режим работы, получить список работающих на ЭВМ процессов и собрать дамп памяти процесса в файл. Дамп памяти собирается постранично, затем анализируется побайтово. Для поиска информации используется сигнатуры файлов и специальные маски (см. рисунок).



Сигнатура PNG-файла

Поиск информации в файле дампа памяти процесса осуществляется путем преобразования введенного пользователем шаблона в последова-

тельность байт. Полученная последовательность сравнивается со всеми возможными последовательностями байт, расположенными линейно, прочитанными из файла.

Преобразование шаблона поиска в последовательность байт осуществляется путем присваивания указателя переменной, являющейся объектом типа данных динамический массив байт, указателю цели поиска. Таким образом, цель поиска рассматривается как динамический массив байт. В случае нахождения совпадения целевого и прочитанного массивов байт позиция прочитанного массива относительно начала файла сохраняется.

Изображения ищутся методом сигнатурного поиска. Этот механизм очень похож на то, как работают антивирусы: для поиска изображений используется набор сигнатур, которые встречаются в том или ином графическом формате. Скажем, в начале всех файлов в формате PNG встречается сигнатура PNG. Обнаружив сигнатуру, алгоритм анализирует соседние байты данных. Если данные указывают на то, что обнаруженный фрагмент принадлежит файлу в известной программе формате, алгоритм рассматривает набор данных в качестве заголовка файла, вычисляя его размер и параметры.

Таким образом, зная сигнатуры информации или то, как она представляется в оперативной памяти, её можно найти и нарушить её конфиденциальность. Поэтому пользователи и разработчики ПО должны иметь представление о том, какая информация находится под угрозой.

Итак, проведено экспериментальное тестирование инструмента. Был создан дамп памяти браузера Yandex. В данном браузере имеется приватный режим работы, когда данные не сохраняются на жесткий диск и данные, передаваемые по сети, шифруются. Этот режим позиционируется как режим с надежной защитой информации пользователя. Однако в оперативной памяти процесса браузера все данные находятся в открытом виде. Поэтому после сбора дампа в 4 Гигабайта, когда в браузере в приватном режиме были открыты страницы социальных сетей, удалось, к примеру, извлечь 836 Мегабайт файлов изображений.

Дальнейшая разработка проекта будет направлена на добавление в инструмент различных сигнатур и масок для поиска информации в дампе памяти. Будет реализован интерефейс для отображения видов и количества извлеченной информации в виде диаграмм и статистики. Тогда пользователи инструмента смогут увидеть, какая информация находится под угрозой, и соответственно продумать и внедрить методы её защиты.

Список литературы

1. Чиликов А. А. Атаки по памяти // Защита информации. Инсайд. – 2011. – № 3. – С. 62-67.

2. Савинов А. Н., Цапина Е. В. Исследование способов атак по оперативной памяти // Научному прогрессу – творчество молодых: материалы XI международной молодежной научной конференции по естественнонаучным и техническим дисциплинам (Йошкар-Ола, 22-23 апреля 2016 г.): в 4 ч. / редкол.: Д. В. Иванов [и др.]. – Йошкар-Ола: Поволжский государственный технологический университет, 2016. – Ч. 3. – С. 137-139.

УДК 004.91

Файзуллин Ранис Марсельевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-11
Кузнецов Владимир Алексеевич
направление Информатика и вычислительная техника
(магистратура), гр. ИВТм-21

Научный руководитель
Савинов Александр Николаевич, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА АЛГОРИТМОВ СИСТЕМЫ ПРОВЕДЕНИЯ И АВТОМАТИЧЕСКОЙ ПРОВЕРКИ ДИКТАНТОВ НА АНГЛИЙСКОМ ЯЗЫКЕ

Без написания диктантов сегодня трудно представить преподавание любого иностранного языка (в том числе и английского). Они позволяют закрепить словарный запас обучающегося. Связный диктант – один из способов развития навыков письменной речи. Помимо закрепления изученной лексики, связный диктант способствует формированию навыков излагать свои мысли на иностранном языке, так как заставляет обучающихся во время диктанта запоминать смысловые синтагмы, догадываться о написании незнакомых слов, используя изученные правила словообразования. Запоминая продиктованное предложение, студент, используя свой опыт, знание правил чтения, а также правила построения английского предложения, анализирует и перерабатывает информацию, чтобы справиться с поставленной задачей.

Таким образом, связные диктанты способствуют не только закреплению изученной лексики, но и развивают общие навыки письменной

речи. Однако, несмотря на глобальную компьютеризацию и внедрение информационных технологий во все сферы человеческой жизнедеятельности, в учебных заведениях диктовка и проверка работы обучающегося проводится самим преподавателем вручную. Автоматизация этого процесса позволит уменьшить нагрузку, ложащуюся на преподавателя, и ускорить проверку студенческих работ [1-5].

В связи с этим актуальной задачей является разработка системы автоматического проведения и проверки диктантов на английском языке. Рекомендуется разработать данную систему в виде веб-портала и веб-приложения. Предложено включить в «Систему автоматической проверки диктантов на английском языке» два режима работы:

1. *Режим добавления нового диктанта*. Разработанный алгоритм (рис. 1) разбивает текст диктанта на предложения. Далее каждое предложение разбивается на слова и отправляется в разработанную экспертную систему для синтаксического и грамматического анализа. В результате анализа определяются правила грамматики, применимые к данному предложению. В разработанную базу данных добавляются исходный текст диктанта и указатели на правила, применимые к каждому предложению исходного текста. Также разработанная экспертная система позволяет найти, добавить и сохранить дополнительные варианты написания каждого предложения исходного текста, которые тоже будут являться правильными. Разработанный алгоритм позволяет автоматически присоединять к добавляемому диктанту все используемые правила грамматики. Это дает возможность заменить ручной труд преподавателя, составляющего диктант, по подготовке диктанта и дальнейшей проверке написанных работ.

2. *Режим проверки написанного диктанта*. Разработанный алгоритм (рис. 2) разбивает написанный пользователем диктант на предложения. Каждое предложение сравнивается с хранящимися в базе данных исходным и дополнительными правильными вариантами написания этого предложения. В случае, если совпадений не обнаружено, предложение разбивается на слова и отправляется в экспертную систему для проверки правил грамматики. Обнаруженные ошибки и указатели на нарушенные правила грамматики в данном предложении сохраняются в базу данных.

Ввод текста диктанта программно представляет собой реализованную на языке PHP форму части графического интерфейса пользователя.

Процедуры разбиения текста на предложения и разбиения предложения на слова представляют собой синтаксический анализатор, реализованный в виде PHP скриптов, посимвольно просматривающий текст

диктанта. Для определения объектов текста предусматривается обнаружение объектов текста – разделителей. Для процедуры разбиения на предложения это точка, восклицательный и вопросительный знаки. Для разбиения предложения на слова – пробел, запятая, кавычки, точки, вопросительный знак, восклицательный знак, дефис и прочие знаки препинания.

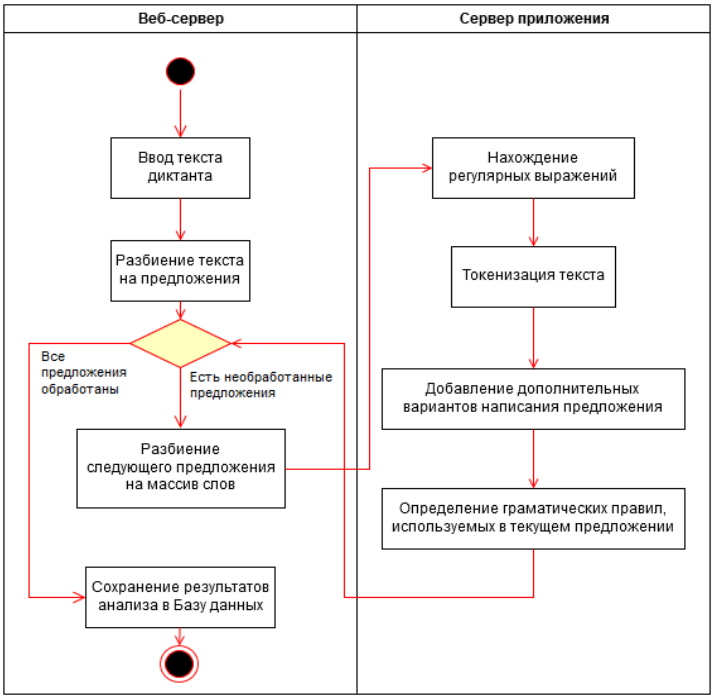


Рис. 1. UML диаграмма деятельности. Укрупненный алгоритм анализа текста нового диктанта при добавлении

Дальнейшим анализом текста занимается разработанная в оболочке CLIPS экспертная система. Правила нахождения регулярных выражений предназначены для анализа предложения как единой текстовой строки без учета свойств слов, входящих в предложение. Предназначены для поиска простых правил грамматики, например, наличия обязательных пробелов между знаками препинания, наличия пробелов между словами, наличия заглавной буквы в начале предложения, наличия правильного знака препинания в конце предложения и т.д.

Затем происходит токенизация предложения путем применения специальных правил экспертной системы, предназначенных для обнаружения структурных элементов в предложении. В правилах учитываются порядок слов в предложении, части речи, числа, лица глаголов и т.п.

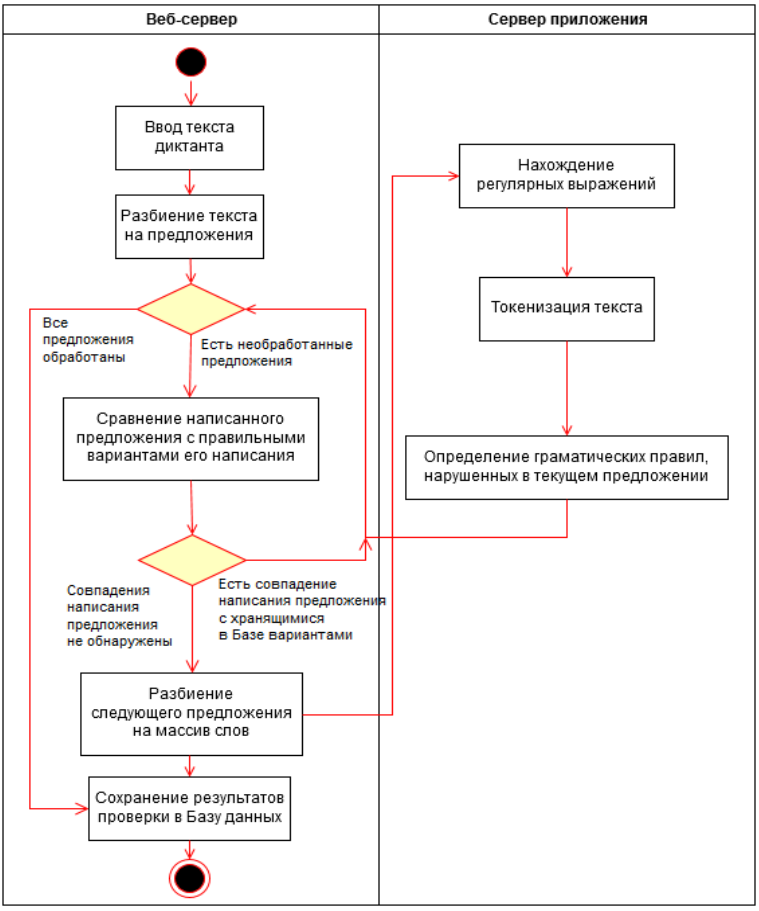


Рис. 2. UML диаграмма деятельности. Укрупненный алгоритм анализа написанного текста диктанта

Одной из проблем написания и проверки диктантов на естественном языке является то, что одно и то же предложение может быть записано правильно в нескольких различных вариантах. Поэтому далее происхо-

дит применение правил, позволяющих найти дополнительные варианты правильного написания предложений. Найденные варианты написания предложения сохраняются в базу данных.

После обнаружения регулярных выражений и определения структуры предложения становится возможным применить правила экспертной системы, предназначенные для поиска правил грамматики, применимых к данному предложению. Взаимодействие с таблицами базы данных происходит путем создания и выполнения запросов INSERT и SELECT на языке SQL генерируемых разработанными PHP скриптами.

Главное отличие второго алгоритма от первого – наличие функции сравнения введенного предложения с имеющимися в базе данных вариантами правильного написания данного предложения. Если введенное пользователем предложение совпадает с одним из введенных предложений, то система считает, что предложение написано правильно. Если совпадения не обнаружены, то система передает набранное пользователем предложение в экспертную систему для анализа, проводимого с целью выявления того, какие правила грамматики в нём были нарушены.

Разработанные алгоритмы при их реализации позволят организовать функционирование портала проведения и автоматической проверки диктантов на английском языке. Преподаватели, за счет функционирования первого алгоритма, будут иметь возможность добавить диктант в систему и сразу увидеть правила грамматики, которые применимы к тексту диктанта. Также данный алгоритм позволит добавить к диктанту дополнительные варианты его правильного написания, что позволит избежать апелляций после проверки диктанта. Обучающиеся за счет применения второго алгоритма смогут оперативно получить оценку за написанный ими диктант и узнать, какие ошибки они допустили и какие правила грамматики нарушили. Кроме того, возможно получение студентами рекомендаций о том, какой грамматический материал им стоит подробнее и основательнее изучить, чтобы восполнить имеющиеся пробелы в знаниях.

Список литературы

1. Коржов В. С. Многоуровневые системы клиент-сервер // Сети. – № 6. – 1997.

2. Ананченко И. В., Шапаренко Ю. М. Современные компьютерные системы контроля знаний учащихся // Символ науки. – 2015. – № 6. – С. 250-253.

3. Газуль С. М., Ананченко И. В., Кияев В. И. Совершенствование образовательного процесса в вузе: активные методы обучения и гибридные информационные системы на основе виртуализации // Современные проблемы науки и образования. – 2015. – № 2. – С. 201.

4. Ананченко И. В., Щербович-Вечер А. В. Проектирование современных инфокоммуникационных сетей с использованием технологий программно-конфигурируемых сетей и виртуализации сетевых функций // Символ науки. – 2015. – № 12-1. – С. 11-13.

5. Голошумов А. Ю. Информационно-технологическое обеспечение процесса экономического образования // Вестник Челябинского государственного педагогического университета. – 2009. – № 9. – С. 22-29.

УДК 004.91

Файзуллин Ранис Марсельевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-11
Пиварелис Любовь Леонидовна
направление Информатика и вычислительная техника
(магистратура), гр. ИВТм-21

Научный руководитель
Савинов Александр Николаевич, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ПРЕДСТАВЛЕНИЕ ИНТЕРЕСОВ ПОЛЬЗОВАТЕЛЯ ИНТЕРНЕТ В ОНТОЛОГИИ

Развитие современных поисковых, рекомендующих и экспертных систем основано на внедрении технологий Web 3.0, т.е. семантической паутины. Создание онтологических описаний предметных областей и наполнение онтологических профилей пользователей создаст основу для внедрения в текущую Всемирную паутину новых подходов к построению систем рекомендации товаров и услуг в Интернете. Процесс отображения онтологических описаний интересов пользователей на аннотации товаров и услуг, выполненных в виде онтологии, позволит генерировать рекламу, направленную на конкретного пользователя.

На данный момент построение рекомендующих систем на основе онтологических профилей является сложным и трудоемким процессом в связи с отсутствием эффективных методов и способов автоматического наполнения онтологий. Быстрота и дешевизна их разработки имеют решающее значение для успеха приложений, основанных на инженерии знаний и семантической паутине. Подход к решению этой проблемы

состоит в создании автоматической или полуавтоматической системы обучения онтологий. Поэтому задача исследования и разработки моделей, методов, способов и алгоритмов автоматического или автоматизированного наполнения онтологий является актуальной на данный момент.

Обучение онтологий – это обнаружение знаний в различных источниках данных и их представление в виде онтологической структуры, вместе с самим процессом наполнения онтологий это представляет собой подход к автоматизации процесса приобретения знаний. Приобретение знаний в предметной области требует много времени и ресурсов. Необходимо разрабатывать методы и приемы, которые позволят уменьшить усилия, необходимые для обучения онтологий. Данные методы должны поддерживать как обучение онтологии с нуля, так и обогащение или адаптацию существующих онтологий.

Одной из важнейших задач создания систем наполнения и анализа онтологий является разработки способа представления и хранения онтологий в ЭВМ. Её актуальность обоснована требованиями к минимально возможному количеству оперативной и внешней памяти, занимаемой онтологией, и скорости анализа знаний, хранимых в онтологии.

В рекомендующих системах, работающих в среде Интернет, с помощью онтологий описываются предметные области, содержащие большое количество фактов и знаний, для хранения и обработки которых необходимо большое количество памяти. Анализ больших онтологий требует значительных временных затрат. Однако пользователь Интернета посещает конкретный ресурс на незначительный промежуток времени. Поэтому необходимо сгенерировать рекомендации и выдать их пользователю практически мгновенно, как только он обратился к сайту. В связи с этим решение задачи оптимального представления онтологий в ЭВМ является важным фактором создания успешных веб-приложений рекламы товаров на основе онтологического профиля пользователя.

Предложенная система рекомендации товаров и услуг на основе онтологического профиля пользователя включает в себя три онтологии:

- онтологический профиль пользователя, хранящий знания об интересах и предпочтениях пользователей;
- мета-онтология, содержащая абстрактные понятия и ключевые термины предметной области;
- онтологическая аннотация товаров, хранящая описание товаров в виде онтологии, построенной на терминах мета-онтологии предметной области.

Для представления и хранения онтологий в современных информационных системах применяется два языка – RDF и OWL. Выбран язык OWL для создания онтологического профиля пользователя в связи с тем, что он имеет ряд преимуществ, важных при реализации разрабатываемой системы:

- создание локальных ограничений области распространения понятия;
- наличие функций работы с множествами понятий;
- возможность задавать мощности свойств.

Разработанное программное обеспечение проводит синтаксический анализ файла OWL онтологии, выделяя типичные для данного формата структуры. Такими структурами являются специальные теги.

Существуют следующие виды OWL тегов, распознавание которых позволит получить представление онтологии в программе:

- тег определения абстрактных понятий, например:

```
<Declaration>
    <Class IRI="#Жанр"/>
  </Declaration>
```

- тег определения ключевых слов, например:

```
<Declaration>
    <NamedIndividual IRI="#Детектив"/>
  </Declaration>
```

- тег определения связей между понятиями или понятиями и ключевыми словами, например:

```
<ClassAssertion>
    <Class IRI="#Жанр"/>
    <NamedIndividual IRI="#Детектив"/>
  </ClassAssertion>
```

- тег определения атрибутов количественных и качественных оценок интереса пользователем, его значения и связи с интересом, например:

```
<AnnotationAssertion>
    <AnnotationProperty IRI="#Оценка"/>
    <IRI>#Детектив</IRI>
    <Literal datatypeIRI=" #PlainLiteral">+10</Literal>
  </AnnotationAssertion>
```

Наполнение файла OWL онтологии происходит путем использования данных тегов. Программное обеспечение генерирует типичные OWL теги и заполняет их на основе собранных в Интернете интересов и предпочтений пользователя, создавая три онтологии, необходимые разрабатываемой системе.

Использование языка OWL позволит реализовать систему интернет-рекламы на основе наполнения, хранения и анализа файлов онтологий, включающих в себя мета-онтологию предметной области, онтологический профиль пользователя и онтологическую аннотацию товаров, построенные на терминах мета-онтологии.

Список литературы

1. Афонин С. А., Голомазов Д. Д., Козицын А. С. Использование систем семантического анализа для организации поиска научно-технической информации // Программная инженерия. – 2012. – № 2. – С. 29–34.

2. Вишняков Ю. М., Хоанг С. Б. Персонификация как средство интеллектуализации обслуживания многоканальной информационной системы // Перспективные информационные технологии и интеллектуальные системы. – 2006. – № 2. – С. 29–38.

3. Городецкий В. И., Тушканова О. Н. Онтологии и персонификация профиля пользователя в рекомендующих системах третьего поколения // Онтология проектирования. – 2014. – № 3(13). – Самара: Предприятие "Новая техника". – С. 7-31.

4. Нагорнов Г. Data-переворот в таргетировании медийной рекламы [Электронный ресурс]. – Режим доступа: http://www.cossa.ru/articles/152/57721/

УДК 004.91

Файзуллин Ранис Марсельевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-11
Филиппов Василий Леонидович
направление Информационная безопасность автоматизированных систем
(специалитет), гр. БИС-41

Научный руководитель
Савинов Александр Николаевич, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СБОР И АНАЛИЗ ФЕНОЛОГИЧЕСКИХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ВЕБ-САЙТА

Проблема фенологических исследований в настоящее время имеет особое значение. Хозяйственная деятельность человека, связанная с любой формой природопользования, требует грамотного планирования сроков проведения хозяйственных мероприятий. Данное исследование

становится еще более актуальным в условиях изменяющегося климата с резкими колебаниями местных погодных условий. Только ежегодные наблюдения за текущими сезонными процессами в конкретной местности дадут возможность проследить тенденции изменений природных процессов, что в свою очередь позволит грамотно планировать оптимальные сроки проведения сезонно-зависимых работ [3].

Сбор и анализ фенологических данных принесет практическую пользу при изучении изменения климата, организации работы МЧС и служб ЖКХ, в сельском хозяйстве, лесоводстве, экологии, рыболовстве и т. д.

Составление справочников и фенологических карт тематической направленности во многом способствует успеху при проведении различных мероприятий во всех описанных выше областях. На основе фенологических наблюдений создаются местные календари природы, отражающие сопряженное развитие сезонных явлений у всех фенологических объектов. Такие календари характеризуют типичные, наиболее вероятные сроки наступления сезонных природных явлений в данном месте и по смыслу напоминают климатические справочники, составление которых также базируется на многолетних наблюдениях [2].

Главной проблемой фенологии является сбор и обработка большого количества данных о наступлении фенологических явлений. Информация о наблюдаемых явлениях собирается на основе гражданской науки – добровольными корреспондентами фенологической сети. К сожалению, после распада СССР в результате упразднения права на бесплатную пересылку фенологической корреспонденции большая часть старейших опытных корреспондентов потеряла возможность переписки и пересылки наблюдений. Практически прекратилась практика проведения семинаров. Снизился объем поощрений. Фенологическая сеть начала катастрофически терять корреспондентов [1, 2].

На данный момент многие наблюдатели в России всё ещё ведут фенологическую работу. В настоящее время собранный фенологический архив практически не используется. Уникальные архивные материалы по фенологической тематике, хотя и являются частью общего архива РГО, практически для исследований недоступны. Это связано не только с недостатком места и должных условий хранения, но и с рядом других причин. Поэтому на сегодняшний день эффективность анализа фенологических наблюдений крайне низкая [3].

На сегодняшний день актуальной является задача разработки средств сбора и анализа фенологических наблюдений от пользователей сети Интернет. Предложено решить проблемы фенологии путем разра-

ботки специализированного веб-сайта сбора и анализа фенологических данных. В настоящий момент прямые аналоги сайта для сбора фенологических данных отсутствуют.

Необходимо разработать веб-сайт, в структуру которого будут входить:

- интерфейс, для ввода пользователями данных о наблюдениях фенологических явлений. Фенологические явления – явления живой и неживой природы. Их отличительной чертой является упорядоченность во времени и периодическая ежегодная повторяемость. Для каждого сезона года наблюдается специфический комплекс явлений. Эти явления называются периодическими или сезонными;
- база данных для сохранения информации о сроках и условиях наступления фенологического явления с привязкой к местности. Срок наступления фенологического явления – самый ранний срок наблюдения, но не связанный с искусственным источником тепла;
- алгоритмы автоматического или автоматизированного анализа фенологических явлений. В данных алгоритмах будут использоваться стандартные фенологические понятия, такие как фенологическая константа, среднесуточная температура, срок наступления явления и ключевые точки. Разработанные алгоритмы будут основаны на технологиях Big Data, экспертных систем, интеллектуального анализа данных, нечеткой логики.

Разрабатываемый сайт может найти практическое применение в различных областях науки, техники, производства и человеческой жизни, так как многие из областей человеческой деятельности зависят от сезонных метеорологических и природных процессов. Проект позволит решить следующие задачи:

- сбор и накопление возможно более полной информации о сезонных событиях в явлениях живой и неживой природы;
- сбор и накопление информации о количестве кормов;
- сравнение хода сезонных явлений в разные годы;
- формирование разветвленной сети наблюдателей, которая позволит детально описывать фенологические процессы, корректировать невольные ошибки и снизит риск пропуска явлений;
- исследование корреляции сроков фенологических явлений;
- отслеживание процессов изменения климата.

Следует восстановить и увеличить сеть добровольных корреспондентов-фенологов для сбора уникальных наземных фенологических наблюдений. Совершенно необходимо создать структуру, способную на современном уровне координировать и направлять наблюдения и ис-

следования в определенное русло хозяйственных и научных интересов общества. На основе полученных данных появляется возможность предсказания урожая для сельского хозяйства, миграции рыб, птиц и животных для охотничье-промыслового хозяйства, рыболовства и т. д. Структурой, позволяющей достигнуть представленных результатов, мог бы стать разрабатываемый портал сбора фенологических наблюдений.

Список литературы

1. Ahas R., Aasa A., Fedotova V. Phenological changes have different rhythm for maritime and continental Europa // Institute Geography, University of Tartu, Institute of Botany (RAN), 2002.
2. Федотова В. Г. Основы фенологии. Ч. 2. Практическая фенология. – СПб.: СПбГЭТУ «ЛЭТИ», 2002. – 35 с.
3. Федотова В. Г. Основы фенологии. Ч. 1. Теоретический курс. – СПб.: СПбГЭТУ «ЛЭТИ», 2002. – 39 с.
4. Шульц Г. Э. Общая фенология. – Л.: Наука, Ленингр. отд., 1981. – 188 с.

УДК 004.93

Федоров Ян Владимирович
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-31

Научный руководитель
Ипатов Юрий Аркадьевич, канд. техн. наук, доцент,
кафедра информатики
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СОВРЕМЕННЫЕ МЕТОДЫ ТЕХНИЧЕСКОГО ЗРЕНИЯ В РЕШЕНИИ ЗАДАЧ НАЗЕМНОЙ ЛЕСНОЙ ТАКСАЦИИ

На сегодняшний день методы и подходы технического зрения способны частично или полностью заменить человека при решении таких задач, как обнаружение, распознавание и измерение параметров объектов на сложном статистически неоднородном фоне. Так, в области лесной таксации можно выделить два научно-технических направления: первое использует крупномасштабные (данные ДДЗ, аэрофотосъемка), а второе – мелкомасштабные (снимки наземной лесной таксации) изображения.

Для первого направления созданы и широко применяются на практике автоматизированные решения: аппаратно-программные средства,

реализующие методы цифровой обработки изображений и распознавания образов [1]. Для второго направления в лесном комплексе страны для определения таксационных параметров (относительная полнота древостоя, процент проективного покрытия растений и освещенность верхнего яруса леса) удалось разработать адекватные математические модели цифровых изображений и синтезировать оптимальные алгоритмы обнаружения заданных визуальных параметров [2, 3].

Маршрут наземной таксации для измерений в заданном выделе

В работах по лесной таксации исследуемую территорию принято разбивать на лесные кварталы и составные части – выделы. Для быстрого и эффективного осуществления работ необходимо определить маршрут наземной лесной таксации и точно знать параметры выдела, такие как ширина и длина выдела, шаг измерений. На рисунке представлена схематическая карта выдела с основными параметрами, которые необходимо знать для проведения таксационных работ. В каждой точке маршрута осуществляется фотосъемка определенных сцен [2] и измерение точных координатно-временных данных [4].

Для решения задачи автоматизированного расчета маршрутов наземной таксации, рассчитываются: длина и ширина лесного выдела (в метрах), шаг (в метрах), начальная точка измерений (географические координаты по GPS/ГЛОНАСС) и направление маршрута (географические направления, например, северо-восток). Так, коммерческие программы ГИС на сегодняшний день очень разнообразны и представляют широкий спектр систем для задач разного класса. Наиболее хорошо себя зарекомендовали для работы с мелкомасштабными «природными» кар-

тами (геология, сельское хозяйство, навигация, экология и т.п.) такие ГИС, как ArcInfo, ArcView GIS и MapInfo, весьма распространенные в мире [5, 6].

Для создания слоев, содержащих необходимые сведения, для ГИС используются данные дистанционного зондирования Земли, аэрофотосъемка и космические снимки. В этом направлении созданы и широко применяются автоматизированные решения: аппаратно-программные средства, реализующие методы цифровой обработки изображений и распознавания образов [6].

Созданный подход обеспечивает статистическую достоверность результатов измерений на заданных выделах и пробных площадях по входным параметрам. Использование данного метода упрощает и ускорят работы таксаторов, а также обеспечивает хорошую систематизацию получающихся данных.

Для цифровых изображений, полученных в точках замера по маршруту (см. рисунок), предусмотрена интеграция данных, полученных со спутниковых радионавигационных систем по протоколу EXIF. Такую возможность обеспечивают современные цифровые аппараты со встроенными и внешними GPS/ГЛОНАСС приемниками или же КПК с соответствующим модулем.

Имеются разные типы радионавигационного оборудования, обеспечивающего получение координатно-временных данных. Однако для разрабатываемого программного комплекса существует функциональные и технические требования, которые будут влиять на конечную производительность системы.

Список литературы

1. Шовенгердт Р. А. Дистанционное зондирование. Модели и методы обработки изображений. – М.: Техносфера, 2010. – 582 с.

2. Ипатов Ю. А. Автоматизированная классификация сцен наземной лесной таксации с использованием статистического анализа текстур // Математические методы распознавания образов: сб. докладов 15-й Всероссийской конференции, г. Петрозаводск. – М.: МАКС Пресс, 2011. – С. 575-577.

3. Кревецкий А. В., Ипатов Ю. А. Комплексированное оптико-локационное обнаружение и оценка параметров объектов наземной лесной таксации // Успехи современной радиоэлектроники. Радиотехника. – 2011. – № 5. – С. 56-60.

4. Использование GPS в лесной сертификации // ЛесПромИнформ. – 2007. – № 1(41).

5. Митчелл Энди. Руководство ESRI по ГИС анализу. Том 1: Географические закономерности и взаимодействия / пер. с англ. – М.: МГУ, 2001. – 190 с.

6. Журкин И. Г., Шайтура С. В. Геоинформационные системы / под общ. ред. И. Г. Журкина. – М.: Кудиц-Пресс, 2009. – 272 с.

УДК 004.31

Фёдоров Ян Владимирович,
Подоплелов Дмитрий Сергеевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Морохин Дмитрий Витальевич, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИССЛЕДОВАНИЕ СПОСОБОВ ВЗАИМОДЕЙСТВИЯ КОНТРОЛЛЕРОВ НА ПРИМЕРЕ КОНТРОЛЛЕРА ATMEGA 328

Рассматривается задача исследования способов взаимодействия контроллеров, которые смогут не только изучить, понять, но и самостоятельно реализовать школьники. Данная работа выполнялась в рамках сотрудничества кафедры ИВС ПГТУ и STEM-центра, действующего на базе факультета информатики и вычислительной техники. По полученным результатам была разработана и реализована искусственная ель с гирляндой, вращающаяся вокруг своей оси.

Способы взаимодействия контроллеров

Для взаимодействия двух контроллеров можно использовать несколько простых по техническому решению способов на основе:

1) фоторезистора и светодиода;
2) пьезоэлемента и микрофона;
3) приёмопередатчиков Bluetooth;
4) радиоприёмника и радиопередатчика на 433 МГц.

Проведённые в рамках данной работы исследования позволили понять и изучить принципы передачи сигналов беспроводным способом, возникающие ограничения и влияние различных помех на передаваемый сигнал. В первом случае для взаимодействия контроллеров использовалась световая волна, по втором – звуковой сигнал, а в третьем и в четвёртом – радиосигналы разной частоты.

В процессе исследования была поставлена цель: определить самый эффективный способ передачи сигналов между контроллерами.

Критериями эффективности были выбраны три показателя: дальность действия, помехоустойчивость и стоимость реализации.

Был проведён ряд экспериментов, в которых между контроллерами Arduino Uno подавались сигналы с использованием различных приёмников и передатчиков.

По первым двум критериям более эффективным оказался радиоинтерфейс Bluetooth, работающий в диапазоне частот 2,4 ГГц. В ходе экспериментов в обычных условиях (т.е. безэховая камера не использовалась) дальность данного интерфейса составила 13,5 м, при этом приём сигнала осуществлялся без каких-либо помех. На втором месте оказался способ, где использовались радиоприёмник и радиопередатчик на 433 МГц. В этом случае дальность составила 2,5-3 м, здесь также не было помех. Дальность передачи между контроллерами при использовании пьезоэлемента и микрофона была немного меньше – 1,3 м. Но в этом случае помеху звуковому сигналу представляли находившийся рядом системный блок компьютера и громкий голос человека. Последний способ со светодиодом и фоторезистором оказался менее эффективным. Его дальность составила 11-12 см, а с препятствиями в виде листа бумаги – всего 2 см.

Таким образом, можно сделать вывод, что способ взаимодействия с радиопередатчиком и радиоприёмником может использоваться в радиоуправляемых игрушках, интерфейс Bluetooth – при связи между двумя устройствами, например телефонами.

Способ с пьезоэлементом и микрофоном может использоваться при записи мелодии, когда на пьезоэлемент загружена мелодия, а микрофон улавливает её и передаёт значения на экран компьютера.

В дальнейшем можно перевести экранные значения на ноты и воспроизвести с другого устройства, но такой способ будет иметь много помех в виде человеческого голоса.

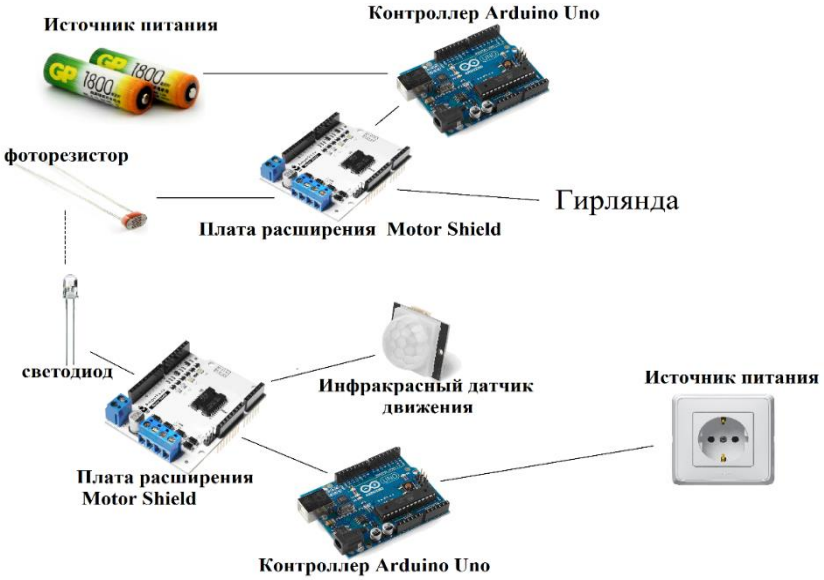
Несмотря на то, что радиоинтерфейс показал лучшие характеристики по критериям «дальность-помехоустойчивость», для проекта «Искусственная ель» он оказался более дорогостоящим, чем остальные. Проанализировав остальные способы относительно простоты реализации, пришли в выводу, что в данном случае устранить помехи при использовании светодиода будет легче, поэтому в проекте был использован именно этот способ взаимодействия контроллеров. Состав используемого оборудования приведён на рисунке.

Описание структуры и принципа действия конструкции

Ёлочка состоит из деревянного стержня и прикрепленных к ней лепестков, сделанных из белых пластиковых бутылок. Края лепестков надрезали таким образом, чтобы они получились «пушистыми». К нижнему концу оси прикрепили круглое пластиковое основание для опоры.

Для верхнего и нижнего блоков отлично подошли упаковки из подCD/DVD дисков «cakebox». В верхнем блоке центральную ось пол-

ностью спилили за ненадобностью. К крышке блока основанием приклеили ёлочку. В нижнем блоке центральную ось спилили не полностью: так как она полая внутри, в ней отлично зафиксировался электродвигатель, который будет вращать верхний блок вместе с ёлочкой. Для этого пришлось перевернуть бокс для дисков вверх дном и на вращающуюся ось двигателя закрепить верхнюю часть конструкции. Для уменьшения нагрузки на двигатель, а также для лучшей опоры ко дну верхнего блока прикрепили три колесика, которые ездят по нижнему блоку.



Состав используемого оборудования

Для определения начала вращения нижний блок должен передавать сигнал верхнему блоку. Это было реализовано посредством установки светодиода с внешней стороны верхней части нижнего блока и фоторезистора в этой же области на верхнем блоке.

Для гирлянды были взяты белые светодиоды. Исходя из возможной мощности электропитания гирлянды были рассчитаны метод соединения светодиодов и их количество. Было решено использовать метод последовательно-параллельного соединения: четыре параллельно соеди-

ненных ветви, в каждой по три последовательно соединенных светодиода на каждые из четырех цветов лампочек гирлянды. Светодиоды соединяли проводами посредством пайки так, чтобы они были равномерно распределены вдоль всей гирлянды. На каждый светодиод надели разноцветные прозрачные бусины, хорошо рассеивающие свет. Для изоляции, прочности и эстетичности вся гирлянда была обмотана белой изолентой.

Внутри верхнего блока находится контроллер Arduino Uno, который управляет гирляндой и принимает сигнал с фоторезистора. К контроллеру подключены две платы расширения MotorShield, которые обеспечивают необходимое напряжение и мощность тока, что необходимо для питания гирлянды. Каждый канал платы расширения питает цепь светодиодов отдельного цвета, что и объясняет количество используемых плат расширения. Все эти элементы питаются от блока из восьми аккумуляторных батарей типа «АА».

В нижнем блоке также находится контроллер Arduino Uno с подключённой к нему платой MotorShield. В данном случае MotorShield необходима для питания двигателя. Контроллер управляет двигателем, светодиодом, который передаёт сигнал на фоторезистор, а также принимает сигнал с инфракрасного датчика движения, который определяет движущиеся рядом объекты.

Датчик движения встроен в фигурку пенопластового снеговика, которая прикреплена к неподвижному блоку. Это позволяет датчику более точно фиксировать изменения вблизи ёлочки, а снеговик гармонично вписывается в общий вид конструкции. Питание элементов нижнего блока происходит за счет инверторного блока питания, который подключается к сети переменного тока 220 В.

Список литературы

1. Бачинин А., Панкратов В., Накоряков В. Основы программирования микроконтроллеров. – М.: ООО «Амперка», 2013. – 207 с.

2. Васяева Е. С., Васяева Н. С. Специфика обучения школьников основам робототехники // Ресурсы робототехнических конструкций как инструмента воспитания и образования детей и юношества: сборник статей по материалам круглого стола в рамках XIX Вавиловских чтений – международной междисциплинарной научной конференции. – Йошкар-Ола: Поволжский государственный технологический университет, 2016. – С. 88-94.

3. Уэйт М., Прата С., Мартин Д. Язык СИ. Руководство для начинающих / пер. с англ. – М.: Мир, 1988. – 512 с., ил.

УДК 004.31

Федоров Ян Владимирович
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41
Тоцкий Алексей Андреевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Васяева Елена Семеновна, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СВЕТОДИОДНАЯ ГИРЛЯНДА НА КОНТРОЛЛЕРЕ ATMEGA 8

В рамках кружка робототехники, действующего при на кафедре ИВС ПГТУ, была поставлена задача разработать светодиодную гирлянду и управляющую ей схему. Одним из важных критериев разработки гирлянды была как можно меньшая стоимость и простота устройства гирлянды, достаточная для понимания учащимися, соответствующая их уровню знаний.

Управляющая схема (рис. 1) распаяна на макетной плате, это решение обусловлено дешевизной данного решения и ограниченным временем исполнения. Главной частью схемы был выбран микроконтроллер ATMega 8 в исполнении 28-выводного DIP-корпуса для удобства его распайки. Прежде всего мы остановились именно на этом решении из-за его совместимости со средой разработки Arduino IDE, уже знакомом воспитанникам кружка. Кроме него, на плате распаяна минимальная обвязка в виде кварцевого резонатора, фильтрующего высокочастотные помехи по питанию конденсатора и стягивающего резистора, подключенного к выводу RESET. К выводам осуществляется подключение нескольких светодиодов, которыми микроконтроллер будет управлять, включая и выключая их.

Светодиоды подключены к микроконтроллеру по схеме с общим катодом (т. е. по схеме «питание – резистор – светодиод – вывод микроконтроллера», а не «вывод микроконтроллера – резистор – светодиод – земля»), так как для каждого порта максимально допустимый входной ток микроконтроллера больше максимально допустимого выходного

тока. Также это обеспечивает меньшую суммарную нагрузку на микроконтроллер при одновременном включении всех светодиодов.

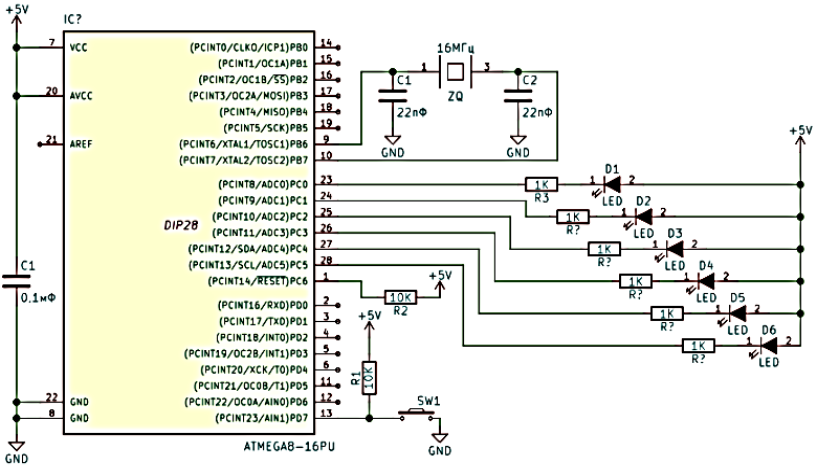


Рис. 1. Управляющая схема

Микроконтроллер ATMega 8 способен работать от внутреннего осциллятора на 8 МГц, но для совместимости с загрузчиком Arduino NG, который работает на частоте 16МГц, было решено использовать кварцевый резонатор с двумя конденсаторами на 22 пФ.

Устройство планируется питать от USB. В связи с тем, что в последнее время распространены зарядные устройства на 5 вольт с USB-выходами, а также благодаря тому, что микроконтроллер работает именно от этого напряжения, было решено отказаться от какой-либо самостоятельной стабилизации напряжения, так как она реализована в самом зарядном устройстве. Трехдневное тестирование работы данной схемы от ЗУ телефона подтвердило правильность принятого решения.

Для фильтрации высокочастотных помех на входе питания используется конденсатор на 0,1 мФ. Это обеспечивает более стабильное питание микроконтроллера путём сглаживания падений напряжения, если таковые происходят.

Кнопка на схеме управления служит для переключения режимов свечения гирлянды. Она подключена к микроконтроллеру по схеме с потягивающим резистором.

Управляющая программа загружается в микроконтроллер при помощи Arduino Uno R3, в который заранее прошивается скетч Arduino ISP. Этот скетч был специально разработан для прошивки микроконтроллеров серии Atmel AVR по интерфейсу SPI. После чего подключаются выводы RESET микроконтроллера к выводу D9 на Arduino, выводы земли, а также одноименные выводы MOSI, MISO и SCL ATMega 8 и Arduino. Завершающим этапом является загрузка управляющей программы с выбором Arduino Uno в качестве программатора.

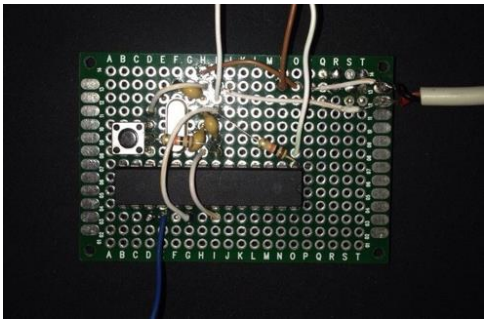


Рис. 2. Фото прототипа управляющей схемы

В результате получилась схема с достаточно низкой стоимостью (рис. 2), которая может быть запрограммирована на разные режимы свечения.

В итоге были приобретены навыки подготовки к работе и непосредственно работы с микроконтроллерами (такие, как их обвязка и загрузка управляющей программы через программатор). Также учащиеся кружка робототехники приобретут или закрепят навыки припаивания деталей к плате и управления свечением гирлянды посредством написания программы для микроконтроллера, с последующей его загрузкой через программатор.

Список литературы

1. Блум Джереми, Изучаем Arduino: инструменты и методы технического волшебства; пер. с англ. – СПб.: БХВ-Петербург, 2015. – 336 с.

2. Минимальная обвязка ATmega8, 168, 328 [Электронный ресурс]. – URL: http://zelectro.cc/atmega_main

3. ATmega8L datasheet [Электронный ресурс]. – URL: http://www.atmel.com/Images/Atmel-2486-8-bit-AVR-microcontroller-ATmega8_L_datasheet.pdf.

4. Using an Arduino as an AVR ISP (In-System Programmer) [Электронный ресурс]. – URL: https://www.arduino.cc/en/Tutorial/ArduinoISP.

УДК 004.056

Филиппов Василий Леонидович
направление Информационная безопасность автоматизированных систем (специалитет), гр. БИС-41

Научный руководитель
Соловьева Татьяна Алексеевна, канд. филос. наук, доцент,
кафедра философии
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИНФОРМАЦИОННАЯ ВОЙНА В XXI ВЕКЕ: МИФ ИЛИ РЕАЛЬНОСТЬ?

Перед тем как рассматривать проблему информационной войны, следует определить понятия и отметить её актуальность.

Информация (от лат. informatio, разъяснение, изложение, осведомленность) – общенаучное понятие, связанное с объективными свойствами материи и их отражением в человеческом сознании. Это необходимый ресурс деятельности человека, отделяющий его от остального мира. Первоначально ученый физик Томас Рон использовал термин «информационная война» в отчете, подготовленным им в 1976 году для компании «Boeing» и названный «Системы оружия и информационная война». Здесь Т. Рон указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время она становится и уязвимой целью как в военное, так и в мирное время. Этот отчет и можно считать первым упоминанием термина «информационная война».

На сегодняшний день у всех стран имеется своя армия и своё оружие. В ряде стран есть даже ядерное оружие, поэтому вести войну традиционными методами – дорого. Дорого как по материальным средствам, так и по человеческим жизням. Кроме того, проводя боевые действия в чужой стране, можно потерять авторитет перед другими государствами. Исходя из этого, гораздо выгоднее использовать информационное оружие и вести информационную войну.

Современный век – век информации. Сегодня каждый человек старается как можно больше узнать, получить как можно больше информации, и он её получает. Огромные потоки информации льются на человека информационным дождём.

Но, несмотря на объёмы, суммарная ценность всей полученной информации невелика, так как больше половины – это всевозможная реклама. То, что остается, нуждается в проверке на достоверность.

Проблема современного человека в том, что он, спешит, ему никогда не хватает времени, поэтому получая очередную порцию информации, он скорее поверит в её правдивость, чем будет тратить своё время, на поиск доказательств или источника. Учитывая этот фактор, человеком можно легко управлять, подкидывая сфабрикованные факты, поверив в которые, он примет ту или иную точку зрения – это и есть проявления информационной войны.

Говоря об информационной войне, нужно вначале понять, что она из себя представляет. Следуя определению, информационная война – это воздействие на гражданское население или военнослужащих другого государства путём распространения определённой информации.

Основные черты информационной войны:

1. Не использование психоактивных веществ, прямого шантажа и запугивания, подкупа, физического воздействия и т.п.

2. Объектом является как массовое сознание, так и индивидуальное. Воздействие применяется на индивидуальное лицо, если от его решения зависит принятие решений по интересующим противоборствующую сторону вопросам.

3. Воздействие ложной информацией может осуществляться как в условиях информационного вакуума, так и в условиях информационного шума.

4. Навязывание чужих идей, способствующих саморазрушению. Именно эта черта делает информационную войну войной.

5. Средствами воздействия являются любые средства передачи информации.

6. Информационное воздействие содержит искажение фактов, навязывает представление, дезориентирующее противника, формирует восприятие, выгодное воздействующей стороне.

Чтобы контролировать и управлять происходящими процессами в обществе, используется информационное оружие, которое представляет собой средства:

- уничтожения, искажения или хищения информации;
- преодоления систем защиты;
- ограничения допуска законных пользователей;
- дезорганизации работы технических средств, компьютерных систем.

К *информационному оружию* можно отнести:

1) компьютерные вирусы – представляют собой программные разработки, способные проникать в среду компьютерных систем и наносить разного рода повреждения;

2) логические бомбы (программные закладки) – программный код, который является безвредным до выполнения определенного условия, после которого реализуется логический механизм;

3) средства подавления информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного управления;

4) средства нейтрализации тестовых программ;

5) различного рода ошибки, сознательно вводимые в программное обеспечение объекта.

Политика применения информационного оружия носит наступательный характер. В реестре современных технологий сетевых войн и новых типов оружия есть оружие, используемое в области идеологии, СМИ, пропаганды, образования, культуры. Этим оружием является тщательно отобранная информация, повторенная нужное количество раз по необходимым информационным каналам.

Если оружие применяется, значит существует противник, который его создает, активирует и направляет, и объект, на который оружие нацелено.

Существуют *объекты информационного поражения*:

1) правящая элита, т.е. люди управляющее государством;

2) материальные объекты и инфраструктура.

Информационное влияние считается оружием массового поражения и имеет много общего с ядерным оружием. Кроме того, то, что зачастую информационная атака носит неявный, скрытый характер, это оружие оказывает непрерывное воздействие на большое количество людей. Также для него характерен как немедленный, так и отложенный поражающий эффект, эффект закрепления и воспроизводства поражающего действия. Фактически это же происходит при взрыве ядерного боеприпаса. Вначале – ударная волна, световое излучение, радиоактивное поражение, все это ощущается немедленно. Отложенное, закрепленное и воспроизводящееся воздействие – это длительное заражение местности, лучевая болезнь, генетические мутации, затрагивающие многие поколения живых организмов.

К результатам информационного оружия, кроме сиюминутной убежденности в достоверности некоего навязываемого факта, относится и полный аналог заражения и ментальных и социальных мутаций. Данное инфицирование подрывной идеологией способно вызывать распространяющиеся на многие годы последствия, например перерождение элиты, потерянное поколение, поколение несбывшихся надежд, перемены в менталитете населения.

Чтобы ответить на вопрос, действительно ли в мире ведётся активная информационная война или нет, необходимо провести анализ. Ана-

лиз будет проводиться на примере России как на самой крупной по территории стране, которая имеет вес в мировом сообществе.

Рассмотрим для начала такую проблему, как нравственный упадок молодёжи. Известно, что молодёжь – это будущее страны. Именно она будет строить и развивать свою родину. Исходя из этого, если какая-либо страна захочет захватить другую страну, ей достаточно будет навязать молодёжи свои ценности и порядки, что хорошо видно на примере России. После распада СССР в страну хлынул поток западной культуры. Неокрепшие умы молодых людей поддались влиянию Запада, формировавшиеся десятилетиями ценности были быстро заменены на ложные. Если раньше большинство людей уже со школьной скамьи рвались открывать мир, покорять космос и развивать индустрию ради благополучия страны, то сейчас цель молодёжи – иметь как можно больше денег, чтобы ни в чём себе не отказывать и жить беззаботной жизнью, что характерно для потребительского общества. Именно этот тип жизни был навязан Западом, и молодёжь, которая воспитывалась новым временем, превращалась не в творцов, а в потребителей.

Помимо планов на будущее изменились и образы героев. Если раньше герой был положительным персонажем, которому присущи такие качества, как мужество, отвага, милосердие и справедливость, то сейчас у героев появились вредные привычки, они стали жестокими, циничными и безнравственными. Поэтому поведение, которое раньше считалось неприемлемым, сейчас становится нормой. Отсюда – и падение нравственности. Исходя из этого примера, хорошо прослеживаются черты, направление «ударов» и результаты информационной войны.

Далее можно рассмотреть ещё одну проблему России – это национализм, который в последнее время набирает обороты по популярности среди молодёжи. Хочется отметить, что в Советском Союзе пропагандировалась дружба народов и все нации приравнивалась друг к другу, но уже к периоду правления М. С. Горбачёва западная культура начала просачиваться сквозь толстые стены железного занавеса. Тогда зародилась первая организация, чьей идеологией являлась по сути фашистская идеология. После же распада Советского Союза и в течение ближайших 5-10 лет образовался не один десяток националистических движений.

Такие расколы происходят внутри одного класса, это приводит к сильному дроблению общества, что значительно ослабляет страну. На этом примере также видны черты и разрушительное влияние информационной войны.

В отличие от таких средств ведения информационной войны, как навязывание своей точки зрения, существует ещё воздействие с помощью искажением фактов. Искажение фактов зачастую используют в средствах массовой информации.

Усугубляет проблему то, что социально-психологическая составляющая информационной войны уже сформировала отношение к ней у большей части населения на подсознательном уровне. В течение последнего десятилетия воздействие на сознание человека резко усилилось в связи с широким распространением Интернет-сети, которая разрушила границы между странами и стала мощнейшим оружием в манипулировании сознанием.

Сегодня на вопрос: информационная война – это миф или реальность, можно с уверенностью ответить, что это реальность. Зная это, нужно как можно тщательней проверять полученную информацию. Кто знает, может, кому-то выгодно, чтобы мы поверили в то, о чём всюду говорится.

Список литературы

1. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства. – М.: ФИЗМАТЛИТ, 2010. – 228 с.

2. Иванов В. Н., Сергеев В. К. Русский мир и социальные реалии. – М., 2008.

3. Новиков Д. А. Социальные сети: модели информационного влияния, управления и противоборства. – М.: ФИЗМАТЛИТ, 2010.

4. Расторгуев С. П. Философия информационной войны. – М.: Аутопан, 2003. – 496 с.

5. Ткаченко С. В. Информационная война против России. – СПб.: Питер, 2011. – 226 с.

УДК 004.056

Филиппов Василий Леонидович
направление Информационная безопасность автоматизированных систем (специалитет), гр. БИС-41

Научный руководитель
Кречетов Александр Александрович, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

МЕТОДЫ И ИНСТРУМЕНТЫ УНИЧТОЖЕНИЯ ДАННЫХ

Уничтожение информации может происходить планово (т.е. по истечении срока хранения информации, списание носителя информации и

т.д.) или экстренно (в случае чрезвычайной ситуации). Такая информация, как государственная тайна, персональные данные, коммерческая тайна, должна удаляться по принципу гарантированного уничтожения информации, так как передача её третьим лицам будет иметь критический характер.

Гарантированное уничтожение может производиться различными методами: физическим, программным, механическим, термическим и химическим. Гарантированное уничтожение данными методами позволяет исключить возможность восстановления информации с носителя, что не даст злоумышленникам шанса получить в свое распоряжение критически важную информацию.

В настоящее время выбор метода ликвидации информации на магнитных носителях не является тривиальным и представляет достаточно сложную многокритериальную задачу. Среди методов уничтожения имеются как относительно простые, которые сможет выполнить работник, не имеющий высокой квалификации, например программный, так и методы, применение которых подразумевает использование сложных средств контроля и обеспечения безопасности оператора, например химический метод.

Самое широкое применение нашли: метод физического воздействия магнитным полем, механический и программный. Результаты сравнения данных методов представлены в таблице.

Сравнение способов уничтожения информации

Средство уничтожения	Способ уничтожения	Скорость уничтожения	Риск восстановления	Возможность работы магнитного носителя после уничтожения	Целесообразность применения данного средства уничтожения информации
Импульс 6В	Физический	Несколько секунд	Гарантированное уничтожение	Носитель уничтожен	1) Экстренные ситуации, при которых возникает срочная необходимость уничтожения информации любой ценой; 2) списание магнитного носителя
Paragon Disk Wiper	Программный	Несколько часов	В зависимости и от алгоритма уничтожения	Возможна эксплуатация носителя	Плановое уничтожение информации
Устройство «Унидиск»	Механический	Несколько секунд	Восстановление маловероятно	Носитель уничтожен	1) Экстренное уничтожение информации любой ценой; 2) списание носителя информации

При сравнении методов уничтожения информации на магнитных носителях выяснилось, что часть методов приводит к уничтожению носителя или является слишком дорогим для единичных случаев уничтожения информации.

Шредирование актуально только для уничтожения большого количества жестких дисков, и уничтожение большого количества дисков делает почти невозможным восстановление информации из отходов.

Уничтожение носителя информации пробойником актуально только для носителя, диски которого имеют стеклянную основу; на носителях, имеющих металлическую основу диска, информация будет уничтожена только в местах пробоя.

Уничтожение информации физическим методом актуально как для экстренных случаев уничтожения информации, так и для планового уничтожения информации. Оно гарантирует уничтожение информации. Например, устройство «Импульс – 6В», приведенный на рисунке.

Внешний вид устройства «Импульс – 6В»

Уничтожение информации программным методом актуально для планового уничтожения информации с работоспособного НЖМД, для экстренного уничтожения этот способ не подходит по причине долгого процесса перезаписи данных. После перезаписи НЖМД готов к работе, эту операцию можно повторять многократно, при этом риск восстановления крайне мал и стремится к нулю.

На данный момент существует много алгоритмов для уничтожения информации программным методом, введенных в стандарты разных стран, например:

- DoD 5220.22-M – стандарт Министерства обороны США, принятый в 1995 году, предполагает 3 цикла перезаписи. В некоторых источ-

никах указано, что для удаления совершенно секретных данных армия США его не использует;

- ГОСТ Р50739-95 – Российский стандарт, принятый и введенный в действие в феврале 1995 года. Предусматривает запись нулями в каждый байт каждого сектора для систем с 4-6 класса защиты и запись псевдослучайных чисел в каждый байт каждого сектора для систем 1-3 класса защиты;
- алгоритм Брюса Шнайера – алгоритм, предложенный Брюсом Шнайером, впервые представленный в 1996 году. Алгоритм состоит из семи циклов, ориентированных на полное удаление информации на жестких магнитных дисках;
- VSITR – Немецкий стандарт, разработанный в 1999 году. Состоит из 7 циклов перезаписи;
- HMG Infosec No.5 – Британский стандарт. Первоначально область перезаписывается маской, состоящей из одного символа, затем – его двоичным дополнением, а после этого любым случайным символом.

В настоящее время такие федеральные органы исполнительной власти Российской Федерации, как Роскомнадзор, ФСТЭК РФ и ФСБ России требуют уничтожать информацию, в частности при передаче носителей между пользователями в сторонние организации для ремонта или утилизации.

Любое государство стремится обеспечить контроль над информацией, связанной с обеспечением национальной безопасности. И поэтому к программному обеспечению, которое поставляется на рынок и используется для построения информационных систем, предъявляются особые требования.

Использование сертифицированных комплексных систем защиты информации, предназначенные для защиты конфиденциальной информации, а также для защиты информации, содержащей сведения, составляющие государственную тайну, необходимо в соответствии с закрепленными в приказах и руководящих документах регулятора.

В связи с этим производители программного обеспечения, осуществляющего гарантированное уничтожение данных, обязаны учитывать требования, налагаемые национальными законами на информационные системы, предназначенные для работы с конфиденциальной информацией.

Поэтому в большинстве систем защиты информации с подсистемами гарантированного уничтожения данных используется Российский стандарт ГОСТ Р50739-95, предусматривающий запись нулями в каждый байт каждого сектора для систем с 4-6 класса защиты и запись псевдо-

случайных чисел в каждый байт каждого сектора для систем 1-3 класса защиты. Однако данный ГОСТ содержит лишь формулировку «Очистка должна производиться путём записи маскирующей информации в память при её освобождении перераспределении», которая не содержит какой-либо детализации относительно порядка перезаписи, количества циклов и битовых масок. В то же время существует действующий руководящий документ Государственной технической комиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», изданный в 1992 году и предусматривающий ряд требований к механизму уничтожения информации для систем определённых классов защищенности. В частности, для классов 3А и 2А «Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов)», для класса 1Г предусмотрена однократная перезапись.

Видно, что данные стандарты были разработаны во времена, когда информационные технологии только начали входить в повседневную жизнь бизнеса, но на текущем уровне развития технологий данные алгоритмы недостаточны для обеспечения ИБ и не позволяют осуществлять защиту информации на должном уровне.

Также для обеспечения качественного уничтожения информации организацией должен быть сформулирован список организационных мер, полностью регулирующих процесс, обеспечивая максимальное качество выполнения работы.

В силу вышесказанного нами начато проведение исследований нахождения оптимального алгоритма, т.е. установление необходимого количества циклов перезаписи, а также нахождение наилучших масок для каждого цикла перезаписи.

Список литературы

1. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 06.07.2016) // СПС КонсультантПлюс. (дата обращения 04.11.2016);

2. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. – М.: Гостехкомиссия РФ, 1992. – 24 с.

3. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – М.: Гостехкомиссия РФ, 1992. – 18 с.

4. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. – М.: Госстандарт РФ, 1995. – 10 с.

5. Беседин Д. И., Боборыкин С. Н., Рыжиков С. С. Предотвращение утечки информации, хранящейся в накопителях на жестких магнитных дисках // Специальная техника. – 2001. – № 1.

6. Боборыкин С. Н., Рыжиков С. С. Оценка эффективности средств уничтожения информации, хранящейся в накопителях на жестких магнитных дисках // Специальная техника. – 2011. – № 3. – 6 с.

7. Болдырев А. И., Сталенков С. Е. Надежное стирание информации – миф или реальность? // Защита информации. Конфидент. – 2001. – № 1.

8. Коженевский С. Методы гарантированного уничтожения данных на жестких магнитных дисках [Электронный ресурс] / С. Коженевский // Публикации ЕПОС. – 2010. – 16 с. – URL: http://www.epos.ua/view.php/pubs_2? subaction=showfull&id=1043964000&archive=&start_from=&ucat=2&. (дата обращения 04.11.2016).

УДК 004.8

Филиппов Василий Леонидович
направление Информационная безопасность автоматизированных систем (специалитет), гр. БИС-41

Научные руководители:
Соловьева Татьяна Алексеевна, канд. филос. наук, доцент,
кафедра философии
Савинов Александр Николаевич, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ПРОБЛЕМА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА. ЧЕЛОВЕК ИЛИ МАШИНА?

Имеется несколько определений искусственного интеллекта.

1. Научное направление, в рамках которого ставятся и решаются задачи аппаратного или программного моделирования тех видов человеческой деятельности, которые традиционно считаются интеллектуальными [1].

2. Свойство интеллектуальных систем выполнять функции (творческие), которые традиционно считаются прерогативой человека. При этом интеллектуальная система – это техническая или программная си-

стема, способная решать задачи, традиционно считающиеся творческими, принадлежащие конкретной предметной области, знания о которой хранятся в памяти такой системы. Структура интеллектуальной системы включает три основных блока: базу знаний, решатель и интеллектуальный интерфейс, позволяющий вести общение с ЭВМ без специальных программ для ввода данных.

3. Наука под названием «Искусственный интеллект» входит в комплекс компьютерных наук, а создаваемые на её основе технологии к информационным технологиям. Задачей этой науки является воссоздание с помощью вычислительных систем и иных искусственных устройств разумных рассуждений и действий.

Может ли машина мыслить? Может ли она мыслить подобно человеческому уму или же программы будут использоваться как инструмент для решения прикладных задач? Может ли машина действовать разумно? Может ли она иметь разум и сознание так же, как их имеет человек? Схожи ли по своей природе человеческий и искусственный интеллект? Эти вопросы волнуют ученых с 1950 года.

Само понятие «интеллект» происходит от латинского ум, рассудок, восприятие, разум [2]. Таким образом, интеллектом называют способность мозга решать интеллектуальные задачи путем приобретения, запоминания и целенаправленного преобразования знания в процессе обучения на опыте и адаптации к разнообразным обстоятельствам.

Одной из проблем искусственного интеллекта является определение критериев, по которым можно установить, является ли субъект мыслящим. А. Тьюрингом была предложена концепция эмпирического эксперимента для определения того, является ли машина мыслящей. Этот эксперимент позже был назван тестом Тьюринга. Он заключался во взаимодействии человека и машины.

Стандартная интерпретация этого теста звучит следующим образом: «Человек взаимодействует с одним компьютером и одним человеком. На основании ответов на вопросы он должен определить, с кем он разговаривает: с человеком или компьютерной программой. Задача компьютерной программы – ввести человека в заблуждение, заставив сделать неверный выбор».

Однако мысленный эксперимент «Китайская комната» Джона Сёрля – аргумент в пользу того, что прохождение теста Тьюринга не является критерием наличия у машины подлинного процесса мышления. Можно и дальше приводить примеры критериев, по которым «машинный мозг» можно считать способным к мыслительной деятельности и тут же находить им опровержения.

Таким образом, единого ответа на вопрос о том, что такое искусственный интеллект и как его можно выделить среди других программ, не существует.

Также в философии имеются гипотезы искусственного интеллекта, такие как «сильный» и «слабый». Теория сильного искусственного интеллекта предполагает, что искусственный интеллект разумен, подобно человеческому уму, и способен осознавать себя. Теория слабого искусственного интеллекта отвергает такую возможность. Это подобие программы для выполнения определенных задач. Понятие «сильного» более полно отображает саму концепцию искусственного интеллекта, так как предполагает наличие у машины таких процессов, как преобразование знания в процессе обучения на опыте и адаптацию к различным обстоятельствам, что и подразумевается под понятием «интеллект».

И когда будет создана действительно разумная машина перед человечеством встанут новые вопросы в области этики.

Если машины будут осознавать себя, смогут рассуждать и иметь чувства, то в чем же будет разница между человеком и машиной? То, из какого материала он сделан? Из органического или неорганического? Достаточно ответить на вопрос, что делает человека человеком? Однозначный ответ на этот вопрос найти сложно. Потому что человека можно рассматривать как существо биологическое и социальное. Эти два начала тесно переплелись. Но какое из них все-таки сильнее? Биологическое или социальное?

Биологические потребности свойственны всем организмам на Земле. Это потребность в дыхании, потреблении пищи, размножении и т.п. Таким образом, человек мало чем отличается от других живых существ.

Рассматривать человека как социальное существо можно, потому что он существует в социуме. В социуме царят свои законы, и, чтобы следовать этим законам, человеку зачастую приходится подавлять свои биологические инстинкты. Люди ограничивают свои поступки не инстинктами, а социальными нормами. Однако многие социальные нормы выросли из биологической целесообразности (например, запрет на инцест, так как кровосмешение повышает вероятность возникновения патологии у ребенка). Таким образом, можно сказать, что человек – существо биосоциальное, так как биологическое и социальное переплелись и невозможно понять, какое из двух начал преобладает. Но стать полноценной личностью человек может только в окружении себе подобных.

Что еще отличает человека от животных, помимо социальных качеств? Это его интеллект – то, что позволяет человеку мыслить абстрактно, заниматься творчеством, делать заключения, решать пробле-

мы, понимать сложные идеи, быстро обучаться и учиться на основании опыта. Благодаря интеллекту человек может познавать мир, постигать суть вещей, понимать, что от него требуется в той или иной ситуации. Но интеллект не может быть главным критерием отличия человека от машины.

Человек имеет также чувства. Он способен испытывать любовь, ненависть, верность, зависть.

И снова вернемся к нашему вопросу. Если машина научится мыслить и чувствовать, то сможет ли она считать себя человеком? Вероятно, сможет. Но человечество не сможет признать машину равной себе.

Однако машину должно что-то отличать от человека, ее создателя. Считается, что человек обладает душой. Согласно многим идеалистическим, дуалистическим философским направлениям и религиозным течениям, душа – бессмертная субстанция, нематериальная сущность, в которой выражена божественная природа его личности, дающая начало и обуславливающая жизнь, способности ощущения, мышления, сознания, чувств и воли, противопоставляемая телу. И не факт, что люди смогут наделить машину душой. Возможно, она будет обладать чувствами, если смоделировать действие гормонов. Можно наделить машину на основе законов логики. Но будет ли машина обладать душой, которой, согласно Библии, человека наделяет Бог?

Если машины смогут осознавать себя и иметь чувства, то возможно ли будет их просто эксплуатировать или же придется ставить их в один ряд с человеком? А зависеть это будет от степени того, насколько искусственный интеллект осознает себя и испытывает ли он какие-либо эмоции. Например, давать им права. Но человек может контролировать уровень развития искусственного интеллекта, чтобы роботы не стали осознавать себя, не могли обладать индивидуальностью. Подобное было описано в романе У. Гибсона «Нейромант». Существует так называемый Регистр Тьюринга, который осуществляет подобную функцию.

А будет ли считаться человеком человек, у которого более 90 % тела заменено на искусственные имплантаты?

Этот вопрос затрагивается в художественном фильме «Двухсотлетний человек», снятом в 1999 году режиссёром Крисом Коламбусом.

Фильм, как и литературные произведения, поднимает проблемы человечности и искусственного интеллекта, рабства и свободы, конформизма и борьбы за свои права, любви, жизни и смерти.

В сюжете фильма созданный робот, которому дали имя Эндрю, выступает с речью в суде, чтобы его признали человеком. Но судья во время заседания указывает на фактическое бессмертие Эндрю, что в

существенной степени препятствует Эндрю быть названым человеком, поскольку все люди смертны и это вызовет негодование в обществе.

Таким образом, следует вывод, что общество не может принять бессмертного человека, а человека делает человеком необратимое разрушение его тела через неизвестный промежуток времени, то есть вызовет обычную, с точки зрения человека, смерть.

И самый волнующий людей вопрос заключается в том, как сложатся отношения людей и машин? Все будет зависеть от того, как люди поведут себя на начальных этапах данных отношений.

Возможно несколько вариантов развития событий.

1. *Машины являются единственными обитателями Земли*. Причин для этого может быть несколько. Либо война между людьми и машинами, как в фильмах «Терминатор» режиссёра Джеймса Кэмерона, «Матрица» снятом братьями Вачовски, «Бегущий по лезвию» режиссёра Ридли Скотта, где машины представлены как сила, пытающаяся свергнуть власть человека. Либо человечество было уничтожено по собственной глупости. Это могут быть эпидемии, войны или техногенная катастрофа. Третий вариант – это какая-то глобальная катастрофа, в результате которой человечество исчезнет. Однако при любом рассматриваемом развитии событий машины останутся и продолжат свое существование и развитие в силу своих сильных преимуществ.

2. *Машины и люди – партнеры*. Сильные стороны есть и у человека, (это его опыт и цели, которые он хочет достигнуть), и у машин (преимущества над физическими способностями человека и возможность достигнуть поставленные цели). И машины могут получить доступ ко всем знаниям и опыту человечества. И, кроме того, получить шанс стать подобными людям. Например, получить эмоции.

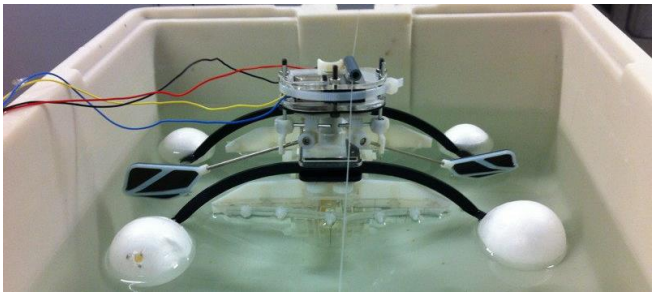
3. *Человек будет создателем и творцом для машин*. Интеллектуальный уровень человечества будет выше, чем у машин. И это будет достигнуто за счет контроля машин, например на основе, трех законов робототехники. Подобное общество описывал в своих рассказах Айзек Азимов в сборнике рассказов «Я, робот», где роботы выступают как помощники людей, нередко являясь более разумными, чем сами люди. Именно в этом сборнике рассказов и были впервые сформулированы известные *три закона робототехники*. Законы гласят:

1) робот не может причинить вред человеку или своим бездействием допустить, чтобы человеку был причинён вред;

2) робот должен повиноваться всем приказам, которые даёт человек, кроме тех случаев, когда эти приказы противоречат первому закону;

3) робот должен заботиться о своей безопасности в той мере, в которой это не противоречит первому и второму законам.

Науку запретить нельзя, поэтому появление машин, превосходящих нас по интеллекту, будет закономерным.



Робот, поглощающий живые организмы

Так, совсем недавно, а точнее 27 октября 2016 года, издание NewScientist ознакомило нас с результатами работ ученых, представляющих Бристольский университет и Роботехническую лабораторию Бристоля. Материал посвящен весьма необычному роботу, который внешне напоминает насекомых, передвигающихся по поверхности воды (см. рисунок) [5]. Но главная особенность изделия кроется не в его внешнем виде, а в возможностях. Дело в том, что робот может получать энергию, поглощая живые организмы. Поглощенный биологический материал может дать ему часть энергии для дальнейшего функционирования.

Хоть размер пищи и ограничен размером «насекомого», снабженного микробным топливным элементом, выступающим в роли его «желудка», но долго ли человечество после усовершенствований данных технологий сможет оставаться на вершине пищевой цепочки?

В заключение хотелось бы сказать, что с созданием полноценного искусственного интеллекта перед человечеством встанет множество проблем. И то, как будут развиваться отношения человека и машины, зависит лишь от того, насколько человек будет разумен и состоятелен в своих решениях.

Список литературы

1. Аверкин А. Н., Гаазе-Рапопорт М. Г., Поспелов Д. А. Толковый словарь по искусственному интеллекту. – М.: Радио и связь, 1992.

2. Большой латинско-русский словарь. Vocabvlarivm latinorvssicvm magnvm [Электронный ресурс]. – URL: http://linguaeterna.com/vocabula/index.php (дата обращения 02.11.2016 г.).

3. Turing A. Computing machinery and intelligence (англ.) // Mind. – Oxford: Oxford University Press, 1950. – № 59. – P. 433-460.

4. Блай Уитби. Искусственный интеллект: реальна ли Матрица. – М.: ФАИР-ПРЕСС, 2004.
5. New Scientist [Электронный ресурс]. – URL: https://www.newscientist.com/article/2110645-soft-robot-with-a-mouth-and-gut-can-forage-for-its-own-food/ (дата обращения 02.11.2016 г.).

УДК 551.524.1:517.518.3

Хохолков Павел Сергеевич
направление Программная инженерия (магистратура), гр. ПСм-12

Научный руководитель
Бородин Андрей Викторович, канд. экон. наук, профессор,
кафедра информатики и системного программирования
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

АДАПТИВНАЯ ВЕЙВЛЕТ-ФИЛЬТРАЦИЯ В ЗАДАЧАХ ОБРАБОТКИ МЕТЕОНАБЛЮДЕНИЙ

Метод измерения температуры воздуха на открытом пространстве основан на использовании термометров, которые постоянно установлены в психометрической будке на высоте 2 м, чем обеспечивается равенство температур воздуха и термометра. Влияние радиации на температурный режим датчиков исключается радиационной защитой (будкой). Температура термометра определяется по изменению одного из термометрических свойств чувствительного элемента [10].

Для минимизации влияния радиации психометрическая будка имеет специальную конструкцию и относительно большие габаритные размеры. Однако иногда место расположения измерительного оборудования накладывает ограничения на исполнение и габариты конструкции для размещения датчиков. В таких случаях часто не удается полностью избежать влияния солнечной радиации на показания датчиков температуры и влажности, что вносит определенные погрешности в измерения. Данное исследование посвящено разработке методов корректировки температурных наблюдений с целью повышения адекватности измерений.

В качестве модельного примера рассмотрим датчик влажности и температуры DHT22, расположенный на стене дома с координатами 56.6481N, 47.9106E в вентилируемой цилиндрической пластиковой конструкции небольшого диаметра. Стена расположена таким образом, что

нормаль к ней ориентирована на северо-восток, а сама поверхность почти всегда закрыта от прямой солнечной радиации расположенными рядом постройками и деревьями. Тем не менее, в летний период в утренние часы возможно попадание прямых солнечных лучей на поверхность защитной конструкции датчика. Это приводит порой к значительным искажениям показаний (см. выделенные фрагменты графика с метками 1, 2, 3, 4). Приведенные на рисунке данные собраны с использованием геоинформационного сервиса «Народный мониторинг» [7].

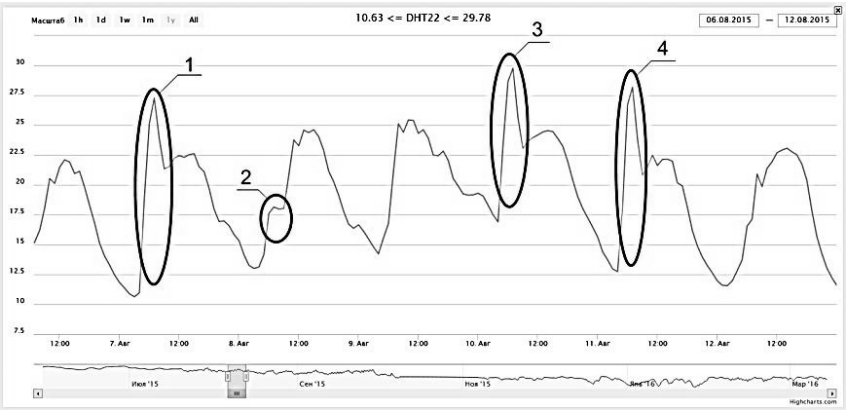


График изменения температуры воздуха с 6 по 12 августа 2015 г.
с выделенными искажениями, связанными с засветкой защитной конструкции датчиков прямыми солнечными лучами в утренние часы

Идея предлагаемого метода компенсации искажений в показаниях датчиков взята из совершенно иной предметной области, а именно из области прогнозирования денежных потоков. В работе [3] впервые, по крайней мере, в Российской Федерации, была продемонстрирована перспективность использования инструментария вейвлет-преобразований в прогнозировании денежных потоков. В течение пяти лет после публикации названной работы это направление получило развитие в методике адаптивной вейвлет-фильтрации (АВФ) временных рядов, связанных с депозитными портфелями российских банков [8]. В частности, в диссертационном исследовании Т. А. Уразаевой [9] АВФ была использована для элиминации процессов, связанных с массовым зачислением заработной платы во вклады и достаточно быстрым изъятием этих средств со счетов «до востребования». Интересно, что ежедневный прилив средств, связанный с зачислением заработной платы, и ежедневный от-

лив, связанный со снятием денежных средств после зачисления заработной платы, были, по крайней мере, в конце 90-х годов прошлого столетия, в среднем пропорциональны объемам соответственно недозачисленных и недоснятых средств заработной платы. Совершенно аналогичной является ситуация накопления тепловой энергии вследствие облучения прямыми солнечными лучами, и ее потери, после устранения доступа прямых солнечных лучей, в пределах объема для размещения датчиков внутри защитной конструкции. Другими словами, дифференциальные уравнения, описывающие и тот и другой процессы, типологически оказываются идентичными. Соответственно идентичные методы могут использоваться и для элиминации идентичных процессов.

В ходе проведения ряда численных экспериментов установлено, что в случае, когда не требуется высокая точность измерений, для снижения вычислительной сложности фильтра вместо АВФ можно использовать фильтрацию на основе фиксированной базисной функции – вейвлета Добеши второго порядка [6]. Именно этот вейвлет из множества стандартных продемонстрировал наилучший результат, который, однако, несколько уступал результатам, полученным на основе АВФ.

В настоящее время система автоматического мониторинга температуры с АВФ соответствующих временных рядов функционирует в составе учебно-испытательного полигона отработки технологий дистрибуции точного времени [1, 2, 4] на одной из площадок размещения оборудования. Алгоритмы АВФ включены в состав программного обеспечения мониторинга состояния стендового оборудования [5].

Список литературы

1. Инновационные подходы к развитию техники и технологий. Кн. 1 / В. М. Антонов, А. В. Бородин, Ю. А. Ипатов и др. – Одесса: Куприенко С.В., 2015. – 172 с.

2. Белоусов С. А., Александров Н. И., Бородин А. В. Единая технологическая платформа разработки подсистем дистрибуции точного времени в сетях передачи данных, построенных на базе оборудования Cisco // Информационные технологии в экономике, образовании и бизнесе: материалы V международной научно-практической конференции (23 декабря 2013 г.). – Саратов: Изд-во ЦПМ «Академия Бизнеса», 2013. – С. 15-18.

3. Бородин А. В., Уразаева Т. А. Вейвлет-преобразования в задачах прогнозирования денежных потоков // Диалог наук на рубеже XX-XXI веков и проблемы общественного развития. Вторые Вавиловские чтения: материалы постоянно действующей всероссийской междисциплинарной научной конференции. Ч. I. – Йошкар-Ола: Марийский государственный технический университет, 1997. – С. 84-85.

4. Бородин А. В., Варламов А. С., Кораблев Д. В. Учебно-испытательный полигон отработки технологий дистрибуции точного времени // Кибернетика и программирование. – 2015. – № 3. – С. 11-23. – DOI: 10.7256/2306-4196.2015.3.15438. – URL: http://e-notabene.ru/kp/article_15438.html

5. Глазырина Т. В., Лукиных Н. А., Бородин А. В. Программный комплекс расширенного мониторинга состояния NTP-серверов компании Symmetricom серий NTS-90 и NTS-100 // Человек, общество, природа в эпоху глобальных трансформаций: безопасность и развитие. Семнадцатые Вавиловские чтения: материалы постоянно действующей международной междисциплинарной конференции. Ч. 2. – Йошкар-Ола: Поволжский государственный технологический университет, 2014. – С. 246-248.

6. Добеши И. Десять лекций по вейвлетам. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. – 464 с.

7. Интернет-проект «Народный мониторинг». – URL: http://narodmon.ru/

8. Уразаева Т. А. Использование вейвлет-преобразований в задаче управления ликвидностью коммерческого банка // Планирование, учет и анализ в социально-экономических системах: межвузовский сборник статей. Юбилейный выпуск. – Йошкар-Ола, 2003. – С. 102-108.

9. Уразаева Т. А. Управление ценообразованием депозитов коммерческого банка: дисс. … канд. экон. наук: 08.00.13. – М.: Московский государственный университет экономики, статистики и информатики (МЭСИ), 2000. – 129 с.

10. Ходжаева Г. К. Метеорологические методы и приборы наблюдений. – Нижневартовск: Изд-во Нижневартовского государственного университета, 2013. – 189 с.

УДК 004.056

Чемоданова Илона Дмитриевна
направление Информационная безопасность
(специалитет), гр. БИс-31

Научный руководитель
Смирнов Владимир Иванович, старший преподаватель,
кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ПРОБЛЕМЫ ПРИМЕНЕНИЯ ПОДХОДА С ИСПОЛЬЗОВАНИЕМ ФИЗИЧЕСКИХ ЭФФЕКТОВ ПРИ ЗАЩИТЕ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

В данной статье обоснована необходимость использования подхода, опирающегося на физические эффекты, в дополнение к системному подходу при прогнозировании возможностей появления технических

каналов утечки информации (ТКУИ). Особое внимание уделено проблемам применения знаний о физических эффектах на практике.

Введение

Защита информации от утечки по техническим каналам (ТКУИ) является слабоформализуемой. Для решения такого рода задач традиционно используется системный подход. Подход, опирающийся на физические эффекты, дополняет системный подход. Это связано с тем, что физические эффекты (ФЭ) являются фундаментальными знаниями, которые можно использовать в различных областях науки и техники.

Системный подход и подход с использованием ФЭ

Системный подход представляет собой «методологическое направление исследования объекта как системы с разных сторон, комплексно, в совокупности отношений и связей между его элементами» [1]. Данный подход является междисциплинарным.

Г. А. Бузов отмечает, что «решение проблемы защиты информации с точки зрения системного подхода можно сформулировать как трансформацию существующей системы в требуемую» [2]. При этом могут быть предложены несколько вариантов такой трансформации. Для качественной оценки существующих вариантов приходится использовать определённые критерии. При выборе рационального варианта в качестве критерия уместно использовать соотношение между ценой защищаемой информации и затратами на её защиту. Желательно получить такой вариант, при котором «обеспечивается требуемая степень безопасности информации и минимизируются расходы на её защиту» [3].

А. Н. Соболев [4] выделил основные составляющие системного подхода при разработке систем информационной безопасности:

1) стадии жизненного цикла источника информации;

2) связь источника информации с компонентами окружающей среды;

3) анализ физических основ технических средств создания, передачи, приема и использования информации;

4) учет направлений развития технических средств;

5) взаимосвязь и взаимозависимость технических средств перехвата информации, противодействия перехвату и контроля состояния системы информационной безопасности;

6) комплексный подход к созданию системы информационной безопасности.

При применении подхода к выявлению ТКУИ, опирающегося на ФЭ, совместно с системным подходом составляющие 3 и 5 могут быть раскрыты полнее, чем при применении только системного подхода.

В основе подхода к выявлению ТКУИ, опирающегося на ФЭ, – взгляд на физический путь переноса информации от её источника к несанкционированному получателю в ТКУИ как на совокупность взаимосвязанных совместимых физических эффектов (см. рисунок) [5].

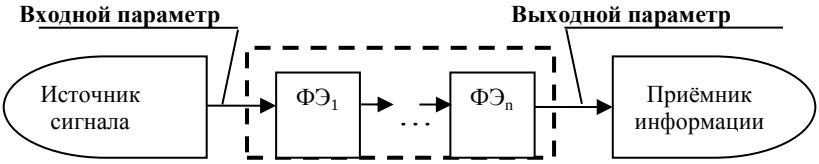


Схема ТКУИ (подход с использованием ФЭ)

Подход с использованием ФЭ применим не только для выявления ТКУИ.

Проблемы применения знаний о ФЭ

Знания о ФЭ могут использоваться в различных областях: в нанотехнологиях [6, 7], в микротеплотронике [8], в микроэлементной базе [9], в области энергоинформационных взаимодействий [10] и др.

А. Ф. Алейников выделяет из последних разработок российских ученых, зарегистрированных в официальном бюллетене российского агентства по патентам и товарным знакам «Программы для ЭВМ. Базы данных. Топологии интегральных микросхем» …» [8] программный комплекс и базы данных, представленные в таблице.

Разработки российских ученых

Разработка	Авторы	Описание
БД ФЭ	Аврамчик Г.Н., Галочкин В.И., Смиренский Е.А., Соболев А.Н.	Позволяет осуществлять синтез принципов действия технических систем различного назначения, на которых проявляются требуемые физические эффекты, прогнозирование направлений развития технических систем.
система Принц	Галочкин В.И., Соболев А.Н.	Позволяет решать задачи на стадии разработки технических приложений по прогнозированию развития технических систем.
БД ФЭ НАНО	Соболев А.Н., Аврамчик Г.Н., Бурмистрова Н.П., Галочкин В.И.	Позволяет осуществлять синтез принципов действия технических систем, оказывает информационную поддержку в научно-техническом прогнозировании и изобретательстве.

А. Н. Соболев выделяет ряд проблем, затрудняющих широкое практическое применение ФЭ [11]:

- отсутствие информации о тех или иных ФЭ у специалистов;
- отсутствие у нас в стране и за рубежом официальной регистрации открытых физических эффектов, что приводит к невозможности оценки общего количества известных человечеству ФЭ;
- незнание специалистом закономерностей технической реализации физических эффектов;
- отсутствие эффективной методологии решения задач, связанных с использованием физических эффектов;
- устаревшая методика преподавания курса физики в системе среднего общего и высшего профессионального образования.

Для устранения данных проблем предлагается создать экспертную систему для внедрения в учебный процесс, что позволит собрать необходимую информацию о ФЭ и получить необходимые навыки будущим специалистам по защите информации.

Заключение

Проблемы применения подхода с использованием физических эффектов при защите информации от утечки по техническим каналам тесно связаны с рядом проблем, затрудняющим широкое практическое применение ФЭ. Предлагается создать экспертную систему, которая позволит собирать информацию о новых физических эффектах станет учитывать опыт российских ученых (различные БД по ФЭ) и будет использоваться в системе высшего профессионального образования.

Список литературы

1. Основы управления информационной безопасностью: учебное пособие для вузов / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – 2-е изд., испр. – М.: Горячая линия-Телеком, 2014. – 244 с. – Серия «Вопросы управления информационной безопасностью». Выпуск 1.

2. Бузов Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации: учебно-методическое пособие. – М.: Горячая линия-Телеком, 2010. – 240 с.

3. Бузов Г. А., Калинин С. В., Кондратьев А. В. Защита от утечки информации по техническим каналам: учебное пособие. – М.: Горячая линия-Телеком, 2005. – 416 с.

4. Соболев А. Н., Кириллов В. М. Физические основы технических средств обеспечения информационной безопасности: учебное пособие. – Йошкар-Ола: МарГТУ, 2004. – 232 с.

5. Смирнов В. И., Пекунов А. А. Защита информации от утечки по техническим каналам: системный подход и подход с использованием физических эффектов // Инженерные кадры – будущее инновационной экономики России:

материалы Всероссийской студенческой конференции (Йошкар-Ола, 23-28 ноября 2015 г.): в 8 ч. – Йошкар-Ола: ПГТУ, 2015. – Ч. 4. Информационные технологии – основа стратегического прорыва в современной промышленности. – С. 95-99.

6. Соболев А. Н., Кириллов В. М., Киселев А. В. Физические основы перспективной вычислительной техники и обеспечение информационной безопасности: учебное пособие. – М.: Гелиос АРВ, 2012. – 256 с.

7. Физические эффекты в нанотехнологиях: учебное пособие / А. Н. Соболев, В. И. Галочкин, Г. Н. Аврамчик, Н. П. Бурмистрова. – Йошкар-Ола: МарГТУ, 2000. – 184 с.

8. Алейников А. Ф., Матасова Ю. А., Морозов Ю. В. Преобразователь тепловых сигналов: монография / РАСХН. Сибирское отделение. – Новосибирск, 2006. – 68 с.

9. Денисенко В. В. Новые физические эффекты в нанометровых МОП-транзисторах // Компоненты и Технологии. – 2009. – № 12 (101). – С. 157-162.

10. Соболев А. Н. Энергоинформационные взаимодействия и информационная безопасность: учебное пособие. – Йошкар-Ола: Марийский государственный технический университет, 2010. – 408 с.

11. Соболев А. Н. Физические эффекты: научное издание. – Йошкар-Ола: МарГТУ, 2001. – 168 с.

УДК 621.396.94

Шелеметьева Яна Владимировна
направление Системы автоматизации проектирования (аспирантура)
Шелеметьев Андрей Михайлович
направление Вычислительные машины, комплексы и компьютерные сети (аспирантура)

Научный руководитель
Смирнов Алексей Владимирович, канд. техн. наук, доцент
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ УДАЛЕННОГО ПРЯМОГО ДОСТУПА К ПАМЯТИ В ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

В настоящее время одной из актуальных задач в исследованиях организации высокопроизводительных вычислительных систем является обеспечение указанных систем высокой пропускной способностью и низкими задержками передачи данных. Низкая скорость ответа на за-

просы в таких системах ведет к критическим и необратимым последствиям, поэтому развитие технологий высокоскоростной и надежной передачи данных является одним из приоритетных направлений в вычислительной технике. Одним из вариантов повышения производительности сетевой вычислительной системы является разгрузка процессоров вычистительных узлов системы от части сетевых вычислений с помощью технологии удаленного прямого доступа к памяти (Remote Direct Memory Access – далее RDMA).

RDMA – это технология, которая позволяет передавать сетевые данные без участия центрального процессора, напрямую из буферов сетевого адаптера в буферы приложения, таким образом, разгружая процессор от обработки данных сети [2].

Высокопроизводительные вычислительные системы, реализующие технологию удаленного доступа к памяти

В настоящее время наиболее известными архитектурными решениями, в которых реализована технология удаленного прямого доступа к памяти, являются высокопроизводительные системы InfiniBand и 10/40 Gigabit Ethernet. В этих системах с помощью протокола RDMA передача сетевых данных из памяти одного компьютера в память другого осуществляется без участия операционной системы. При этом исключается участие центрального процессора в обработке команд и необходимость пересылки данных из памяти приложения в буферную область ОС. То есть данные пересылаются напрямую на соответствующий сетевой контроллер.

Каждая из указанных архитектур имеет особенности реализации. В архитектуре 10/40 Gigabit Ethernet используются стандартные решения Ethernet, которые позволяют без больших программных и аппаратных изменений сопрягать архитектуру 10/40 Gigabit Ethernet с другими вычислительными системами (например, с глобальной вычислительной сетью Internet). Архитектура InfiniBand – более специализированная архитектура, направленная на решение определенного класса задач.

Вычислительные архитектуры Ethernet

В Ethernet сетях используется стек протоколов TCP/IP. Для реализации удаленного прямого доступа к памяти к стандартной архитектуре стека протоколов была добавлена технология IWARP – набор стандартов для обеспечения работы RDMA по IP-сетям. Технология IWARP представляет собой совокупность трех протоколов (MPA, DDP и непосредственно RDMA), лежащих поверх протоколов транспортного уровня и отвечающих за доставку сообщений в память буферов приложений, минуя многократное копирование данных между различными буфера-

ми, например между буфером сетевого адаптера и буфером сетевого стека. Область памяти буферов регистрируется приложениями до начала передачи и передается по сети в специальных сообщениях. Далее, в процессе взаимодействия, узлы сети постоянно обмениваются указанными сообщениями для того, чтобы иметь реальную картину о свободных и занятых областях памяти удаленных узлов. На рисунке 1 представлено положение протоколов IWARP относительно стандартных протоколов сети TCP/IP.

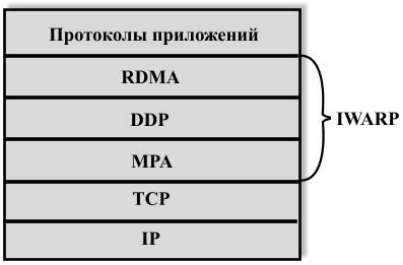


Рис. 1. Стек протоколов сети 10 Gigabit Ethernet

Протокол MPA (Marker PDU Aligned) – промежуточный протокол между TCP и DDP протоколами. Отвечает за фиксирование границ сообщения; сообщение будет той длины, которую требует протокол DDP.

Протокол DDP (Direct Data Placement) отвечает за результативную запись данных, инициализированную протоколами вышестоящего уровня.

С помощью специальных наборов команд, протоколы MPA, DDP, RDMA обеспечивают прямой удаленный доступ к памяти между удаленными узлами в соответствии с требованиями приложений.

Вычислительные архитектуры InfiniBand

Для вычислительной архитектуры InfiniBand определено несколько уровней сетевых протоколов: физический, канальный, сетевой, транспортный и протоколы высшего уровня – приложения [1]. В системах InfiniBand поддерживаются две технологии передачи сетевых данных: стандартная технология приема-передачи данных, в которой сетевой адаптер не интерпретирует виртуальные адреса в физические, определяя тем самым буфер в области памяти, куда необходимо поместить входящие данные; и технология передачи данных с использованием удаленного прямого доступа к памяти. Для передачи данных с использованием стандартных операций приема-передачи в системах InfiniBand определен формат пакета, в состав которого входят заголовки всех сетевых

уровней архитектуры InfiniBand и данные от приложения. Общая структура формата пакета InfiniBand представлена на рисунке 2.

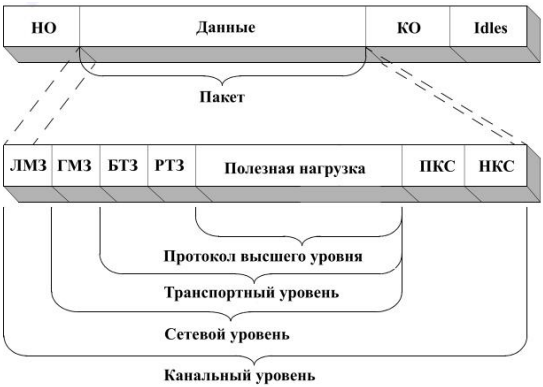


Рис. 2. Общая структура формата пакета InfiniBand: ЛМЗ – локальный маршрутный заголовок, ГМЗ – глобальный маршрутный заголовок, БТЗ – базовый транспортный заголовок, РТЗ – расширенный транспортный заголовок, ПКС – постоянная контрольная сумма, НКС – непостоянная контрольная сумма, НО – начальный ограничитель, КО – конечный ограничитель

За реализацию удаленного прямого доступа к памяти в вычислительных системах InfiniBand отвечает транспортный уровень, который добавляет в формат передаваемого сетевого пакета расширенный транспортный заголовок. Если базовый транспортный заголовок присутствует во всех сетевых сообщениях, то расширенный – только в сообщениях, передаваемых с помощью технологии RDMA. Таким образом, информация о том, что данный пакет следует обрабатывать как команду записи/чтения RDMA, содержится в дополнительном транспортном заголовке RDMA.

Заключение

Для обеспечения высокоскоростной, высокоэффективной, надежной передачи данных с низкими задержками и высокой скоростью ответа в различных вычислительных архитектурах реализована технология удаленного прямого доступа к памяти. Технология позволяет передавать данные без задействия процессоров вычислительных узлов, разгружает их от обработки сетевого трафика и направляет все вычислительные ресурсы процессоров на решение внутренних задач.

Двумя наиболее известными архитектурами, в которых реализована указанная технология, являются высокопроизводительные вычисли-

тельные системы 10 Gigabit Ethernet и InfiniBand. Каждая из обозначенных вычислительных систем имеет свои особенности реализации, а также отвечает различным требованиям, предъявляемым к вычислительным архитектурам. Архитектура InfiniBand является специализированной архитектурой, в которой организована высоконадежная, высокоскоростная передача данных. Архитектура 10 Gigabit Ethernet – универсальная, сопрягаемая с другими вычислительными системами без использования дополнительных устройств, архитектура.

Список литературы

1. InfiniBandTM Architecture Specification Volume 1 Release 1.2.1 Final Release / InfiniBandSM Trade Association – CA.: California USA, 2007. – 1727 с.

2. Recio R. A., Metzler B., Culley P. Remote Direct Memory Access Protocol Specification. – Fremont, CA: RFC, 2007. – 66 с.

3. Understanding iWARP: Eliminating Overhead and Latency in multi-Gb Ethernet Networks: NETEFFECT, Summer 2002. – 5 p.

УДК 658.562

Шишлакова Елена Михайловна
Национальный исследовательский технологический университет «МИСиС»,
гр. САПР-13

Научный руководитель
Аристов Антон Олегович, канд. техн. наук, доцент,
кафедра автоматизированного проектирования и дизайна
ФГАОУ ВО «Национальный исследовательский технологический университет «МИСиС»», г. Москва

ВОПРОСЫ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ МЕТРОЛОГИЧЕСКИМ ОБСЛУЖИВАНИЕМ СРЕДСТВ ИЗМЕРЕНИЙ

В условиях развития техники и технологий, появления новых производств и сфер деятельности, повышения требований к точности измерений при изготовлении продукции расширяется использование различных средств измерительной техники и возрастает роль процедур, обеспечивающих соответствие метрологических характеристик средств измерений (СИ) установленным требованиям. Следовательно, предъявляются повышенные требования к метрологической инфраструктуре и к деятельности центров стандартизации и метрологии, являющихся основой этой инфраструктуры [4].

Требования законодательства, регулирующего данный вид деятельности, предполагают, с одной стороны, значительное количество идентификационных признаков для каждого типа средств измерений и метрологической операции, а с другой – взаимодействие центра стандартизации и метрологии с федеральными информационными базами при осуществлении операций метрологического обслуживания [1-3]. Это приводит к обработке больших объемов информации. Все это обуславливает актуальность внедрения в бизнес-процессы работы центров стандартизации и метрологии современных информационных технологий [5].

В данной работе рассмотрены вопросы автоматизации управления метрологическим обслуживанием средств измерений центра стандартизации и метрологии. Была проанализирована деятельность центра:

1) изучены нормативные правовые акты и внутренние инструкции, регламентирующие деятельность центра;

2) определены факторы, влияющие на внутреннюю логистику при осуществлении метрологических операций;

3) оценена необходимость и полнота ведения баз данных и выходной документации.

Определены следующие цели внедрения автоматизированной системы:

– повышение эффективности и сокращение времени метрологического обслуживания СИ;

– обеспечение беспристрастности (объективных данных) при поверке и калибровке;

– повышение эффективности принятия управленческих решений.

Сформулированы задачи автоматизации:

– автоматическая идентификация СИ и проверка на наличие типа средства измерения в государственном реестре средств измерений, определение типа, модели СИ, импорт данных;

– идентификация процедур обслуживания СИ;

– ведение базы данных СИ, БД результатов поверки, калибровки;

– обеспечение эффективной внутренней логистики;

– формирование отчетных форм.

Для выполнения поставленных задач, используется автоматизированная система, структура которой приведена на рисунке 1.

Установлено назначение каждой из подсистем:

– подсистема идентификации СИ предназначена для идентификации СИ по виду, типу, производителю, срокам метрологического обслуживания;

– подсистема идентификации процедур обслуживания СИ служит для определения процедуры и методики обслуживания. Подсистема должна иметь процедуру импорта методики поверки идентифицированного типа СИ из Федерального реестра;

– подсистема автоматической проверки на наличие оборудования в государственном реестре средств измерений предназначена для поиска СИ в государственном реестре и определения необходимых данных;

– подсистема обеспечения внутренней логистики используется для определения процесса метрологического обслуживания, задействованного персонала;

– подсистема формирования отчетных форм служит для формирования документов о проведенном метрологическом обслуживании и статистических отчетов и форм.

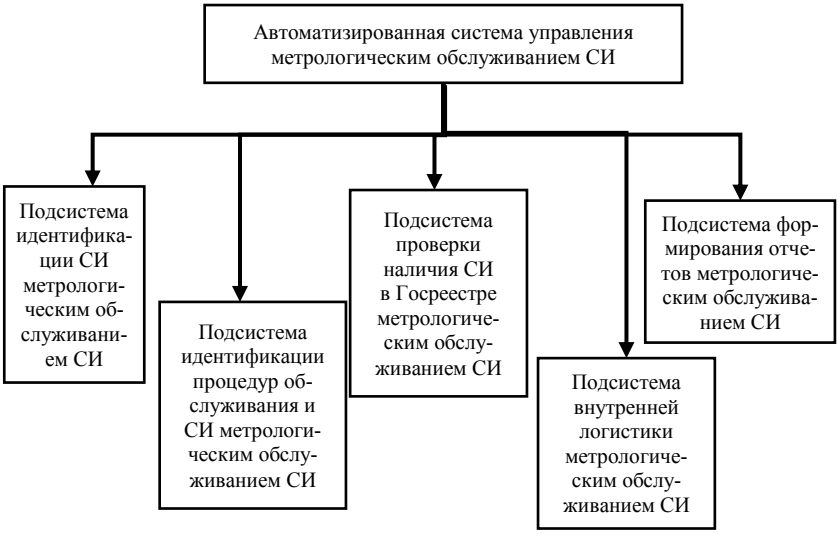


Рис. 1. Структура автоматизированной системы управления метрологическим обслуживанием СИ

На основе проведенного анализа в соответствии со стандартом IDEF0 разработана модель бизнес-процесса AS-IS – «как есть» (рис. 2) и выделены подлежащие автоматизации процессы.

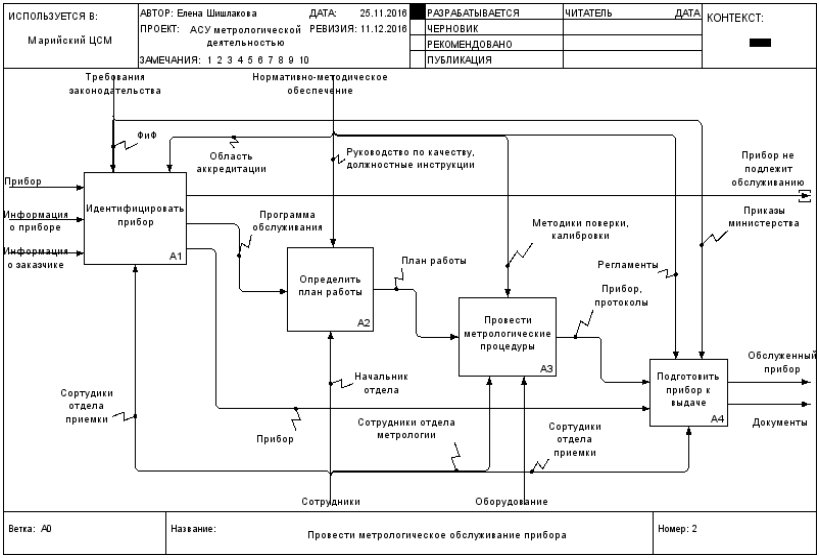


Рис. 2. Бизнес-процесс AS-IS

Таким образом, для достижения поставленных целей в первую очередь автоматизации подлежат процессы А1 «Идентифицировать прибор» и А2 «Определить план работы». Автоматизация этих процессов приведет к сокращению времени работы, количества персонала, исключению ошибок в работе и передаче информации, накоплению данных об использовании СИ. Проект не имеет привязки к конкретной организации, может быть масштабирован и внедрен в центрах стандартизации и метрологии, что полностью соответствует стандарту ГОСТ Р 50.1.028-2001 Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования.

Список литературы

1. РОССТАНДАРТ. Федеральный информационный фонд по обеспечению единства измерений [Электронный ресурс]. – Режим доступа: http://www.fundmetrology.ru/

2. Об обеспечении единства измерений: федеральный закон от 26.06.2008 № 102-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/ document/cons_doc_ LAW_77904/

3. Об утверждении Порядка проведения поверки средств измерений, требования к знаку поверки и содержанию свидетельства о поверке [Электронный ресурс]: приказ Министерства промышленности и торговли РФ № 1815 от 2.07.2015. – Режим доступа: http://www.consultant.ru/law/hotdocs/44100.html.

4. Об утверждении Критериев аккредитации, перечня документов, подтверждающих соответствие заявителя, аккредитованного лица критериям аккредитации, и перечня документов в области стандартизации, соблюдение требований которых заявителями, аккредитованными лицами обеспечивает их соответствие критериям аккредитации: приказ Минэкономразвития № 326 от 30.05.2014 [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/420203443.

5. Баландин А. А., Пахомова М. Н. Автоматизация рабочего места метролога – существенный шаг на пути к повышению качества продукции // Экономическая наука и практика: материалы междунар. науч. конф. (г. Чита, февраль 2012 г.). – Чита: Изд-во «Молодой ученый», 2012. – С. 130-132.

УДК 004.93

Яндыганов Иван Анатольевич
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-11

Научные руководители:
Тюкаев Андрей Юрьевич, канд. техн. наук, доцент,
кафедра информационной безопасности
Ипатов Юрий Аркадьевич, канд. техн. наук, доцент,
кафедра информатики
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА ПРОГРАММНЫХ МЕТОДОВ ДЛЯ ДЕТЕКТИРОВАНИЯ СОБЫТИЙ НА ОСНОВЕ АНАЛИЗА ДИНАМИЧЕСКИХ СЦЕН

На сегодняшний день видеоаналитика – это синтез технологий, который используется для получения различных данных на основе анализа видеоряда в режиме реального времени или из уже сохраненных записей с применением метода компьютерного зрения. Видеоаналитика является программным обеспечением, включающим в себя методы и алгоритмы машинного зрения, которые обеспечивают сбор и последующий анализ данных, полученных из видеоизображений, без участия человеческого фактора [1].

Целью проекта является создание программного средства, которое реализует детектирование статичных объектов в заданной области на основе анализа динамически изменяющихся сцен.

Для разработки на языке C++ была выбрана интегрированная среда разработки Microsoft Visual Studio 2013. Данное средство разработки

обладает большой справочной системой, широкими возможностями по отладке кода и позволяет автоматизировать некоторые рутинные процессы. В разработке программного средства использовались алгоритмы и методы [2-4], а также библиотека OpenCV. Данная библиотека включает в себя множество алгоритмов компьютерного зрения, обработки изображений и численных алгоритмов общего назначения. Плюсом данного выбора является то, что библиотека является кроссплатформенной и распространяется с открытым исходным кодом. Модули, которые использовались при разработке программного средства:

- open_core – предоставляет основной функционал (базовые структуры, вычисления, линейная алгебра);
- open_imgproc – обработка изображений (геометрические преобразования, фильтрация);
- open_highgui – ввод/вывод изображений и видео;
- open_objdetect – детектирование объектов на изображении;
- open_video – анализ движения и трекинг объектов.

Использовалась версия библиотеки OpenCV 2.4.8.

В общем случае алгоритмическая схема программного средства выглядит следующим образом. При запуске программы пользователь вводит путь к видеофайлу и, если файл существует, создается одно основное окно для вывода видеоряда, с отрисованными контурами и прямоугольниками вокруг статичных объектов, и три вспомогательных окна для вывода накопленного фона, маски движения и маски статичных объектов.

Далее производится покадровое считывание видеоряда. Каждый раз при считывании кадра производится проверка его существования и при отсутствии изображения, программа завершает свою работу. Из полученного кадра выделяется область интересов, с которой производятся все дальнейшие вычисления. Затем изображение передается в функцию накопления фона, где вычисляется разница между сохраненным фоном и текущим кадром в оттенках серого. Далее изображение разделяется на каналы RGB и также производится вычисление разницы между сохраненным фоном и текущим кадром в цветном изображении. Затем находится разница между кадром и фоном с помощью локальных бинарных шаблонов (Local Binary Patterns).

После осуществления всех предыдущих операций все полученные разницы складываются в одну итоговую общую разницу, которая переводится в бинарный формат. Данное бинарное изображение является маской движения.

Следующим шагом является обработка маски движения, из которой выделяются все статичные объекты, находящиеся в области интересов

в течение длительного времени. Полученные объекты заносятся в отдельное бинарное изображение, которое является маской статичных объектов. С помощью данной маски находится массив контуров данных объектов и создается массив прямоугольников, определяющих местоположение статичных предметов. Оба массива отображаются в главном окне. Блок-схема функционирования программного комплекса представлена на рисунке 1.

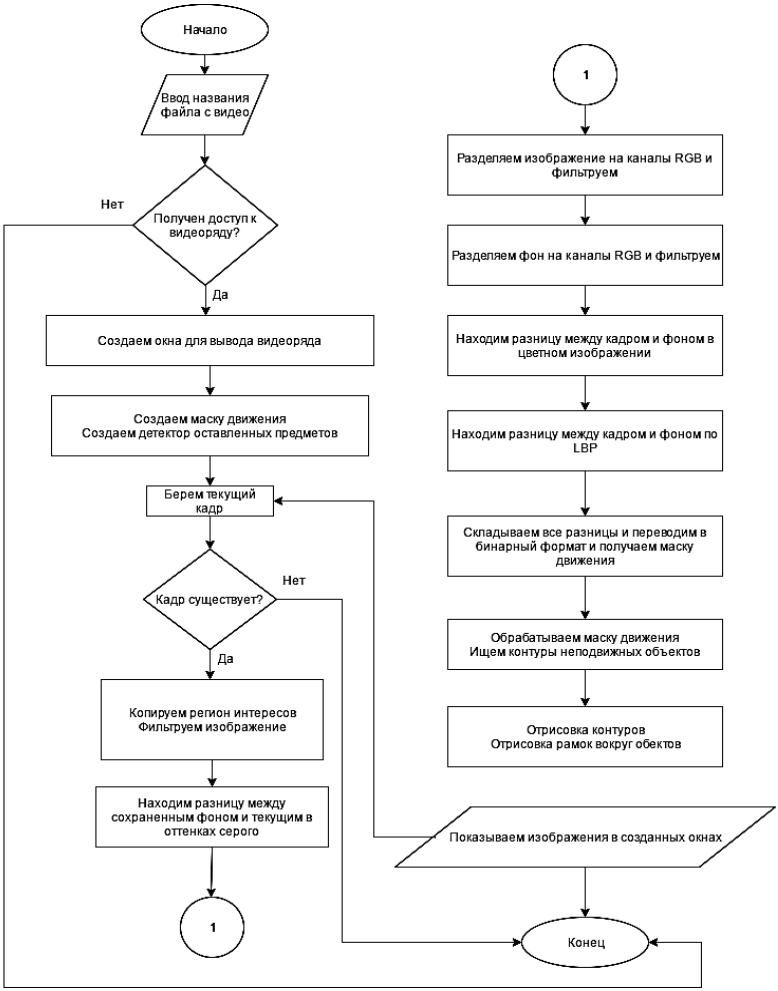


Рис. 1. Алгоритмическая схема программного продукта

Программа работает корректно, если она обнаружила все неподвижные объекты в заданной области. В тестовом видеофайле программа должна обнаружить два неподвижных объекта (рис. 2).

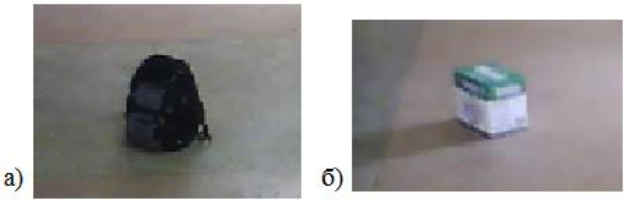


Рис. 2. Статичные объекты в заданной области интересов:
а) наплечный рюкзак; б) картонная коробка.

В процессе работы программа должна обнаружить эти объекты и выделить их прямоугольниками и контурами. В результате работы программное средство обнаружило все неподвижные предметы, которые оказались в заданной области интересов и находившиеся в течение определенного количества времени (рис. 3).

Рис. 3. Обнаруженные объекты

Данный проект может использоваться на практике для обнаружения оставленных предметов в заданной области с целью предупреждения. Этот проект может использоваться на практике для внедрения в более сложную систему видеонаблюдения в качестве отдельного модуля для обнаружения статичных объектов. Кроме того, проект может использоваться в качестве демонстрационного стенда для продолжения исследований в области компьютерного зрения, а также расширения функционала программного средства.

Список литературы

1. Haralick R., Shapiro L. Computer and Robot Vision // Addison-Wesley Publishing Company. – 1992. – Vol. 1. – P. 346-351.

2. Bouwmans T., Baf F. El, Vachon B. Background Modeling using Mixture of Gaussians for Foreground Detection – A Survey // Recent Patents on Computer Science 1. – 2008. – P. 219–237.

3. Piccardi M. Background subtraction techniques: a review // IEEE International Conference on Systems, Man and Cybernetics. – 2004. – P. 3099–3104.

4. Patel B., Patel N. Motion Detection based on multi-frame video under surveillance systems. – 2012. – Vol. 12.

УДК 621.3.977

Яранцев Алексей Михайлович
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Малашкевич Василий Борисович, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

МОБИЛЬНАЯ СИСТЕМА СФЕРИЧЕСКОГО ОБЗОРА С АВТОМАТИЧЕСКОЙ КОРРЕКЦИЕЙ ЛИНИИ ГОРИЗОНТА

В настоящее время цифровая фото- и видеосъемка применяется повсеместно: от исследования космических объектов до проведения семейных праздников. Развитие алгоритмов обработки изображений и повышение производительности вычислительных устройств привели к появлению новых качеств – съемка панорамных и 3D-изображений. В статьях [1-2] описаны системы для создания панорамных статических изображений компаний Apple и Google. Для круговых панорам в них требуется сделать серию последовательных частично перекрывающихся снимков. В статье [3] представлено описание 3D-камеры Ozo фирмы Nokia, которая способна записывать звук и видео с обзором в 360 градусов, а также снимает то, что происходит снизу и сверху благодаря использованию массива из восьми отдельных камер и микрофонов.

Недостатками подобных систем является требование четкой ориентации камеры относительно линии горизонта. Произвольные вращения и перемещения камеры при съемке обычно приводят к нарушению восприятия и деградации «склеек» отдельных кадров синтезированного изображения.

Целью данного исследования является разработка мобильной системы сферического обзора с автоматической коррекцией линии горизонта. Мобильность разрабатываемой системы позволяет отделить камеры от устройств обработки, демонстрации и фиксации изображения, а автоматическая коррекция линии горизонта – проводить съемку при любой ориентации камер.

Реализация системы может быть выполнена в виде сферы с диаметром 10-20 см, которую можно подбросить для съемки сверху, либо вкатить в слепую, опасную зону для визуального изучения ее состояния. Таким образом, рассматриваемая система окажется востребованной как в быту, так и в работе спецподразделений МЧС, МВД и МО.

Аппаратная часть системы состоит из двух блоков:

1. Мобильный блок камер включает 6 видеокамер для съемки по всем направлениям, датчика положения и микрокомпьютера с сетевым Wi-Fi модулем связи. Задачей блока является получение видеопотоков, их предобработка с целью сжатия и мультиплексирование для передачи по беспроводной линии связи. Датчик положения отслеживает сферические углы отклонения оси мобильного блока от вертикали, что позволяет определять камеры, в поле зрения которых находится линия горизонта.

2. Блок обработки и отображения может быть реализован на базе смартфона или в форме специализированного устройства. Назначение блока – отслеживание линии горизонта, отображение видео и управление мобильным блоком.

Программное обеспечение системы включает алгоритмы предобработки (сжатия) и мультиплексирования изображений, а также алгоритмы поворота и сшивки изображений. Для передачи видеопотоков по сети можно использовать реализации протоколов реального времени RTP/RTCP стека TCP/IP. Для реализации функций управления и передачи данных о положении мобильного блока потребуется разработать собственный протокол прикладного уровня.

Существенной проблемой при реализации алгоритмов сшивки, основанных на выделении особых точек изображений и их дескрипторов [4-7], является высокая вычислительная сложность. Создание панорамного видео в режиме реального времени оказывается тяжелой задачей даже для высокопроизводительных современных смартфонов. Для решения этой проблемы предлагается сократить площади перекрытия изображений соседних камер до 20-30% от общей площади кадра, а также применить методы алгоритма LOCOCO [8].

Таким образом, в настоящей работе предложена концепция построения аппаратно-программной системы сферического обзора с автоматической коррекцией линии горизонта. Определены основные блоки системы, принципы и алгоритмы их работы. Лабораторный макет системы может быть реализован на основе известных промышленно выпускаемых изделий. Значительных исследований потребует разработка алгоритмов обработки изображений и управления ими с целью отслеживания линии горизонта и корректировки синтезируемого панорамного видео. В работе определены основные направления таких исследований.

Разработка и реализация предложенной системы значительно расширит возможности бытовой фото- и видеосъемки, предоставляя пользователям новые, ранее недоступные ракурсы съемки. Применение системы в работе спецподразделений обеспечит более безопасные условия при решении задач, связанных с риском для жизни, в очагах природных и производственных катастроф, а также в боевых операциях. Эти обстоятельства определяют перспективы коммерциализации и практическую значимость работы.

Список литературы

1. Photo Sphere Camera: сообщество любителей круговых панорам [Электронный ресурс]. – 2015. – URL: http://www.iphone-gps.ru/2015/02/12/photo-sphere-camera-soobshhestvo-krugovyx-panoram-free/ (дата обращения 18.11.2016).

2. Photo Sphere «сферическая» камера в Android [Электронный ресурс]. – 2015. – URL: http://chezasite.com/android/photo-sphere-sfericheskaya-kame-53941.html (дата обращения 18.11.2016).

3. Nokia представила камеру для съёмки VR-фильмов [Электронный ресурс]. – 2015. – URL: http://hi-news.ru/entertainment/nokia-predstavila-kameru-dlya-syomki-vr-filmov.html (дата обращения 18.11.2016).

4. Бесшовные изображения [Электронный ресурс]. – 2012. – URL: http://wiki.gis-lab.info/w/Создание_бесшовного_изображения (дата обращения 18.11.2016).

5. Детекторы и дескрипторы точек [Электронный ресурс]. – 2010. – URL: http://www.intuit.ru/studies/courses/10621/1105/lecture (дата обращения 18.11.2016).

6. Scale Invariant Feature Transform [Электронный ресурс]. – 2009. – URL: http://www.scholarpedia.org/article/SIFT (дата обращения 18.11.2016).

7. Speeded-Up Robust Features [Электронный ресурс]. – 2008. – URL: http://www.vision.ee.ethz.ch/~surf/eccv06.pdf (дата обращения 18.11.2016).

8. LOCOCO corner detection method [Электронный ресурс]. – 2015. – URL: http://prog3.com/sbdm/blog/tostq/article/details/49247487 (дата обращения 18.11.2016).

УДК 004.7

Яранцев Алексей Михайлович
Федоров Ян Владимирович
направление Информатика и вычислительная техника
(бакалавриат), гр. ИВТ-41

Научный руководитель
Васяева Елена Семеновна, канд. техн. наук, доцент,
кафедра информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

АЛГОРИТМ ЕЗДЫ ПО ЛИНИИ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКОГО ЗРЕНИЯ

Работа современных автономных роботов часто совмещена с постоянным перемещением в динамически изменяющемся пространстве. В настоящее время в связи с интенсивной роботизацией стало необходимо создание таких роботов, которые могли бы не только передвигаться по заранее определенным маршрутам и обнаруживать препятствия, но и определять их, чтобы легко подстроиться под изменяющееся пространство. Эту проблему можно решить с помощью технического зрения. В данной работе рассматриваются алгоритмы определения маршрута движения автономного мобильного робота по траектории в виде линии.

Как правило, в процессе движения робота вокруг него присутствует множество перемещающихся объектов, поэтому он всегда должен не только получать информацию о своем маршруте и перемещающихся объектах, но также должен анализировать окружение, чтобы в случае необходимости иметь возможность грамотно отреагировать на возникшую ситуацию.

В качестве объекта управления алгоритма служит четырехколесная платформа, на которой расположены микрокомпьютер RaspberryPi, камера RaspberryPiCameraboard, а также ArduinoUno для управления движением платформы.

Для осуществления движения робота в изменяющейся среде рассматривается следующий пошаговый алгоритм:

1. Получаем кадр с камеры (рис. 1).

2. Сглаживаем изображение для устранения шумов (рис. 2).

3. Фильтруем изображение по цвету, получая черно-белое изображение (белый цвет – линия, черный цвет – фон) (рис. 3).

4. Подсчитываем количество белых пикселей на двух горизонтальных линиях.

5. По оси x – координатам белых пикселей находим средние точки линий (рис. 4, средние точки отмечены кругами).

6. Строим прямую по этим точкам и считаем угол между прямой и осью Y (рис. 5).

7. Объект, который едет по линии, поворачивает на этот угол (рис. 6, изображение с камеры после поворота).

8. Переход к шагу 1.

Для наглядности продемонстрируем алгоритм по шагам на примере:

Шаг 1

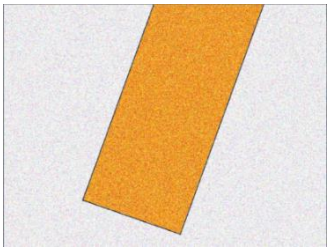


Рис. 1. Шаг 1

Шаг 2

Рис. 2. Шаг 2

Шаг 3

Рис. 3. Шаг 3

Шаг 4
Количество белых пикселей на первой линии: 272, на второй: 274.

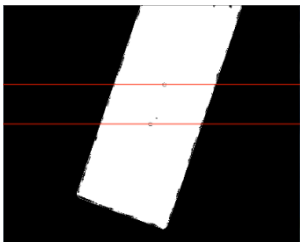


Рис. 4. Шаг 4

Шаг 5
Средние точки:396 и 434.

Шаг 6
Угол: 20.81

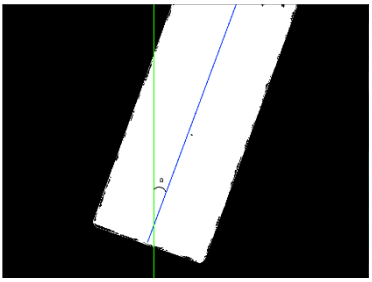


Рис. 5. Шаг 6

Шаг 7

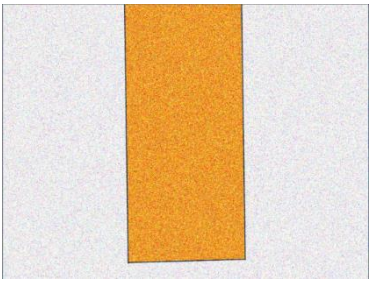


Рис. 6. Шаг 7

Реализация алгоритма

Алгоритм был реализован на языке программирования Python с использованием библиотек OpenCV 2 совместно с функциями библиотек:

- medianBlur – размытие изображения;
- cvtColor – преобразование цветового пространства изображения;
- inRange – проверка нахождения элементов массива в заданных границах.

Предложенный алгоритм распознавания линии справляется с возложенной на него задачей управления движением платформы в условиях изменяющейся среды с достаточной точностью и временем реакции.

В будущем планируется использование более высокопроизводительной системы обработки изображения для расширения возможностей данного алгоритма и увеличения скорости реакции на изменение окружающей среды.

Список литературы

1. Документация библиотеки Open CV [Электронный ресурс]. – URL: http://docs.opencv.org.

2. Документация языка Python [Электронный ресурс]. – URL: http://docs.python.org.

УДК 004.725:006.924.4

Яровиков Григорий Вячеславович
направление Программная инженерия (магистратура), гр. ПСм-11

Научный руководитель
Бородин Андрей Викторович, канд. экон. наук, профессор,
кафедра информатики и системного программирования
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

О ТЕХНОЛОГИИ МОДЕЛИРОВАНИЯ СИСТЕМ ДИСТРИБУЦИИ ТОЧНОГО ВРЕМЕНИ В СРЕДАХ С ТРОИРОВАНИЕМ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Синтез оптимальных технических решений для систем дистрибуции точного времени в мультисервисных сетях передачи данных (МСПД) в качестве первого шага алгоритма оптимизации предполагает построение множества возможных технических решений. В состав этих решений могут входить самые разные компоненты [2]. При этом множество

решений часто строится на комбинаторной основе и не все конфигурации оборудования из этого множества могут априори хорошо (или плохо) выполнять свою функцию. Особенно это касается отказоустойчивых конфигураций, построенных с использованием принципа троирования с функциональной адаптацией элементов избыточности [3, 6].

Работоспособность многих конфигураций, как исходных, так и оптимальных, требует всестороннего тестирования. Испытание конфигураций на реальном оборудовании затруднено, а часто и невозможно, ввиду большого количества задействованных разнородных компонент (специализированные сервера и сервера общего назначения, коммутаторы и маршрутизаторы, линии связи и т. п.). В этих условиях значительный интерес представляют среды виртуализации разнородного оборудования и создание на этой основе испытательного стенда (или даже полигона) [1, 4, 7].

На базе технологий виртуализации, созданных в рамках проектов с открытым исходным кодом, используя IBM PC-совместимые компьютеры общего назначения, необходимо было разработать стенд для тестирования и отладки систем дистрибуции точного времени. В качестве внешнего оборудования по отношению к стенду допускаются лишь специализированные NTP-сервера и GPS-приемники, поддерживающие протокол NMEA. Стенд должен поддерживать эмуляцию сетевого оборудования компании Cisco и серверов с операционными системами семейств Microsoft Windows и Linux. Стенд должен поддерживать функции автоматического конфигурирования типовых элементов МСПД.

В качестве средства виртуализации маршрутизаторов компании Cisco был выбран проект Dynamips, в частности была использована версия 0.2.7 [9]. Эмулятор Dynamips в рамках данной работы используется в режиме гипервизора. Виртуализацию серверов общего назначения обеспечивает программный продукт Oracle VM VirtualBox версии 5.1.10 [10]. Для перехвата и инжекции сетевого трафика на различных интерфейсах компьютеров-хостов используется программный продукт WinPcap версии 4.1.3 [11].

Диалог с гипервизором осуществляет скрипт, написанный на языке программирования VBA, который по описанию варианта технического решения, представленному в виде листа книги Microsoft Excel, формирует необходимую топологию сети, создает файловое окружение для виртуальных маршрутизаторов и осуществляет их запуск. Этот же скрипт посылает команды системе виртуализации Oracle VM VirtualBox по запуску виртуальных машин, эмулирующих сервера общего назначения, включенные в вариант технического решения. В ручном режиме

запускаются лишь виртуальные машины, предназначенные для эмуляции атак. Использование объектной модели Microsoft Excel на верхнем уровне программного обеспечения стенда обусловлено тем, что для пакета прикладных программ «МультиМИР» [8], используемого для оптимизации технических решений в проекте, частью которого является данная разработка, эта модель является «родной».

Проведение испытаний различных технических решений в области дистрибуции точного времени в рамках описанного стенда показало удобство его использования. На одном компьютере с конфигурацией Intel Core i7/16Gb комфортно эмулируется одновременно до 10 маршрутизаторов и 2 серверов общего назначения. Дальнейшее наращивание топологии желательно реализовывать, подключая дополнительные хост-компьютеры, соответственно из расчета 1 компьютер не хуже выше указанной конфигурации на 10 типовых маршрутизаторов.

В настоящее время в рамках представленного стенда обеспечена поддержка типовых источников точного времени на базе GPS-приемников точного времени, поддерживающих протокол NMEA [5]. Была проведена большая работа по выбору параметров виртуальных машин Oracle VM VirtualBox, к которым предполагается физическое подключение приемников по интерфейсам RS-232 и/или USB. Испытания продемонстрировали успешную эмуляцию серверов времении, использующих дисциплину синхронизации 1PPS. Также в целом удалось обеспечить эмуляцию сред с троированием сетей передачи данных и проверку основных технических решений, используемых в рамках концепции троирования.

Список литературы

1. Андреева Н. Е., Бородин А. В. Стенд для исследования технологий дистрибуции точного времени в сетях передачи данных, построенных на базе оборудования Cisco // Человек, общество, природа в эпоху глобальных трансформаций: безопасность и развитие. Семнадцатые Вавиловские чтения: материалы постоянно действующей международной междисциплинарной конференции. Ч. 2. – Йошкар-Ола: Поволжский государственный технологический университет, 2014. – С. 241-242.

2. Бородин А. В. Об импортозамещении при создании систем дистрибуции точного времени в мультисервисных сетях передачи данных // Кибернетика и программирование. – 2015. – № 2. – С.78-97. – DOI: 10.7256/2306-4196.2015.2.14036.

3. Бородин А. В., Шобонова К. А. Разработка архитектуры высокопроизводительных отказоустойчивых вычислительных систем на основе концепции троирования с функциональной адаптацией элементов избыточности // Наука сегодня: постулаты прошлого и современные теории: материалы IV междуна-

родной научно-практической конференции (29 декабря 2015 г.). Ч. 1. – Саратов: Изд-во ЦПМ «Академия Бизнеса», 2015. – С. 56-60.

4. Бородин А. В., Варламов А. С., Кораблев Д. В. Создание учебно-испытательного полигона отработки технологий дистрибуции точного времени в сетях передачи данных // Наука и мир. – 2015. – № 6(22). – Т. 1. – С. 34-37.

5. Бородин А. В. Стоимость владения как критерий архитектуры первичного NTP-сервера на основе GPS-приемников коммерческой точности // Обозрение прикладной и промышленной математики. – 2009. – Т. 16. – В. 3. – С. 507–508.

6. Бородин А. В. Технико-экономическое обоснование варианта резервирования сетевой компоненты отказоустойчивой масштабируемой вычислительной системы специального назначения // Кибернетика и программирование. – 2015. – № 6. – С. 55-70. – DOI: 10.7256/2306-4196.2015.6.17523.

7. Бородин А. В., Варламов А. С., Кораблев Д. В. Учебно-испытательный полигон отработки технологий дистрибуции точного времени // Кибернетика и программирование. – 2015. – № 3. – С. 11-23. – DOI: 10.7256/2306-4196.2015.3.15438.

8. Уразаева Т. А. Алгебра рисков: теория и алгоритмы. – Йошкар-Ола: Поволжский государственный технологический университет, 2013. – 209 с.

9. Cisco 7200 Simulator [Электронный ресурс]. – URL: http://www.ipflow.utc.fr/index.php/Cisco_7200_Simulator (дата обращения 11.11.2016).

10. VirtualBox. Материал из Википедии - свободной энциклопедии [Электронный ресурс]. – URL: http://ru.wikipedia.org/wiki/VirtualBox (дата обращения 11.11.2016).

11. WinPcap [Электронный ресурс]. – URL: http://www.winpcap.org/install/default.htm (дата обращения 11.11.2016).

СОДЕРЖАНИЕ

Научное издание

ИНЖЕНЕРНЫЕ КАДРЫ – БУДУЩЕЕ ИННОВАЦИОННОЙ ЭКОНОМИКИ РОССИИ

Материалы II Всероссийской студенческой конференции

Йошкар-Ола, 21-25 ноября 2016 г.

Часть 4

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – ОСНОВА СТРАТЕГИЧЕСКОГО ПРОРЫВА В СОВРЕМЕННОЙ ПРОМЫШЛЕННОСТИ

Ответственный за выпуск
А. Н. Савинов

Редактор
Л. С. Емельянова

Компьютерная верстка
С. Н. Эштыкова

Подписано в печать 22.12.2016. Формат 60×84 $^{1}/_{16}$.
Бумага офсетная. Печать офсетная.
Усл. печ. л. 14,42. Тираж 100 экз. Заказ № 5955.

Поволжский государственный технологический университет
424000 Йошкар-Ола, пл. Ленина, 3

Редакционно-издательский центр ПГТУ
424006 Йошкар-Ола, ул. Панфилова, 17