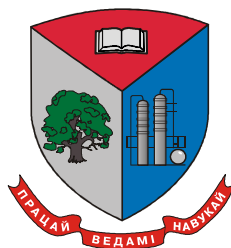


МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ»

Минское областное отделение РГОО
«Белорусское общество “ЗНАНИЕ”»
Международное общество ученых технического образования

*Посвящается
185-летию со дня рождения Д.И. Менделеева
160-летию лесотехнического образования Беларуси
55-летию организации НИЧ БГТУ*



ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

**Материалы докладов 83-й научно-технической конференции
профессорско-преподавательского состава,
научных сотрудников и аспирантов
(с международным участием)**

4-15 февраля 2019 года

Минск 2019

УДК 004:005.745(06)

ББК 32.97я73

И 74

Информационные технологии : материалы 83-й науч.-техн. конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 4-15 февраля 2019 года [Электронный ресурс] / отв. за издание И.В. Войтов; УО БГТУ. – Минск : БГТУ, 2019. – 123 с.

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

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

Рецензенты: д-р техн. наук, проф. кафедры информационных систем и технологий В.Л. Колесников;
канд. техн. наук, зав. кафедрой информатики и компьютерной графики Д.М. Романенко;
канд. техн. наук, декан факультета информационных технологий Д.В. Шиман

Главный редактор

ректор, д-р техн. наук И.В. Войтов

© УО «Белорусский государственный
технологический университет», 2019

СОДЕРЖАНИЕ

<i>Дятко, А. А.</i> Фазовый фронт сигнала двухточечного источника излучения.....	6
<i>Хворост, В. С., Шутько, Н. П.</i> Анализ подходов к пониманию пользовательского опыта и пользовательского интерфейса (UX / UI).	7
<i>Брусенцова, Т. П., Кишкурно, Т. В.</i> Принципы гештальта в дизайне интерфейсов и их влияние на визуальное восприятие.	8
<i>Белькевич, Р. И., Романенко, Д. М.</i> Концепция структуры осаждаемой информации для защиты авторских прав на аудиофайлы.....	10
<i>Осоко, С. А.</i> Решение задачи оптимизации эксгаустерной установки по критерию минимальной мощности привода.....	11
<i>Потапенко, Н. И.</i> Эклектика в современном веб-дизайне	12
<i>Потапенко, Н. И., Сапун, О. Л., Марсель де Луве.</i> Новый взгляд на лекцию в университете	13
<i>Савчук, Н. А., Новосельская, О. А.</i> Преобразование векторных данных в защищённой печатной продукции	14
<i>Мионов, И. А., Борисевич, С. А.</i> Интеграция информационных систем БГТУ в единый электронный университет	16
<i>Вахаб, А., Романенко, Д. М.</i> Метод стеганографического осаждения авторской информации на основе модификации цветовых параметров изображения	17
<i>Ломонос, Г. В., Романенко, Д. М.</i> Автоматическая классификация текстов с использованием нейронных сетей.....	18
<i>Азарчик, Р. В.</i> Сравнительный анализ нотаций моделирования ИТ-продуктов.....	19
<i>Щербакова, А. Н., Кудлацкая, М. Ф.</i> Тренды веб-дизайна 2019	20
<i>Олеферович, А. В., Романенко, Д. М.</i> Анализ результатов распознавания изображений с наличием дефектов.....	21
<i>Лукьянович, И. Р., Блинкова, Л. М., Аникевич, А. Г.</i> Разработка интернет- приложения для самостоятельной работы по английскому языку.....	22
<i>Жаворонок, П. Е., Жиляк, Н. А.</i> Алгоритм определения типа личности методами физиогномики.....	23
<i>Липович, А. В., Бельский, А. Б.</i> Совершенствование информационных ресурсов в сфере образования на основе их мониторинга	24
<i>Ciesielka, P., Urbanovich, P. P.</i> Security of applications for computer games.....	26
<i>Сенюк, В. К., Колесников, В. Л.</i> Бегradientный метод обучения полносвязной нейронной сети прямого распространения	28
<i>Берников, В. О., Урбанович, П. П.</i> Математическое моделирование стеганографической стойкости многоключевой системы	31
<i>Блинова, Е. А.</i> Алгоритмические особенности и оценка эффективности использования стеганографических методов в электронных картах.....	33
<i>Веремчук, С. Э., Гурин, Н. И.</i> Система тестирования знаний на естественном языке на основе семантической сети обучающей системы.....	36
<i>Жук, Я. А.</i> Оценка эффективности работы генератора семантической сети диалоговой информационной системы.....	38
<i>Суцень, А. А., Урбанович, П. П.</i> Применение форматов электронных книг при передаче конфиденциальной информации методами компьютерной стеганографии	39

<i>Шутько, Н. П., Урбанович, П. П.</i> Защита авторских прав на текстовые документы на основе стеганографической модификации цвета символов текста	41
<i>Jaber, G., Patsei.N.</i> Semantic routing scheme for information centric networking	44
<i>Белодед, Н. И</i> Рейтинговые показатели подготовки студентов и система оценки компетентности специалистов	45
<i>Навроцкий, Я. Ю., Пацей, Н. В</i> Сравнительный анализ схем именования в ICN ..	46
<i>Романенко, Д. М., Пацей, Н. В. Мартынюк, А. В.</i> Производительность каскадного кодека для исправления многократных модульных ошибок в беспроводных каналах связи	47
<i>Пацей, Н. В.</i> Алгоритм многоуровневой классификации объектов, основанный на кодах коррекции ошибок	48
<i>Радиванович, Д. А., Сухорукова, И. Г</i> Многокритериальная фильтрация электронной корреспонденции	49
<i>Литвинович, И. А., Наркевич, А. С.</i> Алгоритмы и подходы к обработке профилей социальной сети при поиске по фотографии	50
<i>Северинчик, Н. А., Шиман, Д. В.</i> Алгоритм разрешения консенсуса в Blockchain, основанный на машинном обучении.....	51
<i>Жуляк, Н. А., Шиман, Д. В., Наркевич, А. С.</i> Теоретические основы методологии синтеза вычислительных систем реального времени	52
<i>Капелько, И. В., Шиман, Д. В.</i> Трёхуровневая токенизация для автоматического реферирования текста.....	53
<i>Парамонов, А. И.</i> Удаленный контроль в дистанционном обучении на основе методов идентификации лиц.....	54
<i>Панченко, О. Л., Пацей, Н. В.</i> Методы оперативной классификации текстовых документов.....	56
<i>Рауба, А. А., Сухорукова, И. Г.</i> Разработка алгоритма или метода монетизационных процессов в web-приложениях.....	58
<i>Левин, М. А., Шиман, Д. В.</i> Модель нагрузки для проведения нагрузочного тестирования информационной инфраструктуры.....	60
<i>Демещик, А. С., Сухорукова, И. Г.</i> Сентимент-анализ. Сферы применения, проблемы, задачи.....	62
<i>Бакиев, А. Р., Наркевич, А. С.</i> Алгоритмы и методы определения движущегося объекта для создания облачного видеорегистратора.....	64
<i>Рудяк, И. М., Воронов, А. А.</i> Применение технологии Java для цифровой подписи электронного документа.....	66
<i>Никитенок, В. И., Ветохин, С. С., Бахарь, А. М., Терешко, Е. В.</i> Сравнительный анализ алгоритмов проверки простой гипотезы о параметре экспоненциального распределения	68
<i>Казимова, Д. А., Тусупхан, А. Т., Ермекова, Д.</i> Подготовка ИТ-специалистов в условиях цифровизации Казахстана	69
<i>Горбунова, Н. А., Спирина, Е. А.</i> К вопросу о сущности понятия «Алгоритм»..	71
<i>Демиденко, А. И., Ременюк, О. В.</i> Перспективность и актуальность применения мобильной платформы «1С:Предприятия» в разработке мобильных приложений.....	73
<i>Рейзенбук, К. Э., Иванов, А. А.</i> Автоматизация процесса поддержки принятия решений при кредитовании физических лиц.....	75
<i>Селедцова, А. В.</i> Пути внедрения медицинских информационных систем	77

<i>Шатько, Д. Б., Крюкова, В. В.</i> Информационно-аналитические технологии в системе менеджмента качества образовательной организации.....	79
<i>Демиденко, А. И., Николаенко, Е. П.</i> Влияние цифровизации экономики на информационную безопасность предприятия	81
<i>Крамарь, А. В., Демиденко, А. И.</i> Одностраничный сайт как инструмент предоставления информации компании.....	83
<i>Мамошина, М. А., Демиденко, А. И.</i> Использование гиперконвергентной архитектуры как способ упрощения ИТ-инфраструктуры промышленных предприятий.....	85
<i>Кульмамиров, С. А., Ордабаева, Г. К., Кыдырбекова, А. С.</i> Исследование биометрического способа распознавания личности	87
<i>Семенов, А. С.</i> Гис-анализ обеспеченности населения города Молодечно озелененными участками в жилой застройке	96
<i>Смотриков, Е. С., Демиденко, А. И.</i> Интеграция ERP систем и АСУТП как первостепенная задача современного производства.....	97
<i>Шульгина-Таращук, А. С. Турдыбекова, К. М. Турдыбекова, К. К.</i> Методы шифрования информации	99
<i>Допира, Р. И., Попова, Н. В.</i> Формирование компетенций IT-специалиста применяя метод проектов на занятиях СРСП дисциплины «Программирование на C++».....	101
<i>Крупница, О. В., Бихдрикер, А. С., Панайотов, К. К.</i> Защита облачной архитектуры на основе технологии открытых ключей.....	103
<i>Сырцева, С. В., Буганов, О. В.</i> Применение технологии блокчейн в аграрном секторе	105
<i>Афоница, Ю. А., Демиденко, А. И.</i> Проблемы и перспектива интеграции информационных технологий в психологию	107
<i>Жумагулова, С. К., Нурланова, Б. М.</i> Некоторые вопросы обработки данных	111
<i>Жумагулова, С. К. Спирина, Е. А., Смирнова, М. А.</i> Создание программы криптографического преобразования данных	112
<i>Топаз, А. А., Волосюк, А. И.</i> Дешифрирование лесной растительности на основе спектральных индексов.....	113
<i>Турдыбекова, К. М., Шульгина-Таращук, А. С., Турдыбекова, К. К.</i> Власть информационных и коммуникационных технологий.....	115
<i>M. Błaszczak, P.P. Urbanovich, Server security of the multiplayer game «PROJECT I.G.I. 2: COVERT STRIKE».....</i>	117
<i>P. Rab, P.P. Urbanovich, Methods, software and hardware tools for cryptocurrency technologies</i>	120

ФАЗОВЫЙ ФРОНТ СИГНАЛА ДВУХТОЧЕЧНОГО ИСТОЧНИКА ИЗЛУЧЕНИЯ

Рассматривается анализ фазового фронта электромагнитной волны, создаваемой когерентными источниками излучения из двух точек пространства.

Фазовый фронт электромагнитной волны, создаваемой несколькими (двумя или более) источниками когерентного излучения, имеет довольно сложную форму. Направление вектора нормали к этому фронту определяет направление распространения волны и идентифицируется пеленгатором с направлением на некоторый эквивалентный (виртуальный) источник излучения. При этом, направление, определяемое пеленгатором, может ориентироваться в точку за пределами базы источников излучения [1-2].

Вопросы, связанные с анализом формы фазового фронта электромагнитной волны двух источников когерентного излучения и поведением угломерной системы в этой ситуации рассматривались в ряде работ [1-2]. В отмеченных работах представлены разнообразные подходы к анализу работы угломерных систем в условиях двухточечного источника когерентного излучения. Однако, отсутствие единого подхода затрудняет использование предлагаемых методов анализа для сравнения результатов при решении конкретных задач измерения угловых координат для этих условий.

В результате проведенных исследований получены аналитические выражения и результаты численных экспериментов, позволяющие вычислить угловое положение виртуального источника излучения в системе координат наблюдателя в зависимости от параметров системы излучателей. Показано, что полученные результаты совпадают с результатами, полученными ранее в известных публикациях [1-2] для некоторых частных случаев.

ЛИТЕРАТУРА

1. Куприянов А.И., Сахаров А.В. Теоретические основы радиоэлектронной борьбы: Учебн. пособие / А.И. Куприянов, А.В. Сахаров. – М.: Вузовская книга, 2007.
2. Леонов А.И., Фомичев К.И. Моноимпульсная радиолокация. М., «Сов. Радио», 1970. – 392 с.

АНАЛИЗ ПОДХОДОВ К ПОНИМАНИЮ ПОЛЬЗОВАТЕЛЬСКОГО ОПЫТА И ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА (UX / UI)

В эпоху информатизации всех видов деятельности человека вопросы продвижения бизнеса в сети Интернет, создания бренда компании в соответствии с её целями являются актуальными как никогда прежде. Это объясняется тем, что в каждой отрасли рынка постоянно растет количество компаний, предоставляющих похожие услуги или продающих аналогичный товар. Ещё одной предпосылкой является доступность разработки веб-сайта компании путем различных конструкторов сайтов. Путем правильной организации пользовательского интерфейса (UI), а также формирования определенного пользовательского опыта на лендинг странице (UX) компании могут наиболее эффективно достигать таких целей разработки лендинг страницы, как продажа товара или услуги, получение почтового адреса пользователя, получение заявки на консультацию.

Понятие пользовательского интерфейса достаточно понятно и точно определено в сфере дизайна. Пользовательский интерфейс на веб-странице представлен такими элементами, как кнопки, меню, формы, ссылки, модальные окна, контент. Взаимодействуя с ними, пользователь достигает своих целей на сайте.

Согласно документу международной организации по стандартизации ISO 9241-210:2010 Ergonomics of human-system interaction термин UX (пользовательский опыт) понимается как пользовательское восприятие и реакции на взаимодействие с сервисом, услугой или продуктом. UX включает эмоции, ожидания, предпочтения, личное восприятие, физические, психические и поведенческие реакции, которые возникают перед, во время и после взаимодействия [1]. Таким образом можно сделать вывод, что термин пользовательского опыта намного шире, чем пользовательский опыт работы с сайтом компании. Он также включает особенности услуги или продукта и их влияние на реакции пользователя, работа менеджеров, курьеров, а также реакции, возникшие уже после взаимодействия. Контроль всех сфер взаимодействия с пользователем – достаточно трудоёмкая и глобальная задача, решаемая огромным количеством специалистов различных направлений и координируемая вышестоящим членом компании.

Как часть всего опыта взаимодействия пользователя с продуктом или услугой рассмотрим опыт взаимодействия пользователя с веб-сайтом компании. В UX дизайн входит изучение потребностей пользователей и схем поведения, прототипирование, тестирование и планирование развития. Основные вопросы, решаемые UX дизайнером: постановка целей и задач, подбор подходящих UX инструментов для реализации целей, разработка продукта, максимально удобного и легкого в восприятии целевой аудиторией, анализ конечного результата – соответствует ли продукт ожиданиям заказчика и насколько высок уровень удовлетворенности пользователей [2]. Любое улучшение опыта взаимодействия нацелено на повышение эффективности [3].

Таким образом дизайн интерфейса и разработка пользовательского опыта на веб-сайте преследуют одну и ту же цель – сделать сайт максимально доступным и понятным для пользователя, используя различный инструментарий и подходы. При этом пользовательский интерфейс – это один из компонентов, формирующих опыт взаимодействия пользователя с веб-сайтом.

ЛИТЕРАТУРА

1. ISO 9241-210:2010(en) [Электронный ресурс] / Online Browsing Platform. – Режим доступа: <https://www.iso.org/obp/ui/ru/#iso:std:iso:9241:-210:ed-1:v1:en>.
2. UX дизайнер [Электронный ресурс] / BuduGuru. – Режим доступа: <http://buduguru.org/profession/19>.
3. Гарретт Дж. Веб-дизайн: книга Джесса Гарретта. Элементы опыта взаимодействия / Дж. Гарретт. СПб.: Символ-Плюс, 2008.

УДК 004. 514

Т. В. Кишкурно, ст. преп.; Т. П. Брусенцова, ст. преп.
(БГТУ, г. Минск)

ПРИНЦИПЫ ГЕШТАЛЬТА В ДИЗАЙНЕ ИНТЕРФЕЙСОВ И ИХ ВЛИЯНИЕ НА ВИЗУАЛЬНОЕ ВОСПРИЯТИЕ

Задача дизайнера интерфейсов состоит в том, чтобы сделать интерфейс визуально привлекательным, удобным и интуитивно понятным пользователю.

Человек воспринимает интерфейс с помощью зрения. Но не все что мы видим, воспринимается нами однозначно. Восприятие – поистине таинственный процесс, и то, как человек воспримет что-то, не возможно полностью проконтролировать, но можно предугадывать то,

как поведут себя те или иные группы людей. И в этом нам могут помочь знания ключевых принципов гештальт психологии.

Гештальт (нем. Gestalt – образ, форма, структура) – это пространственно-наглядная форма воспринимаемых предметов, чьи существенные свойства нельзя понять путем суммирования свойств их частей. Гештальт-психология гласит, что человеческому мозгу присуще запоминать целостный образ, а не отдельные его части. Так же и пользователь воспринимает веб-страницу при первом посещении. Важно понять, как дизайн интерпретируется и воспринимается в визуальной коммуникации. Посредством изучения зрительного восприятия были сформулированы многие законы группировки элементов.

Наше восприятие относит элементы как принадлежащие одной группе по следующим признакам: близость, сходство, общая область, непрерывность.

Близость. Элементы, расположенные близко друг к другу, воспринимаются как единая логическая группа. Дизайнеры все время используют закон близости – это один из распространенных способов, с помощью которого мы располагаем элементы интерфейса, чтобы показать их взаимосвязь. Каждый посетитель социальных сетей или интернет-магазинов ежедневно наблюдает этот принцип.

Сходство. Элементы, имеющие сходные визуальные характеристики, воспринимаются как единое целое или как часть одной группы. Сходство часто используется на веб-сайтах интернет магазинов при показе товара.

Общая область. Аналогично принципу близости, элементы, расположенные в одной и той же области, воспринимаются как сгруппированные. Принцип общей области чаще всего используется в блогах. Так пользователю легче воспринимать сразу много информации, ведь разделы поделены на равные области.

Непрерывность. Элементы, следующие за непрерывной линией, воспринимаются как сгруппированные. Чем мягче сегменты линии, тем больше мы видим их как единую форму; наш ум предпочитает путь наименьшего сопротивления. Принцип непрерывности усиливает восприятие сгруппированной информации, создает порядок и направляет пользователей через разные сегменты контента.

Дизайн пользовательского интерфейса – это не только красочные пиксели и яркая графика. В основном это коммуникация, эффективность и удобство. Понимание Гештальт принципов даёт нам возможность создавать более гармоничный дизайн и повышает вероятность успешной передачи нашего сообщения аудитории.

КОНЦЕПЦИЯ СТРУКТУРЫ ОСАЖДАЕМОЙ ИНФОРМАЦИИ ДЛЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ НА АУДИОФАЙЛЫ

Защита авторства в современном обществе является важной и при этом очень сложной задачей. Изучая аспекты внедрения авторской информации в цифровые аудиофайлы, необходимо чётко понимать, как эта информация должна выглядеть, что содержать и какими характеристиками обладать. Отметим, что все существующие форматы авторской информации закреплены в разнообразных международных стандартах ISO, при этом ключевыми являются: ISNI (ISO 27729:2012), ISRC (ISO 3901), ISAN (15706:2002 & ISO 15706-2) и ISMN (ISO 10957). Все стандарты обладают разными характеристиками, но среди них можно выделить общие моменты: информацию необходимо разбивать на блоки, её средняя длина составляет 10-14 символов; информация должна идентифицировать автора (исполнителя), страну происхождения, год создания и связанные имена.

На основе анализа выше приведенных стандартов была предложена следующая концепция, описывающая структуру авторской информации:

- идентификатор состоит из 4 блоков и разделяется символом «-»;
- первый блок – владелец (уникальный символьно-цифровой код из 4 элементов);
- второй блок – автор (уникальный символьно-цифровой код из 4 элементов);
- третий блок – страна выпуска в двух символьной кодировке страны;
- четвертый блок – год выпуска вида YYYY (согласно ISO 8601);
- пятый блок – контрольная цифра.

Последний блок с контрольной цифрой предназначен для защиты от разного рода фальсификации идентификатора автора. Рассмотрим его генерацию на примере следующей авторской информации: Q3KD-GT42-US-2013-8. Для расчёта необходимо взять из таблиц UTF-8 эквиваленты символов идентификатора в шестнадцатеричном виде. Далее эти значения суммируются:

$$Q3KD = 51_{16} + 33_{16} + 4b_{16} + 44_{16} = 113_{16}$$

$$GT42 = 47_{16} + 54_{16} + 34_{16} + 32_{16} = 101_{16}$$

$$US = 55_{16} + 53_{16} = A8_{16}$$

$$2013 = 32_{16} + 30_{16} + 31_{16} + 33_{16} = C6_{16}$$

Итого:

$$113_{16} + 101_{16} + A8_{16} + C6_{16} = 382_{16}$$

Переводя число из шестнадцатеричной системы счисления в десятичную, получим $382_{16} = 898_{10}$. Далее к полученному значению применяем операцию вычисления остатка от целочисленного деления на 10 и получаем следующую контрольную цифру $898 \bmod 10 = 8$. Стоит отметить, что для подтверждения уникальности идентификатора предполагается использование операции хеширования.

УДК 674.08:621.867.8

С. А. Осоко, ассист. (БГТУ, г. Минск)

РЕШЕНИЕ ЗАДАЧИ ОПТИМИЗАЦИИ ЭКСГАУСТЕРНОЙ УСТАНОВКИ ПО КРИТЕРИЮ МИНИМАЛЬНОЙ МОЩНОСТИ ПРИВОДА

Для сбора и удаления, образующихся при работе деревообрабатывающего оборудования опилок, стружки и пыли существуют цеховые системы пневмотранспорта древесных отходов. Эти установки кроме своей основной функции выполняют также функции вытяжной вентиляции помещений.

Ранее проведенными исследования [1] установлено, что системы пневмотранспорта в деревообработке обладают следующими особенностями: высокой долей потребления электроэнергии в цеховых энергозатратах (20–70%), удельные энергозатраты 0,2–0,3 Вт·ч/(кг·м) и наличие электроприводов значительной мощности 17–45 кВт. Практика проектирования и результаты исследований эксгаустерных установок показывают, что большая часть энергозатрат в них приходится на трубопроводы, доля которых составляет обычно 65–75% общих потерь давления. Это обстоятельство требует соответствующего внимания при разработке мер по энергосбережению.

Для поиска оптимальной конфигурации сети трубопроводов в цеховой эксгаустерной установке было проведено исследование. Установлено, что изменение расположения коллектора, магистрали и циклона позволяет уменьшить потери давления. В результате уменьшается требуемая мощность привода эксгаустерной установки. Установлено, что таким способом можно сократить энергопотребление на 5%.

Полученные результаты позволяют говорить, что разработанная методика оптимизации конфигурации сети трубопроводов может быть использована в целях энергосбережения при проектировании и модернизации цеховых систем пневмотранспорта древесных отходов.

ЛИТЕРАТУРА

1. Трофимов, С. П. Снижение энергозатрат в трубопроводах цеховых систем пневмотранспорта древесных отходов / С. П. Трофимов // Ресурсосберегающие и экологически чистые технологии : тезисы докладов Второй научно-технической конференции, Гродно, 8-9 октября 1996 г. – Гродно : Гродн. гос. ун-т им. Я. Купалы, 1996. – С. 119-120.

УДК 004.514

Н.И. Потапенко, ст. преп. (БГТУ, г. Минск)

ЭКЛЕКТИКА В СОВРЕМЕННОМ ВЕБ-ДИЗАЙНЕ

История веб-дизайна насчитывает не более чем четверть века. Однако за этот относительно короткий промежуток времени произошли и происходят кардинальные изменения в веб-проектировании, это касается как внешнего оформления сайтов, так методов верстки и программирования.

Изменяются способы оформления и подачи контента, инструменты взаимодействия с пользователем. Мобильные технологии также вносят свои коррективы в представления о том, каким должен быть сайт.

К различным веб-стилям добавляются различные технологические эффекты в виде анимации, синемаграфов, параллаксов, видеофонов, морфинга и сторителлинга. Веб-сайт – отражение нашей реальности через призму восприятия веб-дизайнера, заказчика, потребителя, общих тенденций в сфере экономики, политики, искусства. В последние два-три года наблюдается уход от явно выраженных сложившихся стилей к эклектике. Эклектика – смешение, соединение разнородных стилей, идей, взглядов и т. п. Веб-дизайнеры также стали использовать смешение стилей в веб-дизайне.

Стало достаточно сложно отнести стиль современного веб-сайта к какому-либо сложившемуся стилю. Присутствует смешение различных стилей. Можно выделить следующие тенденции:

– цветовые ассоциации и смешение цветов для объединения пространства; яркие элементы в виде кнопок, больших меню, инте-

рактивные персонажи, появляющиеся внезапно на традиционном сайте и призванные привлечь внимание;

– ретро-элементы в смешении с синемаграфами, анимацией, вкраплением ярких элементов;

– минимализм превращается в нео-минимализм с яркими акцентами, большими фото, иногда и параллаксами, морфингом.

Эклектика свободна от стереотипов. Помимо смешения стилей, технологичности на дизайн сайтов влияют и технологии виртуальной реальности, 3D и нейроинтерфейсы, голосовые помощники.

ЛИТЕРАТУРА:

1. Сырых Ю. А. Современный веб-дизайн. Настольный и мобильный-3-е изд.- М.: Диалектика, 2014. – 381с.

2. <https://ru.wikipedia.org/wiki/> [Электронный ресурс]

УДК 004.514

Н. И. Потапенко^{*}, ст. преп.; О. Л. Сапун^{**}, зав. каф. ИТиМЭП,
к. п. н.; Марсель де Луве^{***}, директор
(*БГТУ, **БГАТУ, г. Минск, ***Leerbeleving, Нидерланды)

НОВЫЙ ВЗГЛЯД НА ЛЕКЦИЮ В УНИВЕРСИТЕТЕ

На формирование поколенческих ценностей влияют многие факторы – политические, экономические, социальные, технологические. Особую роль играет модель воспитания, принятая в семье. Выделяют три основных группы ценностей: универсальные (общечеловеческие); групповые; личностные (собственные ценности конкретного человека). Для поколения молодых людей, нынешних студентов, родившихся в период 2000-2010 годов присущи такие черты как индивидуализм, инфантилизм, «клиповое мышление», отсутствие живого общения («цифровые аборигены»), сосредоточенность на своём внутреннем мире, ставка на собственный потенциал и свою уникальность, создание своего мира (зачастую виртуального). В этих условиях перед педагогами стоит непростая задача- как организовать подачу знаний и обеспечить эффективность обучения? Традиционные методы вербальной лекции не работают. Поэтому должны принимать во внимание и использовать следующее: ускорять подачу информации и скорость обучения, использовать все возможности визуализации (яркость, зрелищность, наглядность), вводить в обучение элементы соревновательности, интерактивные динамические задания, дискуссия, мозговой штурм, кейс-метод, проблемные лекции (возможно, с обсуждением через Интернет в режиме он-лайн), использовать тренинговые формы работы, приме-

нять современные онлайн инструменты для организации фронтальной работы, такие как <https://ru.padlet.com/> - виртуальные доски для совместной работы, <https://kahoot.it/> - сервис для создания опросов и викторин, доступных и через мобильные устройства. Переключение внимания, создание игровых ситуаций отвлекает от монотонности изложения материала, создает элементы соревновательности и в конечном итоге повышает мотивацию у студентов.

ЛИТЕРАТУРА

1. У. Штраус, Н. Хоув «Поколения: История Будущего Америки» (Generations: The History of America's Future), 1991
2. Теория поколений: педагогам, учителям, родителям и детям [Электронный ресурс], доступ: <https://letidor.ru/>

УДК 004.056.53

Н. А. Савчук, магистрант;

О. А. Новосельская, доц., канд. техн. наук (БГТУ, г. Минск)

ПРЕОБРАЗОВАНИЕ ВЕКТОРНЫХ ДАННЫХ В ЗАЩИЩЕННОЙ ПЕЧАТНОЙ ПРОДУКЦИИ










Векторные данные позволяют качественно воспроизвести любое изображение в печати, поскольку не зависят от настроек изображения. Основу защиты документов составляют специальные штриховые изображения – как правило гильоши, которые воспроизводятся на бумаге специальными красками и способами печати. Для воспроизведения цветного гильоша возможно использовать триаду CMY со 100% заливками, которая в этом случае не требует растривания. Цветность узора будет определяться частотой и толщиной векторных штриховых элементов. Поскольку стандартным наблюдателем без специальных устройств невозможно определить исходное изображение и соотношение контуров для передачи градаций красками, то структура векторного изображения позволит применять их как средство защиты полиграфической продукции от фальсификации.

В работе разработаны видимые глазом узоры, создающие имитацию радужной печати, на основе векторных штриховых изображений. При этом особенностью элементов является сохранение штрихов при многокрасочной печати даже с использованием стандартного печатного оборудования. Эффект радужности реализуется за счет смешения субтрактивного синтеза при наложении красок и аддитивного синтеза при рассмотрении отпечатанного изображения с определенно-

го расстояния. Конечный узор определяется степенью приближенности линий и толщиной контуров. Изменяя угол поворота, радиус кривизны, масштаб и степень близости линий между собой достигается переменность цвета и форм.

Разработанные изображения были распечатаны и осуществлено измерение цвета. Результаты измерения представлены в таблице.

Таблица 1 – Среднее значение координат цвета

Рисунок и масштаб воспроизведение	Оптическая плотность по краскам			
	С	М	У	К
 (50%)	0,188	0,62	0,778	0,392
 (100%)	0,228	0,536	0,806	0,378
 (500%)	0,24	0,41	0,848	0,32
 (50%)	0,164	0,67	0,734	0,394
 (100%)	0,144	0,49	0,558	0,316
 (500%)	0,092	0,154	0,126	0,13
 (50%)	0,358	0,952	0,66	0,614
 (100%)	0,592	0,862	0,554	0,726
 (500%)	0,404	0,512	0,332	0,468

Ни одна точка не воспроизводится с заданным соотношением цветовых координат. Определяются доминирующие цвета, но также присутствуют примеси. Таким образом, если изначально не знать о параметрах задания цветного защитного элемента, то воспроизвести аналогичный эффект будет невозможно.

ИНТЕГРАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ БГТУ В ЕДИНЫЙ ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ

Система «Электронный университет» предназначена для автоматизации управления образовательным процессом, научно-исследовательской деятельностью, финансово-хозяйственными процессами обеспечения жизнедеятельности вуза, а главное – обеспечивает их полную интегрированность в информационно-коммуникационную образовательную среду университета. Система позволяет в любое время и практически в любом месте, где есть доступ к сети Интернет, использовать все ресурсы университета. Результат – создание комплексной среды, обеспечивающей студента и преподавателя на протяжении всего обучения современными технологическими решениями.

Проанализировав опыт других университетов можно выделить следующие основные модули электронного университета: веб-портал университета; электронная библиотека; система дистанционного обучения; электронная почта; облачное хранилище; сервисы для абитуриентов: онлайн регистрация для поступления в ВУЗ, назначение времени сдачи вступительных экзаменов, рассылка электронных писем с информацией о поступлении; сервисы для студента: информация об академической успеваемости за весь срок обучения, учебный план, уведомления о необходимости выплат, сервисы для преподавателя: возможность просмотра преподавателями списка студентов своего курса, академической успеваемости студентов курса, онлайн выставление оценки в электронную зачетку студента, составления индивидуального расписания преподавателя; сотрудничество с компаниями-работодателями, планирование и отслеживание бюджета: управление активами, контроль выплат, приобретение товаров и сервисов; управление финансовой деятельностью, генерация отчетов по финансовой деятельности, управление сопровождающей финансовой документацией; управление персоналом, учет трудовой деятельности каждого сотрудника, расчет заработной платы, ведение истории сотрудников; формирование отчетов по преподавателям, студентам, финансовому положению университета.

Разработка и интеграция специализированных подсистем в единый комплекс позволяет выстроить взаимосвязанные процессы управления и аналитической обработки данных на различных этапах деятельности университета.

МЕТОД СТЕГАНОГРАФИЧЕСКОГО ОСАЖДЕНИЯ АВТОРСКОЙ ИНФОРМАЦИИ НА ОСНОВЕ МОДИФИКАЦИИ ЦВЕТОВЫХ ПАРАМЕТРОВ ИЗОБРАЖЕНИЯ

Проблема защиты авторских прав существенно обострилась в связи с вступлением человечества в цифровую эру, где вся информация хранится и передается в цифровом виде. Одним из направлений решения указанной проблемы является применение современных стеганографических методов.

Ранее описывалась [1] предлагаемая модификация техники осаждения авторской информации для метода LSB, суть которой заключалась в следующем. Авторский текст, как и в методе LSB, в соответствии с кодировкой ASCII преобразуется в числовой вид, однако замена значений трех составляющих цвета (red, green, blue) будет осуществляться не в двоичном, а в десятичном виде.

В ходе исследования было обнаружено, что при определенных ситуациях осаждение авторской информации по данному методу может приводить к существенному изменению цвета (в пределах 5-10%), что является недопустимым. Соответственно было предложено выполнять следующие предварительные операции. На первом этапе вычисляется сумма ASCII кодов осаждаемой информации. Так, например, если авторский текст будет DMITRI, то данный параметр будет составлять $68+77+73+84+82+73=457$. Пусть 6 пикселей изображения, в которые будет осаждаться авторский текст, будут: RGB (81 83 82), (53 55 54), (78 74 75), (99 93 95), (83 75 72), (86 88 85) (полужирным начертанием отмечены цифры, подлежащие замене при осаждении). Рассчитаем сумму чисел, составленных из подлежащих замене цифр для каждого пиксела: $12+34+85+95+32+65=323$. Далее вычисляется понижающий осаждаемые числа коэффициент: $323/457 = 0.706$ или примерно 70 % (для буквы А это соответствует вычитанию $65 \times 0.3 = 21$). Далее из каждого кода осаждаемого символа вычитается данное число, т.е. осаждению будут подлежать следующие значения: 47 56 52 63 61 52. В целом исследование показало, что введение понижающего коэффициента позволит добиться различия в цветах истинных и модифицированных (с осажденной информацией) пикселей изображения в пределах 2-4%, что является допустимым.

ЛИТЕРАТУРА

1. Вахаб А., Романенко Д.М. Методы цифровой стеганографии на основе модификации цветковых параметров изображения // Труды БГТУ. 2018. № 1(206): Физ.-мат. науки и информатика. С. 94-98.

АВТОМАТИЧЕСКАЯ КЛАССИФИКАЦИЯ ТЕКСТОВ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

В современном информационном обществе с активным и повсеместным использованием компьютеров, а также с увеличением объемов хранящейся информации в электронном виде автоматическая классификация текста, т.е. определение принадлежности текста к некой категории, является актуальной и крайне важной задачей.

Классификация применяется в решении многих практических задач, таких как: фильтрация документов; распознавание спама; автоматическое аннотирование; поиск текстовых документов; навигация по большим информационным ресурсам; подбор рекламы; составление интернет-каталогов; классификация новостей; индексация данных в поисковых запросах и т.д.

Если данные не структурировать, не распределять по категориям, то через некоторое время будут накоплены массивы плохо структурированной информации, а отсутствие возможности вовремя и быстро получить необходимую информацию по нужной теме сделает бесполезной большую часть накопленной базы знаний.

Классификация текстов, являющаяся одним из способов структурирования данных, – это сортировка текстовых документов по заранее определенным категориям (тематика, стиль и т.д.). Методы классификации текстовых документов лежат на стыке двух областей: информационного поиска и машинного обучения. Общие части двух этих подходов – способы представления документов и способы оценки качества классификации текстов, а различия состоят только в способах собственно поиска. Как мощный механизм обучения нейронные сети могут широко применяться в различных отраслях. Нейросети должны использоваться для обобщения данных, а не для определения, атрибуты и критерии которого крайне важны при сборе и анализе данных. Обучающиеся машины часто используются при формализации знаний из данных реального мира, но все же сами обучающиеся машины не могут генерировать принципы формализации – здесь не обойтись без помощи человека. Применение автоматических систем классификации текстов позволит сократить трудозатраты человека на рубрикацию и поиск необходимой информации предоставляемой информационными системами, а также позволит сократить участие или вовсе не привлекать специалистов при размещении информации в базе знаний.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ НОТАЦИЙ МОДЕЛИРОВАНИЯ ИТ-ПРОДУКТОВ

Можно выделить две основные проблемы при проектировании ИТ-продуктов:

1. Создание проекта продукта, который бы, представлял из себя максимально полное описание функционирования объекта проектирования с оптимизацией всех процессов при выполнении определённых бизнес-правил и обязательного достижения поставленной цели.

2. Обеспечение конечных пользователей удобным интерфейсом, т. е. создавать такие ИТ-продукты, которые позволили бы пользователю выполнять с помощью ЭВМ необходимые действия без глубокого изучения в полном объеме специальной литературы.

Для успешной реализации проекта, объект проектирования должен быть прежде всего адекватно описан, построены полные и непротиворечивые функциональные и информационные модели объекта.

Для построения и описания моделей и используются различные методологии и нотации.

Рассматриваемые нами методологии и нотации: ARIS (Architecture of Integrated Information Systems) – eEPC (Event-driven Process Chain), SADT (Structured Analysis and Design Technique) – (IDEF0), UML (Unified Modeling Language) – Activity Diagram (UML) и BPMN.

По результатам анализа можно сделать следующие выводы. Методология EPC не акцентирует внимание на степени детальности и полноты получаемых диаграмм и могут применяться, когда ведущая роль в организации процесса сохраняется за человеком. Нотация IDEF0 не поддерживает иллюстрацию потоков данных и логику взаимодействия, а инструментальные средства построения подобного рода диаграмм подходят для целей моделирования и реинжиниринга бизнес-процессов. Также отсутствует возможность реализации функциональных IDEF-моделей в объектно-ориентированном программном коде. Диаграммы UML и BPMN поддерживают и описание логики взаимодействия, и отображение объектов данных. Диаграммы UML ориентированы на разработку программного обеспечения. С помощью инструментальных средств, поддерживающих нотацию BPMN, одинаково успешно можно решать задачи и по моделированию бизнес-процессов, и по автоматизации деятельности предприятия.

ТРЕНДЫ ВЕБ-ДИЗАЙНА 2019

Современный и стильный дизайн сайта – это дизайн, который соответствует современным трендам, и от этого зависит успех вашего сайта. Каждый год многое меняется в веб-дизайне, поэтому чтобы сайт выглядел современно и приносил доход, перед его созданием нужно продумать дизайн с точки зрения не только визуального восприятия, но и простоты использования. Рассмотрим основные тренды в веб-дизайне в 2019 году и проведем анализ, какие изменения стоит внести на сайт БГТУ ФИТ, чтобы он был современным и простым в использовании.

1. Яркие цвета. В 2019 году цвета будут еще более яркими, смелыми и насыщенными, чем в 2018. Сайт БГТУ ФИТ относится к информационному сайту, поэтому не совсем уместно насыщать дизайн яркими цветами.

2. Видеоконтент. Видео привлекает внимание пользователей, чем дольше пользователь остается на вашем сайте, тем выше вероятность его конверсии. На сайте БГТУ ФИТ есть пример внедрения видео на странице «Абитуриенту».

3. Иллюстрации. Иллюстрация может играть роль как декоративного элемента, так и информативного. На сайте ФИТ имеются красочные иллюстрации на странице «Советы», что несомненно является плюсом.

4. Микро-анимации. Микро-анимация привлекает внимание пользователей, обеспечивает интуитивно понятный интерфейс при просмотре веб-сайта. Рекомендуется добавить анимированное меню на сайт ФИТ, это сделает его более динамичным и привлекательным.

5. Минимализм. Это дизайн с преобладанием светлых оттенков и невесомых фигур. Дизайн сайта ФИТ не является исключением.

6. Собственные изображения. Собственные фотографии отражают только вашу тематику и отличают вас от конкурентов. На главной странице сайта ФИТ находится слайдер с собственными фотографиями. Но следует заменить темный фон слайдера на светлый, это ближе стилю минимализм. Недостатком сайта является отсутствие контента в фотогалерее.

Кроме представленных выше рекомендаций, необходимо подобрать для сайта ФИТ современные шрифты. Например, шрифт Century Gothic выглядит лаконично, современно, соответствует ин-

формационному сайту. Так же стоит добавить больше свободного пространства, что соответствует популярному на сегодняшний день стилю минимализм. Для этого был модифицирован слайдер на главной странице и футер сайта. Небольшие изменения с учетом современных трендов могут преобразить дизайн, сделать его более приятным и облегчить восприятие дизайна пользователем, а также поиск необходимой информации.

УДК 004

А. В. Олеферович, ассист.;

Д. М. Романенко, доц., канд. техн. наук (БГТУ, г. Минск)

АНАЛИЗ РЕЗУЛЬТАТОВ РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЙ С НАЛИЧИЕМ ДЕФЕКТОВ

Распознавание образов на изображении является важной и одновременной сложной задачей, которую приходится решать в условиях глобальной информатизации и автоматизации практически всех сфер деятельности человека. Ранее в качестве метода распознавания был выбран метод контурного анализа [1]. Однако в ходе его изучения было выявлено, что основным недостатком является существенное влияние дефектов изображения на точность процесса распознавания. Был сделан вывод о том, что метод контурного анализа требует проведения предварительной обработки изображения. Контурный анализ подвержен главным образом воздействию двух групп факторов, отрицательно влияющих на результаты распознавания.

Первая группа факторов связана с проблемой выбора контура на изображениях. Контур – строго определенная дискретная структура. Однако слабовыраженные объекты имеют большое количество реальных изображений. Объект может не иметь четкую границу (размытым в виду различных факторов), он может быть идентичным по яркости и цвету с фоном. Все эти факторы приводят к тому, что контур может быть не выбран или выбран неправильно.

Ко второй группе факторов относятся различные дефекты изображения (шумы, царапины и т. д.), которые существенно усложняют (либо снижают эффективность) процесс распознавания. Наибольшее влияние в данной группе факторов оказывают царапины. Методы обнаружения границ выделяют в изображении только пиксели, лежащие на контуре. На практике, это множество пикселей редко отображает контур достаточно точно, по причине царапин, которые имитируют

разрывы контуров из-за неоднородности освещения, а значит, при их наличии зачастую нарушается целостность контуров.

Далее с помощью гистограммы изучалось влияние степени дефекта изображения на определение контура, а следовательно и процесс распознавания в целом.

Таким образом необходимо отметить, что метод контурного анализа достаточно хорошо справляется с распознаванием образов на изображениях плохого качества с достаточно большим количеством дефектов. Однако если говорить об его применении в качестве инструмента для извлечения и сравнения образов, например, товарных знаков, логотипов и т.д. с разных изображений (одно – оригинальное, второе – анализируемое), то однозначно можно говорить о необходимости проведения предварительной обработки с целью сохранения истинных разметов объектов, полученных после этапа распознавания.

УДК 004.738.1

И. Р. Лукьянович, доц., канд. техн. наук;
Л. М. Блинкова, ст. преп.; А. Г. Аникевич, студ. (БГУ, г. Минск)

РАЗРАБОТКА ИНТЕРНЕТ-ПРИЛОЖЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО АНГЛИЙСКОМУ ЯЗЫКУ

Наибольшую важность в настоящее время приобретают педагогические подходы и технологии, которые ориентируются не столько на усвоение обучающимися знаний умений и навыков, сколько на создание определенных условий, в которых студенту дается возможность самостоятельно контролировать свой маршрут и темп обучения. Такую возможность дает смешанное обучение, которое сочетает в себе электронные и традиционные методы.

Разработка программных ресурсов, реализующих элементы такой технологии обучения, является важной задачей, требующей участия преподавателей-предметников и специалистов по информационным технологиям. Лежащий нашей разработки «Сборник упражнений к практической грамматике английского языка = A Practical English Grammar Programmed Workbook» Р.У. Маркли и Э.У. Брокмана с дополнительными упражнениями Л.А. Барминой и И.П. Верховской не только позволяет организовать самостоятельную работу студентов, но и хорошо подходит для алгоритмизации и программной реализации.

Интернет-приложение, разрабатываемое нами по названному учебному пособию, позволит студенту самостоятельно изучать грамма-

тические правила в интерактивном режиме, а преподавателю получать информацию о результатах работы студента. Установка такого ресурса на сайте факультета и необходимость обеспечения доступа с различных устройств, включая мобильные, накладывает ограничения на размеры приложения и требует определенной организации взаимодействия между клиентом и сервером. Важной особенностью разработки должна быть возможность модульного наращивания системы. Онлайн-технологии в наибольшей степени адаптируют образование к условиям быстрого меняющегося современного мира - они делают материал доступным для обучающегося в любом удобном для него месте и в любое время.

УДК 004.031.43–044.962

П.Е. Жаворонок, магистрант;
Н.А. Жилияк, доц., канд. техн. наук (БГТУ, г. Минск)

АЛГОРИТМ ОПРЕДЕЛЕНИЯ ТИПА ЛИЧНОСТИ МЕТОДАМИ ФИЗИОГНОМИКИ

Алгоритм использует детектор на основе гистограммы направленных градиентов. Данная техника основана на подсчете количества направлений градиента в локальных областях изображения. Она вычисляет на плотной сетке равномерно распределенные ячейки и использует нормализацию перекрывающегося локального контраста для увеличения точности. Дескриптор НОГ, таким образом, является хорошим средством нахождения людей на изображениях.

Модель лица представляет собой шестьдесят восемь точек, расположенных по всей поверхности лица. По данной модели обучается предиктор формы для распознавания лица на изображении. Для наилучшего определения точек изображение переводится в оттенки серого. Далее с помощью библиотеки и обученной модели создается двумерный массив координат.

Для определения формы бровей вычисляется площадь треугольников, на которые образно разбит исследуемый объект лица. Исходя из этих площадей выбирается тип бровей.

Для описания характера человека по глазам необходимо вычислить ширину и высоту каждого глаза, найти расстояние между внутренними его углами, вычислить угол наклона глаза.

Для определения формы губ необходимо вычислить ширину и высоту рта и каждой губы. После этого необходимо измерять расстояние от подбородка до центра рта и от кончика носа до центра рта. Так же необходимо найти отношение каждой из этих длин к длине от кон-

чика носа к подбородку.

Физиогномика — псевдонаучный метод определения типа личности человека, его душевных качеств и состояния здоровья, исходя из анализа внешних черт лица и его выражения.

Определив тип каждого элемента лица используя методы физиогномики можно переходить к определению типа личности человека, описанию его психотипа и темперамента.

УДК 004.418:371.1.07

А. В. Липович, зам. начальника отдела;
А. Б. Бельский, системный аналитик
(ГИАЦ Минобразования, г. Минск)

СОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ В СФЕРЕ ОБРАЗОВАНИЯ НА ОСНОВЕ ИХ МОНИТОРИНГА

В условиях формирования информационного общества и цифровой экономики информационные ресурсы учреждений образования (ИР УО) становятся важным инструментом продвижения образовательных услуг не только на внутреннем, но и на мировом рынке. В связи с этим Министерством образования Республики Беларусь уделяется значительное внимание повышению содержательности ИР УО, что отражено в Концепции развития экспорта услуг (продвижение бренда «Образование в Беларуси») на 2018–2020 гг. [1]. Одним из мероприятий, предусмотренных данной концепцией, является проведение ежеквартального мониторинга качества размещения и обновления информации на интернет-сайтах учреждений образования.

Первые два мониторинга (за 3 и 4 квартал 2018 г.), в рамках которых были проверены 37 ИР учреждений высшего образования, осуществлялись в ручном режиме. На рисунке 1 отображены результаты этих мониторингов, представляющие оценку наличия на ИР УО информации по 16 содержательным критериям. Из данной гистограммы видно, что, во-первых, основные выявленные проблемы содержания ИР УО связаны с отсутствием информации о работе информационно-консультационного пункта Минобразования для иностранных граждан, ссылок на страницы учреждения в социальных сетях (в соответствии с письмом Министерства образования от 09.07.2018 № 08-23/1434 обязательным является наличие официального аккаунта в Facebook), а также справочной информации о Беларуси. Во-вторых, проведение мониторинга ИР УО в 3 квартале 2018 г. способствовало значительному повышению показателей качества информационного

наполнения данных ресурсов в 4 квартале, особенно по критерию наличия сведений о структурном подразделении УО, работающем с иностранными гражданами.

В то же время осуществление полноценного мониторинга ИР УО требует существенного расширения как перечня критериев, так и состава проверяемых организаций. Проведение такого мониторинга является весьма трудоемкой задачей, в связи с этим на протяжении 2018 г. ГИАЦ Минобразования разрабатывалась автоматизированная информационная система аудита ИР УО (АИС Мониторинг).

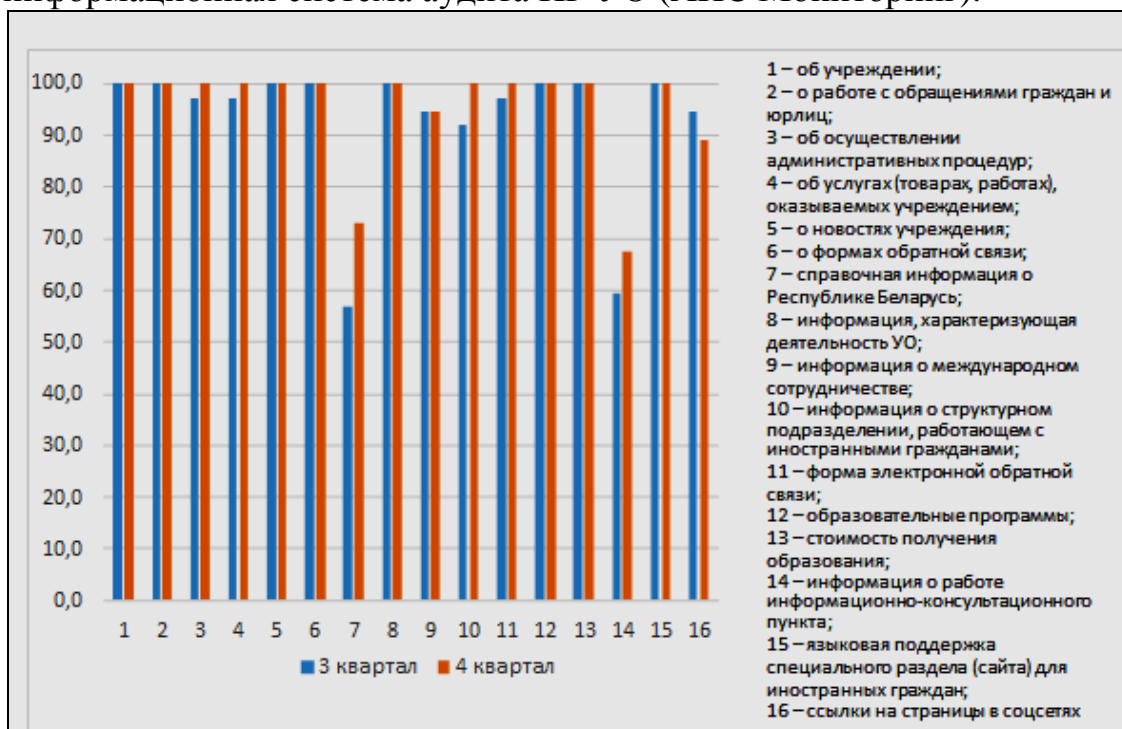


Рисунок 1 – Удельный вес ИР УО Республики Беларусь, содержащих информацию по указанным критериям в 2018 г., % от числа

Для разработки макетов АИС Мониторинг были использованы следующие программные средства: язык разметки HTML, каскадные таблицы стилей CSS, система управления реляционными базами данных Microsoft SQL Server и платформа для разработки веб-приложений ASP.NET. Данная АИС предусматривает формирование технического и экспертного рейтингов ИР УО, при этом оценка показателей технического рейтинга осуществляется в автоматизированном режиме, а экспертный рейтинг формируется 220 специалистами, назначаемыми управлениями образования и имеющими доступ к АИС. После проведения мониторинга ответственные лица от учреждений образования и местных исполнительных органов в сфере образования, имеющие доступ к АИС, проводят работу по устранению выявленных

нарушений.

Для дальнейшего совершенствования процессов мониторинга ИР УО целесообразно уточнить перечень критериев и разработать методику их оценки экспертами; обеспечить публикацию перечня ИР УО, в наибольшей степени соответствующих требованиям; организовать обучающие семинары по работе с АИС.

ЛИТЕРАТУРА

1 Об утверждении Концепции развития экспорта услуг (продвижение бренда «Образование в Беларуси») на 2018–2020 годы: приказ Министра образования Респ. Беларусь, 20 февр. 2018 г., № 130 // Эталон – Беларусь [Электронный ресурс] / ИЦПИ. – Минск, 2018.

УДК 004.42

P. Ciesielka, student (Lublin Catholic University, Poland);
P.P. Urbanovich, prof. (BSTU, Minsk, Belarus)

SECURITY OF APPLICATIONS FOR COMPUTER GAMES

The purpose of this paper is to analyze some aspects of the functionality of multiplayer computer games in relation to their structure and security. The main aspect of multiplayer games is to allow the player to the game together with other people. For this purpose, players must be at least two, however, their number can reach even thousands. The most widely used and most popular multiplayer game mode in modern times is the network game. Multiplayer games do not necessarily have to be played using more than one device.

If we talk about the security of our games or applications, we must bear in mind that it is impossible to completely secure such a structure. A programmer only can minimize risk or bypass problems.

The most important structural unit of the game is the database [1]. The security of databases is based on the use of a wide range of information security to protect them (database systems, database applications or function storage, potential added data, database servers and related network connections) against breach of confidentiality, integrity and security of accessibility. There are many types of control: technical, procedural, administrative and physical. This class of protection is a specialized topic in the wider field of computer security, information security and risk management.

Examples of types of threats that can occur in database systems are [2, 3]:

unauthorized, immeasurable or improperly performed activity by an authorized user, administrator, network managers,

getting malicious software that has the following effects: unauthorized access, disclosure of personal or proprietary data, deletion or corruption of data or programs, interruption or denial of authorized access to the database, attacks on other systems and failures of database services,

performance limitations,

physical damage to database servers caused by equipment failure, lightning, fire or liquid flooding,

improper creation of projects, databases, related programs and systems with errors creating various inconsistencies in security (eg unauthorized escalation of rights), loss or corruption of data, performance degradation, etc.,

data corruption or loss due to incorrectly entered data or commands.

Taking into account the listed and other important features we have created an application that allows you to implement the basic functions of a multiplayer computer game.

The structure of the application in the form of the created classes is shown in Figure 1.

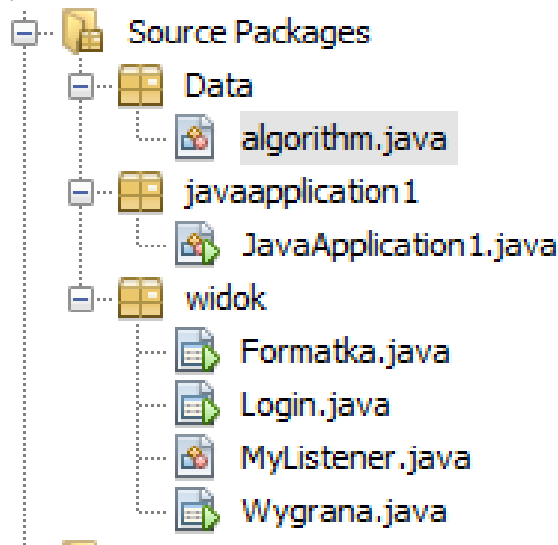


Fig. 1 – Classes structure in the application

In fig.1 we see three packages. The first is the Data package with the class algorithm.java containing the methods needed to perform calculations. The second (javaapplication1) in which the JavaApplication1.java class is contained is used to run the entire application. The third package called widok with classes Formatka.java, Login.java and Wygrana.java; in this package we also have the MyListener.java class that supports click events.

It should be noted that the Algorithm class implements the function of cryptographic encryption based on RSA. The RSA functions were written using security and crypto libraries. The first one is responsible for creating a pair of keys based on the size of 2048 bits. These keys are, of course, public and private.

The programming environments that were used in the creation of the application were IntelliJ IDEA and NetBeans. IntelliJ IDEA was used to create our database.

Currently developed application is being tested.

REFERENCES

1 Urbanowicz, P. Bazy danych: teoria i praktyka / Paweł Urbanowicz, Marcin Płonkowski, Dmitry Urbanowicz. – Lublin: KUL, 2010. – 382 s.

2 Ochrona informacji w sieciach komputerowych / pod red. prof. P. Urbanowicza. – Lublin: KUL, 2004. – 150 s.

3 Urbanovich, P. P. Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii/ P.P. Urbanovich: ucheb.-metod. posobiye dlya stud. – Minsk: BGTU, 2016. –220 s.

УДК 004.85

В. К. Сенюк, магистрант;

В. Л. Колесников, проф., д-р техн. наук (БГТУ, г. Минск)

БЕГРАДИЕНТНЫЙ МЕТОД ОБУЧЕНИЯ ПОЛНОСВЯЗНОЙ НЕЙРОННОЙ СЕТИ ПРЯМОГО РАСПРОСТРАНЕНИЯ

Градиентные методы обучения нейронных сетей при обратном распространении ошибки требуют больших затрат времени при сложных вычислениях частных производных, градиентов, изменений весов, моментов и скорости обучения. В виду большого объема вычислений при использовании градиентных методов хорошая сходимость алгоритмов достигается за большое количество эпох [1].

При решении тестовой задачи классификации нейронной сетью (при обучении градиентным методом) на вход подавалась относительно малая выборка данных, для активации нейронов использовалась сигмоидальная функция, методом «проб и ошибок» выбирались значения момента и скорости обучения. При этом, «приемлемые результаты», – сходимость и энергия ошибки достигались при обучении, примерно, за 10 – 15 тысяч эпох.

Представлялось целесообразным проанализировать «неградиентные» методы обучения нейронных сетей с целью выявления их достоинств и недостатков по сравнению с другими методами обучения.

Для решения задачи была разработана нейронная сеть с самоорганизацией, а для ее обучения использовался алгоритм «WTA» (победитель получает всё), который является аналогом алгоритма Ллойда для решения задачи кодирования. Целью обучения сети с самоорганизацией на основе конкуренции нейронов считается такое упорядочение нейронов (подбор значений их весов), которое минимизирует значение ожидаемого искажения, оцениваемого погрешностью аппроксимации входного вектора значениями весов нейрона-победителя. При P входных векторах X и применении евклидовой метрики эта погрешность, называемая также погрешностью квантования, может быть выражена в виде

$$E = \frac{1}{P} \sum_{i=1}^P \|x^i - w_w\| \quad (1)$$

где w_{win} – вес нейрона-победителя при предъявлении вектора x^i .

В соответствии с алгоритмом после предъявления вектора x рассчитывается активность каждого нейрона. Победителем признается нейрон с самым сильным выходным сигналом, т.е. тот, для которого скалярное произведение весов синапсов на входные значения является наибольшим. Это произведение соответствует наименьшему евклидовому расстоянию между входным вектором и весовым вектором нейрона. Победитель получает право уточнить свои веса в направлении вектора x согласно правилу Кохонена [2]

$$w_{win} \leftarrow w_{win} + \alpha [x - w_{win}], \quad (2)$$

где α – коэффициент скорости обучения.

Одно из достоинств алгоритма заключается в том, что коэффициент скорости обучения не подбирается «случайным образом», а в начале обучения инициализируется значением приблизительно равным единице и уменьшается в процессе обучения до значения близкого к нулю.

В полном виде анализируемый алгоритм можно представить следующим образом:

1. Нормализация данных обучающей выборки. На вход нейронной сети подаются нормализованные переменные.

2. Весовые коэффициенты нейронной сети инициализируются случайными значениями. Обычно эти значения находятся в диапазоне [-0.5; 0.5].

3. На входы сети подается нормализованный входной вектор одного из примеров обучающей выборки. Производится прямое распространение сигналов по нейронной сети.

4. Среди всех нейронов скрытых слоев осуществляется поиск нейрона с самым большим выходным значением N_{win} (нейрон-победитель).

5. В соответствии с пунктом 2 осуществляется обновление весового вектора нейрона-победителя.

6. Цикл повторяется с шага 3 до исчерпания количества эпох обучения.

Анализ алгоритма обучения производился на примере той же тестовой задачи классификации и обучающей выборки (таблица 1). При обучении в тысячу эпох сеть уже выдавала правильный результат, что доказывает быструю сходимость алгоритма.

Таблица 1 – Сравнение методов обучения НС

Параметры	Обучение с вычислением градиента	Обучение без вычисления градиента
Скорость обучения (V)	Подбирается вручную до достижения оптимального результата	Устанавливается примерно равным единице и уменьшается в процессе обучения до значения близкого к нулю $\alpha = \frac{\alpha}{N}$ где N – количество эпох обучения
Градиент (G)	Вычисляется в процессе обучения НС	Не используется
Количество эпох обучения (E)	Зависит от порога ошибки. В тестовой задаче E равно 10-15 тысячам эпох	E равно одной тысяче эпох
Конечное значение ошибки	Равно пороговому значению	На тестовой задаче равно примерно 0.0002

Таким образом, обучение на основе неградиентного метода позволяет отказаться от подбора гиперпараметров сети, градиента и других величин, вычисление которых является достаточно ресурсоемким без потери качества классификации и скорости обучения. На рис.1 показаны значения ошибки сети по эпохам обучения. Можно видеть, что уже на сотой эпохе сеть выдавала достаточно малую ошибку, что говорит о том, что после ста эпох обучение сети можно было бы остановить и, при этом, классификация осуществлялась бы правильно.

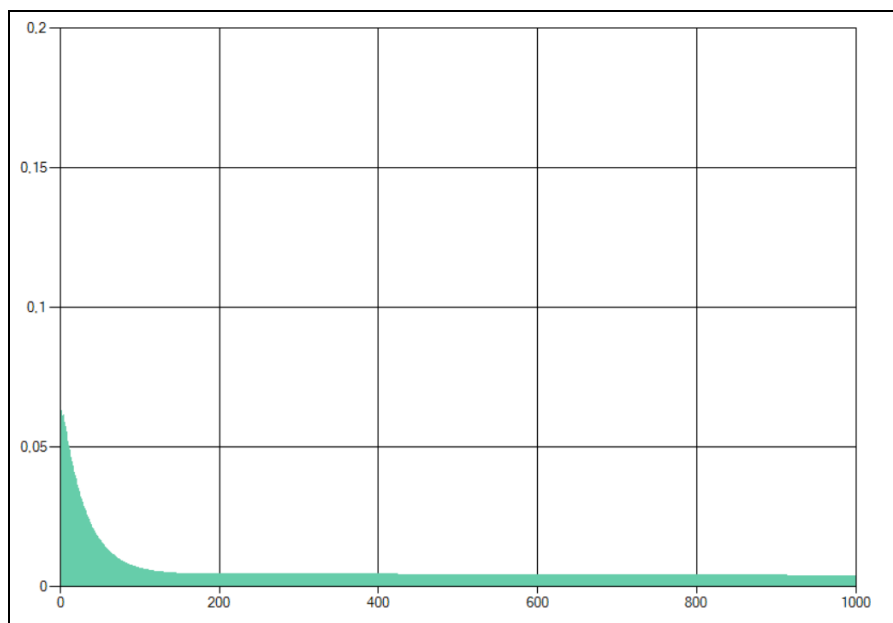


Рисунок 1 – Сходимость алгоритма

Также следует отметить простоту программной реализации описанного неградиентного метода обучения, по сравнению с методом градиентного спуска с обратным распространением ошибки. Неградиентные методы требуют меньше вычислительных ресурсов, что обусловлено применением простейших структур данных и тривиальных математических операций. Среднее количество тактов времени, затраченное на обучение нейронной сети равно трем млн.

ЛИТЕРАТУРА

- 1 Rojas R. Neural Networks. A Systematic Introduction / R.Rojas. – Springer, 1996. – 220 с.
- 2 Хайкин С. Нейронные сети / Саймон Хайкин. – Вильямс, 2006. – 1104 с.

УДК 003.26+004.056

В. О. Берников, асп.;

П. П. Урбанович, проф., д-р техн. наук (БГТУ, г. Минск)

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ СТЕГАНОГРАФИЧЕСКОЙ СТОЙКОСТИ МНОГОКЛЮЧЕВОЙ СИСТЕМЫ

Под стеганографической стойкостью информационных систем понимается уровень их защищенности перед попытками несанкционированного извлечения, разрушения, искажения или удаления осажден-

ных в стеганоконтейнеры сообщений, а также обеспечение целостности осажденных сообщений при случайной или преднамеренной модификации самого стеганоконтейнера [1]. В докладе рассматриваются существующие подходы в математическом моделировании различных типов стеганосистем, основной целью которого является оценка стеганостойкости.

Особенностью анализируемых систем является использование достаточно большого числа ключей, используемых как для осаждения/извлечения сообщений, так и для предварительного преобразования осаждаемой в контейнер информации, а также соответствующего преобразования этой информации после ее извлечения. Такие стеганосистемы мы классифицируем как многоключевые [2-3].

В основе многих моделей лежит известная схема взаимодействия субъектов (Алиса, Боб и др.) криптографической системы, предложенная Р. Ривестом. Однако многоключевая стеганосистема характеризуется рядом особенностей. Основными из таких особенностей являются следующие. Во-первых, стеганосистема интегрирует в себе, по существу, ряд систем (по числу ключей), каждая из которых может ассоциироваться с криптосистемой. Во-вторых, устойчивость стеганосистемы (в особенности при использовании текстовых документов-контейнеров [4]) следует рассматривать не только в привязке к атакам на основе аппаратно-программных средств и анализа соответствующих математических выражений, но также и на основе визуального анализа стеганоконтейнера [2-3].

В докладе рассмотрена общая классификация атак нарушителя на стеганосистемы с учетом отмеченных здесь особенностей.

Так называемый теоретико-информационный подход моделирования используется для обнаружения факта существования скрытой передачи информации на основе вычисления относительной энтропии сообщения-содержимого контейнера. Данный подход использует идеальную модель Керкгоффа, которая предполагает, что атакующая сторона (нарушитель) знает полное описание стеганосистемы, ему известны вероятностные характеристики скрываемых сообщений, ключей, формируемых стеганоконтейнеров. Для достижения высокого уровня стойкости стеганосистем необходимо, чтобы энтропия ключа была больше или равна энтропии сообщения, в противном случае, мы имеем дело с незащищенной системой.

Существует теоретико-сложностный подход, который использует дополнительное криптопреобразование стегосообщения (один из ключей многоключевой системы). Данный подход сводится к трудной в вычислительном смысле задаче при использовании односторонних

функций. В зависимости от выбранного алгоритма шифрования можно оценивать стойкость стеганографических систем. Теоретические подходы в целом можно использовать для оценки стойкости многоключевой стеганографической системы, однако имеются существенные недостатки использования данных подходов.

Очевидно, что использование идеальной модели криптосистемы Керкгоффса не вполне адекватно реалиям информационно-скрывающих систем. Если передаваемые избыточные сообщения сжимаются с частичной потерей данных, или канал связи может вносить помехи в передаваемые информационные потоки, то данные подходы не будут иметь смысла, так как будет иметь место отклонение статистики наблюдаемого нарушителем в канале связи сообщения от среднестатистических характеристик пустых контейнеров и будет выявлен факт наличия стеганоканала.

ЛИТЕРАТУРА

1 Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ./ П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2 Urbanovich, P. Theoretical Model of a Multi-Key Steganography System / P. Urbanovich, N. Shutko // Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science. Vol. 2, Chapter 11. – Lublin : KUL, 2016. – P. 181-202.

3 Urbanovich, P. A formal description of a multi-key steganographic systems / P. Urbanovich, N. Shutko, A. Zapala// 10th Intern. Conf. NEET'2017, Zakopane, Poland, June 27 – 30, 2017. – P. 47.

4 Берников, В.О. Анализ стеганографической стойкости текстового документа-контейнера в многоключевой стеганосистеме// 69-я НТК студентов и магистрантов: сб. науч. работ: в 4-х ч., 17-22 апреля 2018 г. – Минск: БГТУ, 2018. – Ч. 4. – С.14-17.

УДК 003.26

Е. А. Блинова, ст. преп. (БГТУ, г. Минск)

АЛГОРИТМИЧЕСКИЕ ОСОБЕННОСТИ И ОЦЕНКА ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ В ЭЛЕКТРОННЫХ КАРТАХ

Электронные карты – это набор компьютерных файлов, содержащих пространственные данные в векторном формате. Электронные

карты широко используются в приложениях для управления инфраструктурой населенных пунктов, навигации и чрезвычайных ситуаций. Изготовление электронных карт требует значительных затрат, и картографическая информация должна быть предоставлена конечному пользователю с учетом защиты как от неправомерного использования, так и от умышленного искажения данных. Поскольку электронные карты могут только ограниченно использовать криптографические методы защиты на уровне файла или GIS-системы, наиболее оптимальным представляется использование стеганографических методов.

В литературе широко освещается возможность осаждения скрытой информации в файлы электронных карт. В период с 2000 по 2018 годы выросло число публикаций, посвященных проблеме осаждения скрытых данных в файлы электронных карт, в то время как ранее основной интерес сосредотачивался на растровых картах, которые представляют собой изображение. Основные подходы к осаждению скрытых меток в электронные карты приведены в таблице 1.

Таблица 1 – Основные подходы к осаждению скрытых меток в электронных картах

Наименование	Описание
Нулевые водяные знаки	Использование ключевых характеристик контейнера при генерации водяного знака
Адаптивные водяные знаки	Размещение водяного знака в определенной области в зависимости от характеристик контейнера
Множественные водяные знаки	Наличие нескольких разноплановых водяных знаков
Обратимые водяные знаки	Возможность получить оригинальный контейнер после извлечения водяного знака
Аддитивные водяные знаки	Добавление водяного знака в координаты вершин полиномов пространственных объектов

При осаждении скрытых меток (водяного знака) все стеганографические методы могут быть разделены на две основные группы: изменение характеристик отдельных вершин пространственных объектов и трансформация пространственного объекта в целом. При изменении характеристик отдельных вершин пространственных объектов встраивание может производиться путем изменения младших цифр координат вершин пространственных объектов, изменением топологии, т.е. объединением или разделением пространственных объектов, а также делением электронной карты на взаимосвязанные части. Достоинствами таких методов являются простая программная реализация и объем размещаемого водяного знака, а основным недостатком — низкая стойкость к атаке на конкретный метод. К методам трансформации про-

странственного объекта в целом относятся методы, использующие вейвлет-преобразование, дискретное преобразование Фурье и дискретное косинусное преобразование. Такие методы обеспечивают высокую стойкость к атакам, основанным на пространственных преобразованиях, таких как поворот или масштабирование, однако они подходят не для всех типов электронных карт и сложно реализуются.

ЛИТЕРАТУРА

1 Блинова Е.А., Смелов В.В. Применение стеганографических методов при хранении картографической информации в экспертной системе прогнозирования последствий разлива нефтепродуктов// Сахаровские чтения 2017 года: Экологические проблемы XXI века, материалы 17-й МНК, 18-19 мая 2017. Международный государственный экологический институт им. Д. А. Сахарова Белорусского государственного университета. Минск. 2017. С. 223–224.

2 Блинова Е.А., Урбанович П.П. Защита целостности данных электронных карт стеганографическим методом// Тезисы 4-ой Международной научно-практической конференции «Веб-программирование и интернет-технологии WebConf2018», 14-18 мая 2018. БГУ. Минск. 2018. С. 147.

3 Блинова Е.А., Урбанович П.П. Стеганографический метод на основе встраивания дополнительных значений координат в изображения формата SVG // Труды БГТУ. Сер.3, Физ.-мат. Науки и информатика, № 1(206). Минск, БГТУ. 2018. С. 104-109.

4 Блинова Е.А., Голик А.А. Модификация стеганографического метода на основе встраивания дополнительных значений координат в изображения формата SVG // Развитие информатизации и государственной системы научно-технической информации (РИНТИ-2018): доклады XVII Международной конференции, Минск, 20 сентября 2018 г. Минск: ОИПИ НАН Беларуси, 2018. С. 130-133.

5 Blinova E., Shutko N. The use of steganographic methods in SVG format graphic files // New Electrical and Electronic Technologies and their Industrial Implementation; proc. of the 10-th Intern. Conf., Zakopane, Poland, 23–26.06.2017. / Lublin University of Technology; Media Patronage “Przegląd Elektrotechniczny”. Lublin. 2017. P .45.

СИСТЕМА ТЕСТИРОВАНИЯ ЗНАНИЙ НА ЕСТЕСТВЕННОМ ЯЗЫКЕ НА ОСНОВЕ СЕМАНТИЧЕСКОЙ СЕТИ ОБУЧАЮЩЕЙ СИСТЕМЫ

Целью исследования является разработка системы тестирования знаний на основе семантической сети обучающей системы [1]. Система тестирования знаний нужна для автоматизации контроля знаний. В процессе контроля приобретенных знаний система будет задавать вопросы тестируемому с последующей сверкой ответов в соответствующей базе знаний и оценивать правильность ответов. В настоящее время существует множество автоматизированных тестов, но большинство из них сводится к анализу ответов «да/нет» или «выберите из списка предложенных вариантов». Данная же система должна анализировать письменный или устный ответ на вопрос без предложения вариантов ответа. Такое тестирование также может помочь и в самостоятельном освоении материала.

Семантическая сеть – это информационная модель предметной области, имеющая вид ориентированного графа, вершины которого соответствуют объектам предметной области, а дуги (рёбра) задают отношения между ними.

Для хранения семантической сети в цифровом виде используется список дуг в базе данных. Дуга же содержит в себе 2 вершины и связь между ними. Также в дополнительной таблице можно хранить информацию об окончаниях, шаблонах и другой информации о семантической сети [2, 3].

Разработанная система тестирования имеет клиент-серверную архитектуру и предоставляет возможность выбирать одну или несколько тем по учебному материалу для тестирования обучаемого. Система может оценивать ответ тестируемого как правильный, частично правильный или неправильный, начисляя определенное количество баллов, при этом оцениваются и ответы, приведенные в виде развернутых предложений.

Алгоритм функционирования системы тестирования следующий:

- 1) на сервере задаются параметры: тема или темы для тестирования (список представленных к выбору тем загружается динамически из базы данных);
- 2) создается тест с заданными на сервере параметрами;

3) при создании теста запрашивается создание локальной базы знаний.

4) по исходным параметрам выбирается из базы данных определенное количество записей на заданную тему;

5) по полученным из базы данных записям формируется список вопросов (без ответов) и отправляется клиенту;

6) происходит процесс тестирования клиента в виде последовательного вывода вопросов, на которые тестируемый записывает ответы в текстовом виде;

7) по завершению тестирования, ответы тестируемого отправляются на проверку на сервер;

8) генерируются проверочные строки из базы данных для последующего их сравнения с ответами тестируемого;

9) происходит сверка ответов клиента и проверочных строк, сгенерированных из базы данных, с выставлением оценок к каждому отдельному ответу;

10) на сервере и клиентах выводится результат прохождения теста.

Проанализировав содержание базы знаний обучающей системы, можно выделить несколько типов вопросов:

1 простые вопросы, когда требуется только один ответ, и только один является приемлемым;

2 вопросы с несколькими вариантами правильных ответов, когда за каждый из правильных ответов насчитываются баллы, т.е. может быть засчитан частично правильный ответ;

3 вопросы с несколькими равнозначными правильными ответами, что предполагает несколько правильных ответов-синонимов, но их не нужно перечислять. Например, «обычный» и «естественный» каждый из этих ответов правильный, но не нужно перечислять каждый из них для того, чтобы правильно ответить на вопрос;

4 комбинации перечисленных типов вопросов.

Проверка каждого ответа на вопрос происходит следующим образом: сначала на сервере, присланным ответам сопоставляются сверочные строки. Каждое слово, хранящееся в сверочной строке, ищется в качестве подстроки в ответе клиента, за каждое совпадение с подстрокой начисляется 1 балл. Итоговое количество баллов за ответ выставляется в зависимости от типа вопроса. В первом типе ответ будет засчитан только если были найдены все строки из сверочной строки, во втором типе, может быть засчитан частично правильный ответ, при проверке третьего типа выставляется отдельная оценка по каждой вы-

деленной части ответа и в итоге идет наибольшая оценка, полученная за фрагмент.

Представленная структура и функционал разработанной системы тестирования позволяют проводить проверку ответов в виде развернутых предложений. Однако следует отметить, что база данных системы тестирования на данном этапе разработки может формироваться лишь экспертом и с использованием шаблона, при котором вопрос задается к ключевому понятию, или предложению с конкретными словами, по корням которых можно проверить правильность ответа тестируемого.

ЛИТЕРАТУРА

1. Гурин Н. И., Герман О.В. Компьютерные обучающие системы в издательском деле Ч. 2 //БГТУ, 2015. 192 с.

2. Гурин Н. И., Герман О. В. Интеллектуальный анализатор запросов к базе знаний мультимедийного электронного учебника // Труды БГТУ. 2010. №6: Физ.-мат. науки и информатика. С. 167–170.

3. Гурин Н. И., Жук Я. А. Генератор семантической сети информационной системы в таблицу реляционной базы данных // Труды БГТУ. 2015. № 6: Физ.-мат. науки и информатика. С. 181–185.

УДК 003.26

Я. А. Жук, асп. (БГТУ, г. Минск)

ОЦЕНКА ЭФФЕКТИВНОСТИ РАБОТЫ ГЕНЕРАТОРА СЕМАНТИЧЕСКОЙ СЕТИ ДИАЛОГОВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

При анализе генератором семантической сети (ГСС) содержания информационных систем были выявлены различные лингвистические, графические и мультимедийные элементы. Для корректной обработки данных элементов и расчета их важности потребовалось провести оценку эффективности работы ГСС с выявлением и подсчетом ситуаций, требующих дополнительной отладки. Оценка эффективности работы ГСС предлагается производить путем сравнения предложений из содержания электронного учебника с результатами анализа данных предложений с помощью ГСС. Как и в других методах оценки эффективности программ обработки естественного языка, сравнение выполняется экспертом. В качестве информационных систем для анализа с помощью ГСС выбраны отдельные параграфы электронных учебников по дисциплинам «Электрохимия» и «Микробиология», представленные в HTML-формате. Эффективность работы ГСС Э предлагается рассчитывать по формуле:

$$\Theta = \frac{C_K + B_K}{C_O + B_O},$$

где C_K – количество корректно выявленных с помощью ГСС семантических связей; B_K – количество корректно выявленных с помощью ГСС вспомогательных предложений; C_O – общее количество семантических связей, выявленных экспертом; B_O – общее количество выявленных экспертом вспомогательных предложений.

Эффективность работы ГСС составила 55% при анализе параграфа электронного учебника по электрохимии и 64% при анализе параграфа электронного учебника по микробиологии. Кроме того, было выявлено 5 типов ошибок, связанных с восполнением недостающих членов предложения, отсылками к предыдущим предложениям, обработкой списков, выявлением границ предложений, и предложениями необычной структуры, что позволяет сконцентрировать усилия по совершенствованию ГСС на конкретных задачах.

УДК 004.056

А. А. Сущенья, магистрант;

П. П. Урбанович, проф., д-р техн. наук (БГТУ, г. Минск)

ПРИМЕНЕНИЕ ФОРМАТОВ ЭЛЕКТРОННЫХ КНИГ ПРИ ПЕРЕДАЧЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ МЕТОДАМИ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Актуальность исследований в области стеганографии обусловлена, в том числе, остротой проблемы защиты конфиденциальных данных от несанкционированного использования. Ввиду этого существует необходимость расширения и углубления теоретической базы стеганографии как платформы для тайной передачи и хранения информации [1].

С развитием информационных технологий стали появляться цифровые объекты, имеющие в своей структуре избыточность, которую можно использовать для реализации стеганографических методов. Одними из таких объектов являются электронные книги (ЭК). На сегодняшний день наиболее популярными форматами ЭК являются: FB2, EPUB, MOBI, KF8, DJVU, RTF. Однако для реализации стеганографических преобразований наиболее целесообразным форматом из перечисленных является EPUB. Рассмотрим структуру данного формата. EPUB – это ZIP-файл, сжатый особым образом. В этом можно убедиться изменив расширение файла .epub на .zip и разархивировав его любым архиватором.

Минимальный набор файлов, который входит в EPUB должен быть следующим:

- файл *mimetype*, сострочкой «application/epub+zip»;
- папка META-INF с файлом *container.xml*, который указывает, где хранится содержимое книги;

- папка OPS, в которой должны быть:

- ✓ файл с метаданными книги; списком всех файлов, которые нужны для ее содержимого; описанием последовательности чтения файлов и путеводителем по ключевым файлам;

- ✓ файл *toc.ncx*, содержащий оглавление ЭК в том виде, в котором оно будет прочитано программой для чтения; файл *stylesheet.css* с описанием стилей оформления текста;

- ✓ файлы содержимого в формате XHTML; папки с иллюстрациями и шрифтами.

Исходя из того, что объект формата EPUB содержит XHTML-файлы, становится возможным использовать такие способы внедрения информации в электронную книгу, как, например, метод пробелов, метод кавычек, метод изменения порядка следования атрибутов [2-4].

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ./ П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2. Сушня, А. А. Стеганографическое преобразование текстов-контейнеров на основе языков разметки / А. А. Сушня // 68-я научно-техническая конференция учащихся, студентов и магистрантов, 17-22 апреля, Минск : сборник научных работ : в 4 ч. Ч. 4 / Белорусский государственный технологический университет. – Минск : БГТУ, 2017. – С. 145-149.

3. Сушня, А.А. Идея и архитектура веб-приложения, использующего в качестве стеганографического контейнера документы формата DOCX / А. А. Сушня // Международная научно-практическая конференция, 14–18 мая, Минск: сборник научных работ, Белорусский государственный университет. – Минск: БГУ. – С. 170.

4. Сушня, А.А. Модификация стеганографического метода изменения междустрочного расстояния электронного документа/ А.А. Сушня, Е.А. Блинова, П.П. Урбанович// Технические средства защиты информации: тезисы докладов XVI Белорусско-российской научно-технической конференции, 5 июня 2018 г., Минск. – Минск: БГУИР, 2018. – С. 90-91.

ЗАЩИТА АВТОРСКИХ ПРАВ НА ТЕКСТОВЫЕ ДОКУМЕНТЫ НА ОСНОВЕ СТЕГАНОГРАФИЧЕСКОЙ МОДИФИКАЦИИ ЦВЕТА СИМВОЛОВ ТЕКСТА

Кроме скрытой передачи сообщений [1], стеганографические методы являются одним из перспективных инструментов для аутентификации и маркировки авторской продукции с целью защиты авторских прав на цифровые объекты от пиратского копирования. Такие специальные сведения могут рассматриваться в качестве доказательств при рассмотрении споров об авторстве или для доказательства нелегального копирования [2].

Актуальной является задача разработки новых методов, повышающих устойчивость к атакам, т. е. снижающим вероятность извлечения сообщения из контейнера. Один из новых методов для скрытия секретного сообщения в текстовом документе основывается на следующем положении. Цвет символа в текстовом процессоре Microsoft Word представлен в цветовой модели RGB. Незначительное изменение цвета символа не воспринимается человеческим глазом. Используя данную физиологическую особенность, можно незаметно производить встраивание информации.

При реализации известного метода LSB [1] встраивание производится в последние 1–2 бита цвета пикселя изображения. Адаптация алгоритма к тексту позволяет производить встраивание в последние 3–5 бит цвета символа. Увеличение числа используемых бит цвета в тексте, по сравнению с графикой, происходит из-за того, что изображение, как правило, содержит градации и переходы от одного цвета к другому. Текст монотонен и выполняется в большинстве случаев одним цветом, поэтому становится возможным увеличение используемого для встраивания цветового диапазона [3].

При скрытии данных в документе, который предназначен для последующей печати, в качестве изменяемых символов не могут использоваться невидимые знаки (пробелы, табуляции, переводы строк и т. д.), поэтому в этом случае производится дополнительная проверка. Выбор символов для хранения скрытой информации происходит случайным образом. В ходе экспериментов установлено, что модификация до 4-х младших символов цветовой координата каждого канала (RGB) в 100% случаев остается незамеченной поль-

зователем, которому не известен факт осаждения в документе невидимой информации.

Специально для реализации на практике данного метода было создано программное средство (*Sword*), диаграмма деятельности которого показана на рисунке 1.

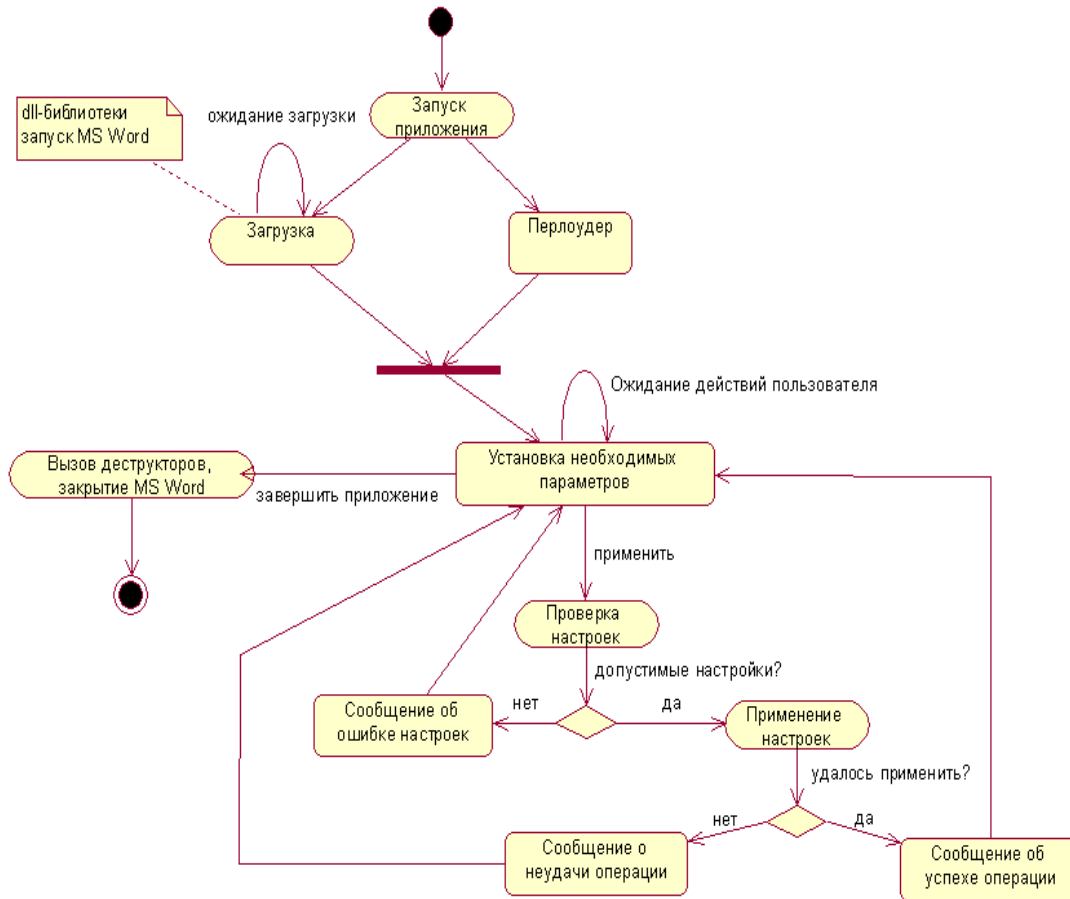


Рисунок 1 – Диаграмма деятельности программного средства *SWord*

Обязательными требованиями для работы программного средства являются наличие на компьютере пользователя Framework 2.0 или выше, а также MS Office Word 2003 или выше. Данным требованиям соответствует большинство компьютеров, работающих на операционных системах Windows. Программное средство реализовано с помощью языка программирования C# в среде разработки Visual Studio 2008 Express, для взаимодействия с объектами MS Office Word используется dll-библиотека Microsoft.Office.Interop.Word.

Установка необходимых параметров в программе осуществляется с помощью трех блоков, в которых задается: стегосообщение (в случае извлечения заполнять не надо), контейнер и настройки, на основе которых происходит скрывание/извлечение сообщения (ключ).

Цвет символа, в котором будет производиться скрывание, форми-

руется исходя из цвета символа-образца и заданного в настройках смещения. По умолчанию это смещение добавляется к основному цвету.

После встраивания необходимой информации есть возможность просмотреть измененный документ нажатием кнопки «Показать». При использовании кнопки «Отметить» синим маркером будут выделены символы и пробелы, в которые проводилось встраивание необходимой информации (рис. 2).

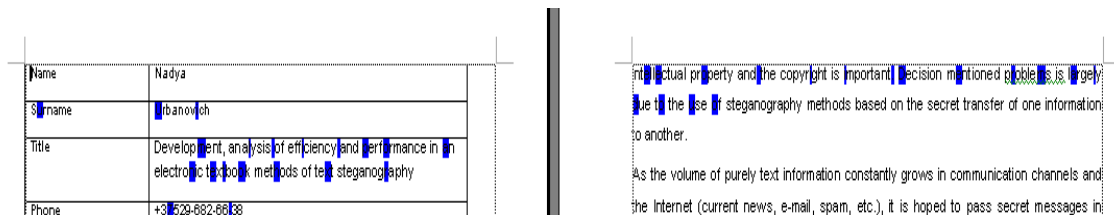


Рисунок 2 – Фрагмент стеганоконтейнера со встроенным сообщением

При скрытии данных в документе, который предназначен для последующей печати, в качестве изменяемых символов не могут использоваться невидимые знаки (пробелы, табуляции, переводы строк и т. д.). В ходе экспериментов установлено, что модификация до 4-х младших символов цветовой координата каждого канала (RGB) в 100% случаев остается незамеченной пользователем, которому не известен факт осаждения в документе невидимой информации.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации / П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.
2. Шутько, Н.П. Моделирование стеганографической системы в задачах по охране авторских прав/ Н.П. Шутько, Н.И. Листопад, П.П. Урбанович// Восьмая МНТК «Информационные технологии в промышленности» (ITI'2015) : тезисы докладов (2–3 апреля 2015 года, Минск). – Минск: ОИПИ НАН Беларуси, 2015. – С. 30-31.
3. Шутько, Н. П. Математическая модель системы текстовой стенографии на основе модификации пространственных и цветовых параметров символов текста / Н. П. Шутько, Д. М. Романено, П. П. Урбанович // Труды БГТУ. – Минск : БГТУ, 2015. – № 6 (179). – С. 152-156.

SEMANTIC ROUTING SCHEME FOR INFORMATION-CENTRIC NETWORKING

Most of the routing schemes (in DONA/CBCB / PURSUIT/....) are based on publisher/subscriber interaction. It use filters to match rendezvous points between subscriber interests and publisher advertisement compared to the conventional IP.

Due to the high mobility of terminals in nowadays networks, publisher and subscriber should hold a *Dynamic Address* that may be changed according to their place in the network.

To serve Subscribers requesting Information with *Any Data Content* from *Any Publisher*, name should represent the content. Additionally, to serve requesting *Specific Data Content* from *Any Publisher* name should be unique.

Our proposed naming scheme is based on three dimensions knowing that the user (publisher/subscriber) should label the data with least one dimension. The three dimensions are:

1. Geographical address ex. Ipv6: its importance is in simplify routing and it is dynamic that is based on the location of the publisher/subscriber in the network and this address helps in mobility
2. User (publisher/subscriber) ID address is related to the terminal as MAC address (media access control address).
3. Semantic address: it is set of keywords that define the data.

Semantic resolution server (broker) will translate the set of keywords to a hierarchal address based on a predefined semantic tree that is known at all routers.

The figure below is extracted from the ICN architecture and shows the naming scheme.

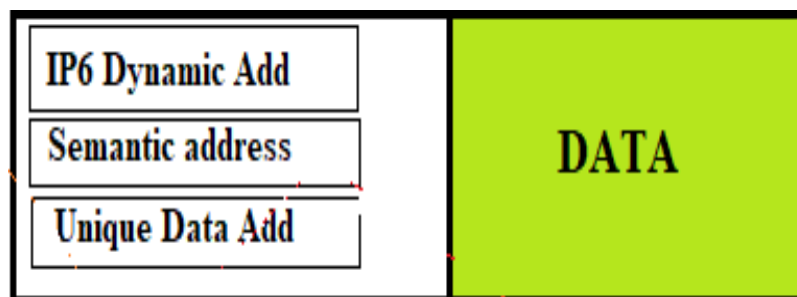


Figure. SICN naming scheme

РЕЙТИНГОВЫЕ ПОКАЗАТЕЛИ ПОДГОТОВКИ СТУДЕНТОВ И СИСТЕМА ОЦЕНКИ КОМПЕТЕНТНОСТИ СПЕЦИАЛИСТОВ

Информационные технологии могут быть использованы при обучении студентов несколькими способами. В самом простом случае реальный учебный процесс идет по обычным технологиям, а информационные технологии применяются лишь для промежуточного контроля знаний студентов в виде тестирования. Во втором варианте осуществляется постоянный контроль прохождения учебно-тематического плана каждым студентом индивидуально. Для достижения этой цели прибегают к использованию рейтинговых систем обучения.

На кафедре программной инженерии УО Белорусский государственный технологический университет развивается проект «Интегрированная информационная система управления учебным процессом». В рамках проекта разработаны модели, архитектура и построены подсистемы.

В подсистеме программное обеспечение и данные реализованы в виде блоков (объектов). Каждый из блоков представляет собой информационную подсистему второго уровня (0-й уровень – корпоративная/серверная часть; 1-й уровень - локальные подсистемы. Создаются обычно с учетом функционального признака; 2-й уровень – подсистема (блок, объект), реализующая конкретную функцию, связанную с обслуживанием учебного процесса).

В работающем приложении реализованы только три показателя, но для любителей использовать большее количество критериев оценки деятельности студента программных ограничений нет.

Рейтинговая технология обучения обладает рядом преимуществ по сравнению с другими технологиями и традиционными формами организации учебного процесса и главное - может быть легко адаптирована для оценки компетенций при подготовке специалистов управления.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СХЕМ ИМЕНОВАНИЯ В ICN

При проектировании архитектуры ICN одной из основных задач является именованье информационных объектов и сервисов. Структура имен и их семантика оказывают существенное влияние на другие аспекты архитектуры. Одними из основных вариантов именованья являются иерархические и flat имена. Иерархические имена – это имена с явной структурой, где каждая часть имеет определенное значение. Flat или неструктурированные имена – это неструктурированная уникальная строка, обычно, фиксированного размера. Примером flat имен может быть GUID, например, d744a113-6275-457f-ae6d-eacbc7abd997. Важной особенностью иерархических имен является то, что они легко воспринимаются человеком, в то время как flat имена хорошо распознаются машинами.

Первой архитектурой, в которой использовались flat имена был проект DONA. В DONA каждый информационный объект или сервис связан с владельцем. Имя объекта формируется из криптографического хэша публичного ключа владельца P и его уникального названия L. Имена при этом получаются - неструктурированные, независимые от приложения, независимые от местоположения и глобально уникальные.

Архитектура PURSUIT также использует flat имена. Информационные объекты в PURSUIT определяются уникальной парой идентификаторов – идентификатором области и идентификатором рандеву. Иерархические имена получили широкое распространение в сетях CCN/NDN.

В архитектуре SAIL имена информационных объектов одновременно являются неструктурированными и иерархическими. SAIL определяет схему URI имен как ni://A/L, в которой имена состоят из авторитетной части A и локальной части L. Каждая часть может быть хешем, что позволит проводить самосертификацию, или любой другим видом строки, что позволит использовать их как обычные URL.

Интересное решение используется в MobilityFirst. Каждому сетевому объекту назначается глобальный уникальный идентификатор (GUID) через глобальную службу имен, которая переводит понятные человеку имена в GUID.

Н. В. Пацей, доц., канд. техн. наук;
Д.М. Романенко, доц., канд. техн. наук; А. В. Мартынюк
(БГТУ, г. Минск)

ПРОИЗВОДИТЕЛЬНОСТЬ КАСКАДНОГО КОДЕКА ДЛЯ ИСПРАВЛЕНИЯ МНОГОКРАТНЫХ МОДУЛЬНЫХ ОШИБОК В БЕСПРОВОДНЫХ КАНАЛАХ СВЯЗИ

В результате проведения исследований выполнена модификация программной модели каскадной схемы помехоустойчивого кодека. Добавлено сохранение параметров составных кодов и экспериментальных данных, полученных в ходе моделирования работы в базу данных PostgreSQL. Разработана модель базы данных. Добавлен режим командной строки для выполнения автоматизированного тестирования. Выполнено моделирование для различных комбинаций составных кодов с перемежителями и без, для разных длин пакетов, скорости кода, уровня шума в канале, типов ошибок (единичные, модульные и их комбинации).

Установлено что для исправления модульных и единичных ошибок в беспроводных каналах связи эффективно использование каскада из двух сверточных кодов, что снижает BER на два порядка или каскада с первым - циклическим, а вторым - сверточным составным кодом, что подымает результирующую скорость каскадного кода на 0,2-0,4.

Определены оптимальные длины кодового слова для циклических кодов ($n = 129 \div 189$);

Установлен процент средней избыточности для фонтанных LT-кодов, исправляющих 20% стираний в канале. Он составил в среднем от 20 до 60 % Однако, практическое использование LT-кода в составе каскадных схем затруднено.

В ходе экспериментального моделирования проанализирована зависимость вероятности битовых и модульных ошибок от различных значений сигнал/шум (от 1 до 10 и от 1 до 35), подобраны оптимальные параметры и комбинации составных кодов.

Разработаны рекомендации по практическому использованию модели адаптивного каскадного кодирования/декодирования избыточных кодов.

АЛГОРИТМ МНОГОУРОВНЕВОЙ КЛАССИФИКАЦИИ ОБЪЕКТОВ, ОСНОВАННЫЙ НА КОДАХ КОРРЕКЦИИ ОШИБОК

В последнее десятилетие широкое распространение получила область, связанная с машинным обучением, в частности для решения задач классификации.

При накоплении (или непрерывном поступлении) большого числа информации часто требуется выполнить автоматизированную классификацию, как категоризацию объектов в один из predetermined классов. Фактически классификация, как одна из задач машинного обучения, отличается тем, что множество допустимых ответов конечно.

В области интеллектуальной бинарной классификации было предложено много хороших методов. Используемые до недавнего времени алгоритмы обычно основывались на стандартных подходах различной сложности: метрические классификаторы, методы ближайших соседей (KNN), байесовские классификаторы, нелинейный метод опорных векторов (SVM). Однако, многие реальные проблемы требуют многоклассовых решений. Поэтому любой из перечисленных методов может быть обобщен на многоклассовый случай. Такое обобщение является сложной задачей. Здесь важно сочетание трех параметров: точности классификации, устойчивости к переобучению и вычислительной эффективности.

Огромное увеличение количества доступных объектов (данных) привели к появлению новых алгоритмов автоматической классификации. Например, был предложен метод построения алгоритмов обучаемой классификации, основанный на теории помехоустойчивого кодирования или самокорректирующихся кодов ЕСОС (Error Correcting Output Coding). ЕСОС является средством объединения любого количества бинарных классификаторов в модель с несколькими классами. Несмотря на это, по-прежнему существует множество открытых вопросов о возможностях ЕСОС.

МНОГОКРИТЕРИАЛЬНАЯ ФИЛЬТРАЦИЯ ЭЛЕКТРОННОЙ КОРРЕСПОНДЕНЦИИ

Наиболее популярным и эффективным подходом для фильтрации электронной корреспонденции на данный момент является использование машинного обучения с учителем с различными признаками, основанными как на содержании сообщений, так и на свойствах отдельных профилей пользователей.

Машинное обучение (machine learning) – это область научного знания, имеющая дело с алгоритмами, «способными обучаться». Необходимость использования методов машинного обучения объясняется тем, что для многих сложных – «интеллектуальных» – задач (например, распознавание рукописного текста, речи и т. п.) очень сложно (или даже невозможно) разработать «явный» алгоритм их решения, однако часто можно научить компьютер обучиться решению этих задач. Одним из первых, кто использовал термин «машинное обучение», был изобретатель первой самообучающейся компьютерной программы игры в шашки А. Л. Самуэль в 1959 г. Под обучением он понимал процесс, в результате которого компьютер способен показать поведение, которое в нее не было заложено «явно». Это определение не выдерживает критики, так как не понятно, что означает наречие «явно». Более точное определение дал намного позже Т. М. Митчелл: говорят, что компьютерная программа обучается на основе опыта E по отношению к некоторому классу задач T и меры качества P , если качество решения задач из T , измеренное на основе P , улучшается с приобретением опыта E .

На этапе классификации и оценки были протестированы 5 алгоритмов: наивный байесовский классификатор (NaiveBayes classifier), метод k ближайших соседей (k -nearest neighbors algorithm, k -NN)), метод опорных векторов (SVM), дерево принятия решений (Decision tree), случайные леса (Random forest).

В результате проведенного исследования данных алгоритмов машинного обучения лучший результат продемонстрировал алгоритм Random Forest - 93%. Наиболее высокий известный результат в данной задаче составляет 98%, однако в нем отсутствуют какие-либо ограничения на историчность признаков.

АЛГОРИТМЫ И ПОДХОДЫ К ОБРАБОТКЕ ПРОФИЛЕЙ СОЦИАЛЬНОЙ СЕТИ ПРИ ПОИСКЕ ПО ФОТОГРАФИИ

На сегодняшний день поиск профилей в социальных сетях по фотографии – один из основных источников информации об окружающих, выполнение таких запросов требует использования эффективных алгоритмов поиска.

Связи между пользователями возникают не случайным образом. Согласно социологической теории шести рукопожатий любые два человека на Земле разделены не более чем пятью уровнями общих знакомых и, соответственно, шестью уровнями связей. Формальная математическая формулировка теории — диаметр графа знакомств не превышает 6. Для практической реализации алгоритма построим граф социальных связей, узлами которого являются социальные объекты, представленные пользовательскими профилями, а рёбра — это социальные связи между ними.

Обход данного графа начинаем от профиля пользователя, выполняющего поиск, пропуская первый уровень его социальных связей (его друзей). Производим распознавание лица на фотографии профиля каждого уровня и сравнение полученного результата с заданным изображением, если совпадение найдено – возвращаем результат и продолжаем поиск, так как могут встречаться «двойники» или близкие родственники, которые могут иметь одинаковые отличительные черты лица, по которым алгоритм распознавания лиц определит их совпадение.

Применение описанного алгоритма обхода профилей пользователей социальной сети позволит в сотни раз сократить время поиска профиля пользователя, который находится в том же городе (стране) или имеет общий круг социальных интересов с инициатором поискового запроса.

ЛИТЕРАТУРА

1. Claude Berge The Theory of Graphs (Dover Books on Mathematics) - New York, Dover Publications, September 4, 2001, 272p
2. Социальные сети и виртуальные сетевые сообщества / отв. ред. Верченков Л.Н., Тищенко В.И. М: ИНИОН РАН, 2013.360 с.

АЛГОРИТМ РАЗРЕШЕНИЯ КОНСЕНСУСА В BLOKCHAIN, ОСНОВАННЫЙ НА МАШИННОМ ОБУЧЕНИИ

Blockchain позиционируется как технология, которая должна изменить устоявшиеся подходы к построению различных информационных систем, не зависимо от их сферы. Существующие алгоритмы разрешения консенсуса весьма хорошо справляются с задачами, которые перед ними поставлены. Самый распространённый Proof-of-work добивается этого путём огромных вычислений, которые в дальнейшем нигде не могут быть применимы. Согласно bitcoinwatch, мощность сети Bitcoin, работающая на Proof-of-work, составляет 271 PFLOPS (10^{15}), что превышает показатель самого мощного суперкомпьютера Titan в 15 раз.

Машинное обучение, которое представляет из себя класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение в процессе применения решений множества сходных задач. Использование позволит помимо эффективного решения поставленной задачи ещё и получить, например, искусственную нейронную сеть (НС). В данном случае идея о регулировании третьим независимым лицом сохраняется, но в этом случае экземпляры НС нужно расположить на каждом узле, и постоянно обучать, на основе уже принятых данных, для сохранения децентрализации.

В рамках подготовки к конференции ППС была разработана и обучена упрощенная нейронная сеть на основе открытых данных и требований необходимых для корректного функционирования данное НС в блокчейне. Результатом стало весьма быстрое удостоверение в корректности транзакции (около 0.08 мс на одну транзакцию), однако существует ряд проблем, которые необходимо решить, чтобы внедрить данную НС в действующий Блокчейн.

Н.А. Жилияк, доц., канд. техн. наук;
Д.В. Шиман, доц., канд. техн. наук; А.С. Наркевич, ст. преп.
(БГТУ, г. Минск)

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ МЕТОДОЛОГИИ СИНТЕЗА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

Большинство известных подходов к проектированию сложных технических объектов, в том числе, радиолокационных систем и комплексов, также их средств встраиваемой вычислительной техники, предполагает создание множества альтернативных вариантов системы с последующим их анализом с целью выбора оптимального (оптимальных) по заданным критериям качества. В рамках теории синтеза вычислительных систем реального времени (ТСВСРВ) множество альтернативных вариантов определяется множеством векторов назначения для графа вычислительного алгоритма (ГВА) реализации заданной математической модели и, соответственно, модели вычислительного процесса, подлежащего реализации проектируемой вычислительной системы (ВС) [1].

Предлагаемая методология синтеза, основанная на базе математических моделей с заданными характеристиками, используется при синтезе специализированных вычислительных устройств для формирования отраженных сигналов. Синтезированные устройства, по сравнению с устройствами, синтезированными на основе базовой математической модели известными методами синтеза [2], обладают следующими свойствами: простота, низкие себестоимость, энергопотребление, вес, габариты, высокая надежность, технологичность, обусловленная возможностью реализации всех структурных составляющих средствами цифровой вычислительной техники.

ЛИТЕРАТУРА

1. Жилияк Н.А. Базовый алгоритм синтеза вычислительных систем реального времени Н.А. Жилияк, А.С. Кобайло // Труды БГТУ. Сер. VI, Физ.-мат. науки и информатика. – 2007. – Вып. XV. – С. 147–150.
2. Кобайло, А.С. Новые положения теории синтеза вычислительных систем реального времени в учебных курсах ВУЗов / А.С. Кобайло // Высшее техническое образование: проблемы и пути развития. Материалы VI Международной практической конференции. Минск: БГУИР, 2012. – С.222–223.

ТРЕХУРОВНЕВАЯ ТОКЕНИЗАЦИЯ ДЛЯ АВТОМАТИЧЕСКОГО РЕФЕРИРОВАНИЯ ТЕКСТА

Автоматическое реферирование – это составление коротких изложений материалов, дайджестов, т.е. извлечение наиболее важных сведений из одного или нескольких документов и генерация на их основе лаконичных отчетов.

В основе алгоритма лежит метод TF-IDF (от англ. TF — term frequency, IDF — inverse document frequency) – статистическая мера, используемая для оценки важности слова в контексте документа, являющегося частью коллекции документов или корпуса.

Перед применением каких-либо методов реферирования необходимо использовать предварительную обработку текста: удаление стоп-слов, исправление грамматических ошибок.

Под трехуровневой токенизацией подразумевается, что токеном будет являться не только какое-то отдельное слово, но и предложение и абзац. Токеном первого уровня будет абзац текста, который включает в себя коллекцию токенов второго уровня – отдельные предложения этого абзаца. Токеном третьего уровня является слово. Для каждого слова будет выделена его лемма – неизменная, исходная форма слова, а для нее рассчитана TF-IDF. Где TF – отношение числа вхождений некоторой леммы к общему числу слов документа. Таким образом, оценивается важность леммы в пределах отдельного документа. IDF – это обратная частотность документов. Она измеряет непосредственно важность термина. В моем алгоритме ее можно выразить формулой:

$$IDF = \log(\max(TF)/f),$$

где f – частота вхождения леммы в корпус текста.

После расчёта TF-IDF у каждого слова есть свое числовое значение, выражающее его вес в тексте. Для расчёта веса предложений необходимо сложить значения токенов (слов), которые входят в состав этого предложения и разделить на их количество. Далее ту же операцию необходимо применить и для абзацев: сложить значение весов предложений и разделить на количество этих предложений в абзаце.

Таким образом можно выделить наиболее значимые слова, а на их основе выделить наиболее важные части текста.

УДАЛЕННЫЙ КОНТРОЛЬ В ДИСТАНЦИОННОМ ОБУЧЕНИИ НА ОСНОВЕ МЕТОДОВ ИДЕНТИФИКАЦИИ ЛИЦ

Дистанционное обучение приобретает сегодня массовое распространение. Практически каждый крупный учебный центр предоставляет доступ к своим учебным курсам, что открывает новые возможности для удаленного доступа к знаниям. Известны системы обеспечения организации дистанционного учебного процесса, которые включают и проведение контроля. Однако все еще остро стоит вопрос гарантирования добротности и подтверждения самостоятельности прохождения аттестации. В работе предлагается решение по мониторингу удаленных рабочих мест при прохождении аттестации. В основе решения используется методика идентификации лиц в видеопотоке, который передается с веб-камеры удаленного рабочего места.

Цель настоящей работы состоит в том, чтобы в реальном времени осуществлять контроль и идентификацию пользователя с использованием бытовой видеокамеры, при этом, не требуя больших вычислительных ресурсов, временных затрат, специализированной аппаратуры и обеспечивать анализ в каждый момент времени без задержки и ложных срабатываний.

Программная реализация выполнена на языке программирования Python [1]. Были использованы возможности библиотеки NumPy и открытой библиотеки OpenCV [2, 3].

При выборе метода распознавания лица были учтены такие моменты: положение лица на изображении фронтальное или с незначительным отклонением, в кадре возможно наличие более одного лица, возможна плохое освещение объекта. Сравнительный анализ подробно описан в статье [4]. Для решения был использован метод Виолы-Джонса [5], в котором используется интегральное представление изображения, что позволяет без особых задержек рассчитать суммарную яркость произвольного треугольника на изображении. На вход подается полутоновое изображение и с помощью функции `detectMultiScale()` из библиотеки OpenCV для каждой области изображения рассчитывается признак Хаара. На полученном изображении производится оценка антропометрических точек, что эквивалентно обнаружению характерных черт лица. То есть идентификация изображения лица выполняется на основе выделения его геометрических характеристик.

Путем сопоставления точек и поворота изображения на вычис-

ленный угол выполняется нормализация. Для этого использована стандартная функция библиотеки OpenCV – CropFace(), на вход которой подаются изображение, значения центров глаз, необходимый размер изображения на выходе (например, 100x100 px). Центры глаз находятся по опорным точкам как среднее арифметическое между краями глаз. Использование функции CropFace в нашем случае будет достаточно, поскольку к изображению применяются лишь такие деформации как вращение и масштабирование. На этапе идентификации сравниваются вычисленные признаки неизвестного лица (полученного с камеры), с признаками лиц, которые хранятся в базе данных программы. В качестве метрики выбирается стандартное евклидово расстояние.

Предварительное тестирование показало приемлемые результаты. Сейчас программа находится в стадии опытной эксплуатации, в результате которой планируется подготовить требования к рабочему месту (освещенность, угол обзора камеры и т. п.) и определить допустимый для этих условий уровень погрешности идентификации.

Мониторинг рабочего места с возможностью идентификации лица оператора позволит в реальном времени контролировать ход аттестации. Построенная на базе предложенного решения автоматизированная система проведения удаленного контроля знаний предполагает протоколирование всего процесса. В протоколе могут быть отмечены различные нетипичные ситуации, как например, отсутствие за рабочим местом, присутствие другой личности (подмена) или присутствие дополнительных лиц (несколько человек в кадре). Такой подход дает возможность проводить удаленную аттестацию параллельно для большого числа учащихся.

ЛИТЕРАТУРА

1. Мищенко, Е.С. Сравнительный анализ алгоритмов распознавания лиц [Электронный ресурс]. Режим доступа: http://yrw.jvolsu.com/attachments/article/191/6_Mischenkova.pdf
2. Python Software Foundation. Python 3.7.2 documentation [Электронный ресурс]. Режим доступа: <https://docs.python.org/3/>
3. NumPy developers. NumPy [Электронный ресурс]. Режим доступа: <http://www.numpy.org>
4. OpenCV team. OpenCV [Электронный ресурс]. Режим доступа: <https://opencv.org>
5. The Allen Institute for Artificial Intelligence (AI2). Viola–Jones object detection framework [Электронный ресурс]. Режим доступа: <https://www.semanticscholar.org/topic/Viola–Jones-object-detection-framework/234542>

МЕТОДЫ ОПЕРАТИВНОЙ КЛАССИФИКАЦИИ ТЕКСТОВЫХ ДОКУМЕНТОВ

Классификация текстов – одна из важных задач информационного поиска заключающаяся в отнесении документа к одной или нескольким категориям из заранее определенного набора на основе анализа содержания этого документа.

Для решения задач текстовой классификации используются методы машинного обучения. Они отличаются такими особенностями как:

- высокая скорость классификации;
- снижение роли человека в процессе получения решения.

В диссертации был выбран именно этот подход. была поставлена цель: экспериментально исследовать методы автоматизированной классификации текстовых документов.

А также ряд задач: проанализировать и обобщить существующие методы автоматизированной классификации текстовых документов (КТД); оптимизировать один из существующих методов КТД; реализовать программное средство для исследования характеристик существующих методов КТД; провести исследование по быстродействию, точности классификации и функциональных возможностей в сравнении с своим доработанным методом.

Для реализации программного средства был выбран язык Python. Так как он уже имеет ряд вспомогательных библиотек таких как:

- IPython – это интерактивная оболочка с широким набором возможностей и ядро для Jupyter. Jupyter notebook является графической веб-оболочкой для IPython;
- Scikit-learn для работы с классическими алгоритмами машинного обучения;
- Pandas для извлечения и подготовки данных;
- Matplotlib для визуализации данных.

В качестве исходных данных были взяты тематические новости, которые были собраны в наборы данных в файлы формата csv. Таких набора два: один для обучения модели (train.csv), а второй для проведения тестов (test.csv)

Данные файлы размещены следующим образом: первым идет номер класса к которому принадлежит текст от 1 до 4 (так как у нас 4 класса World, Sports, Business, Sci/Tech). далее идет заголовок новости и потом уже сам текст статьи (рисунок 1).


```

"3", "Building code back in hot seat", "With insurance claim projections fr
"2", "UPDATE 1-Gibernau cruises to victory at Czech GP", "Spaniard Sete Gib
"1", "Singapore #39;s new PM delivers national day rally speech", "Singapor
"3", "Marks and Spencer loses crown as Britain's top clothing retailer (AF
"2", "Gymnast Khorkina Says 'Judges Robbed Me'", " MOSCOW (Reuters) - Russi
"3", "Stocks May Rally if Oil Eases", " NEW YORK (Reuters) - Investors will
"1", "COTE D IVOIRE: All sides pledge commitment to peace process again &l
"1", "Palestinians Chide U.S. Over Settlements", "JERUSALEM - Palestinian l
"2", "Greek Weightlifter Stripped of Olympic Medal, Ejected From Athens &l
"2", "England humble Windies", "ONCE the tailenders of world cricket, Engla
"1", "Iraq clashes kill 40, handover talks stall", "US tanks rumbled to witi
"1", "Train set ablaze as violence spreads in Bangladesh", "Dhaka, Aug 22.
"1", "North Korea Denounces Mass Defection", "North Korea has denounced as
"3", "Judge gives United temporary reprieve", "A federal bankruptcy judge h
"2", "UPDATE 1-Gibernau storms to pole for Czech GP", "Spaniard Sete Gibern
"2", "Swiss pair eliminates Holdren, Metzger", "Stein Metzger screamed, as
"1", "Mob sets fire to train in protest at attack", "An angry mob set fire
"3", "BA prepares new sick leave deal", "British Airways says it will intro
"3", "Asda clothing overtakes M amp;S", "Marks amp; Spencer is no longer th
"3", "India News gt; Trucker #39;s strike enters second day:", "The Delhi
"4", "Amazon.com to Acquire Retailer Joyo.com", "Internet retail giant Amaz

```

Рисунок 1 - Файл с входными данными

Для классификации были применены следующие методы: Naive Bayes: Bernoulli Naive Bayes, Multinomial NB; SVM (support vector machine): Linear SVM.

На рисунке 2 представлен процесс работы программы.



Рисунок 2 - Процесс работы ПС

На рисунке 3 представлены результаты работы методов, а также коэффициент точности. Можно увидеть, что наилучший результат показал метод SVM.

```

Показатель точности Бернулли
0.8902631578947369
Результат классификатора
['Business' 'Science and Tech' 'Science and Tech
'Science and Tech']
print (accuracy_score(test_lbl, ypredMnb))
Multinomial accuracy score
0.8935526315789474

print (accuracy_score(test_lbl, ypredLsvm))
Linear Svm accuracy score
0.91

```

10

Рисунок 3 - Показатели точности для каждого из методов

Далее были построены матрицы путаницы. На рисунке 4 представлена для метода SVM. Числа по диагонали, они еще выделены красным показывают количество корректно классификации для каждого класса. А те что не по диагонали показывают ошибочные классификации (например, 140 кл. Sport было неправильно клас-но как кл. World).

Из матрицы так же было видно, что у метода SVM было меньше всего ошибочных классификаций.

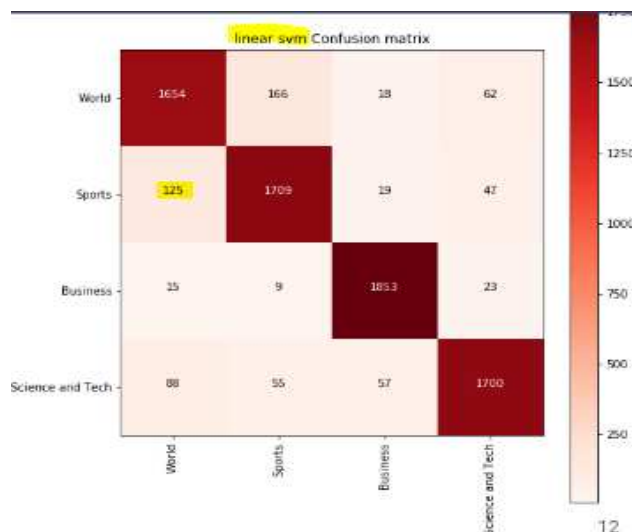


Рисунок 4 -Матрица путаницы

Подводя итог, на данном наборе данных и данными набором классов наилучший результат в текстовой классификации показал метод SVM.

В дальнейшем планируется доработать метод SVM. Результаты, которые будут получены в ходе его работы сравнить с уже имеющимися. Добавить больше алгоритмов. Прodelать тесты на других наборах данных с другим количеством классов.

УДК 621.967

А.А. Рауба, магистрант; И.Г. Сухорукова, ст. преп. (БГТУ, г. Минск)

РАЗРАБОТКА АЛГОРИТМА ИЛИ МЕТОДА МОНЕТИЗАЦИОННЫХ ПРОЦЕССОВ В WEB- ПРИЛОЖЕНИЯХ

Разработчики создают приложения с разной целью. Кому-то нужно повысить уровень лояльности аудитории к своей компании, кто-то хочет получить больше клиентов, а кто-то просто желает заработать здесь и сейчас. Зачастую создаваемые приложения – это дополнительный маркетинговый канал для бренда, который во многих случаях начинает работать практически сразу после запуска.

При этом часть разработчиков создают что-то свое, поскольку хотят приобщиться к рынку, где некоторые приложения (например, WhatsApp) стоят миллиарды долларов.

Для монетизации сайтов существуют немного другие модели монетизационных процессов, в сравнении с мобильными или настольными, они в основном заключены в рекламных интеграциях, но

также присутствуют и другие виды заработка, которые зачастую используются в web-приложениях:

- партнерские программы;
- контекстная реклама;
- тизерная реклама;
- реферальная программа;
- баннеры;
- продажа ссылок;
- файлообменники;
- публикация заказных статей;
- прямые продажи;
- торговля трафиком.

Все эти варианты по-своему хороши, каждый преследует определенную цель, но каждый из этих методов имеет собственные минусы в отношении к пользователям: большая стоимость покупки приложения, надоедливая реклама, ограничения в использовании, высокая стоимость дополнительного функционала и т. д. Иногда различные подходы могут комбинироваться между собой, грань между функционалом, сервисом и контентом, равно как и между своим и чужим может быть весьма условной, стираться или отсутствовать напрочь. Все эти методы могут использоваться параллельно друг другу, при этом увеличивая или уменьшая прибыль и неудобства для пользователя. Эффективность методов проверяется только на практике, но надо подразумевать, что для разных типов приложений и решаемых ими задач подходят разные способы монетизации. Что-то подходит для ленивых, а что-то требует капитальных вложений и серьезной работы. Что-то дает отдачу быстро и в больших объемах, а что-то медленно и маленькими порциями. Где-то нужно ориентироваться на число пользователей, а где-то на число возвратов.

В рамках подготовки магистерской работы будет произведен анализ уже существующих методов монетизации приложений различных категорий (web, мобильные и т.д.), выявление ярких минусов и плюсов. На основе этих данных планируется разработать новый метод или алгоритм монетизации web-приложений, в котором будут отражены все положительные качества уже существующих методов. Созданный алгоритм будет применен в web-приложении по учету и анализу показателей работы персонала предприятия.

ЛИТЕРАТУРА

1. Ирина Ленград, «Мобильный маркетинг для бизнеса», стр. 1-18
2. Андрей Меркулов, «Монетизация бизнеса», стр. 12-25
3. Kathy Williams Chiang, Andrew Roman Wells, «Monetizing

Your Data», 2017

4. Монетизация приложений Windows [Электронный ресурс] – <https://msdn.microsoft.com/ru-ru/dn659712.aspx>

5. Способы монетизации сайта [Электронный ресурс] – <https://ifish2.ru/sposoby-monetizatsii-sajta/#i-2>

УДК 004.75

М. А. Левин, магистрант;
Д. В. Шиман, доц., канд. техн. наук (БГТУ, г. Минск)

МОДЕЛЬ НАГРУЗКИ ДЛЯ ПРОВЕДЕНИЯ НАГРУЗОЧНОГО ТЕСТИРОВАНИЯ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Для проведения нагрузочного тестирования в направлении объёмного тестирования и тестирования производительности необходимо провести следующие подготовительные этапы:

1. Анализ инфраструктуры;
2. Конфигурация тестового стенда;
3. Разработка модели тестовой нагрузки;
4. Реализация модели тестовой нагрузки.

По завершении этих этапов можно приступить к проведению тестирования и анализ результатов тестирования.

Анализ инфраструктуры проходит следующим образом: необходимо определить, какие программные и аппаратные средства используются для выполнения поддержки работоспособности системы на текущем уровне.

Конфигурация тестового стенда включает в себя определения параметров тестируемой системы и внедрение программного или программно-аппаратного (гибридного) средства для проведения тестов.

Разработка модели – самый сложный и длительный этап проведения тестирования. Он включает в себя аналитику данных о потенциальных пользователях, создание прототипов пользователей, оценка нагрузки, генерируемой разными видами пользователей, создание сводной характеристики каждого класса пользователей, описание сценария имитации каждого вида пользователей и выбор имитационных инструментов.

Реализация модели включает в себя написание программного средства/скрипта для готового программного средства для проведения тестирования и организацию средств для сбора аналитики по поведению среды во время тестирования (т.е. для сбора результатов тестирования).

Основной упор в представленной работе можно сделать на разработку тестовой имитационной нагрузки. Сам процесс разработки можно разделить на следующие этапы:

1. анализ требований. Требования включают в себя время отклика (время необходимое для получения ожидаемого результата), интенсивность (число запросов в секунду – (Qps), используемые ресурсы (загрузка процессора, кол-во используемой памяти, дисковое и сетевой I/O), максимальное количество пользователей (определяет число пользователей, способных работать с системой в условиях заданной конфигурации);

2. анализ целевой аудитории включает в себя сбор статистических данных об активности пользователей, разделение пользователей по типу выполняемой деятельности (классификация), описание сценариев тестирования на основе реального поведения пользователя каждой группы, создания графика распределения операций, выполняемых пользователями в течении дня

3. определение базового профиля нагрузки предполагает определение задач, которые выполняет модель в соответствии с тем, какой класс пользователей она имитирует.

4. разработка моделей нагрузки

Для проведения анализа целевой аудитории была рассчитана статистика по следующей общности студентов:

а) 3 курс - ИСиТ – 10 человек, ПОИТ – 15 человек, ПОиБМС – 4 человека;

б) 4 курс - ИСиТ – 28 человек, ПОиБМС – 13 человек.

В качестве основного инструмента для проведения тестирования в работе рассматривается Micro Focus LoadRunner, как утилита для автоматизированного нагрузочного тестирования.

Для выполнения тест необходимо написать скрипт. Написание скрипта можно разделить на следующие шаги:

1. Запись скрипта: обычно это первый шаг скрипта, на котором каждое действие пользователя записывается в скрипт.

2. Запуск и проверка: после того, как сценарий написан, запустите его, чтобы убедиться, что он работает правильно. Проверьте любое воздействие на интерфейс, производительность и т.д.

3. Улучшение сценария: после проверки результатов выполнения сценария, улучшите сценарий, добавив контрольные точки, проверив данные, добавив транзакции и точки останова.

4. Перезапуск и проверка: как и ранее, повторите сценарий и убедитесь, что все работает должным образом.

5. Настройка параметров среды выполнения: настройка и кон-

троль длительности шага, изменение времени, параметры прокси-сервера и хотите ли вы игнорировать какие-либо внешние ресурсы.

В результате проведённой деятельности была построена имитационная модель для 3 классов пользователей, в соответствии со специальностями студентов-программистов УО БГТУ, подготовлена стендовая модель и проведено предварительное (конфигурационное) тестирование.

ЛИТЕРАТУРА

1. Black, R. Critical Testing Processes Plan, Prepare, Perform, Perfect/ R. Black. – Boston: Addison-Wesley, 2014. – с. 65-97.

2. Molyneaux, I. The Art of Application Performance Testing: From Strategy to Tools / I. Molyneaux, /– O'Reilly Media; 2 edition, 2014, P. 181-202.

УДК 004.41

А.С. Демещик, магистрант; И. Г. Сухорукова, ст. преп.;
(БГТУ, г. Минск)

СЕНТИМЕНТ-АНАЛИЗ. СФЕРЫ ПРИМЕНЕНИЯ, ПРОБЛЕМЫ, ЗАДАЧИ

Сентимент-анализ (анализ тональности, англ. Opinion mining) – класс методов контент-анализа в компьютерной лингвистике, предназначенный для выявления в тексте эмоционально окрашенной лексики, а также мнений автора по поводу объектов и/или событий, которые описываются в тексте. Иными словами, можно сказать, что сентимент-анализ – это выявление тональности текста при помощи методов NLP (англ. natural language processing – обработка естественного языка), статистики, машинного обучения.

Стоит отметить, что «тональность», либо «эмоциональная окраска» бывает не только биполярной (например, «положительная» или «отрицательная»). Иногда рассматривается третья граница – «нейтральная». Так же, тональность может выражаться с помощью некой шкалы различной размерности, например – рейтинг комментария в звездах, от 0 до 5.

Задачей анализа тональности является нахождение мнений в тексте и определение их свойств. В зависимости от поставленной задачи нас могут интересовать разные свойства, например, автор, то есть лицо, которому принадлежит мнение; тема – то, о чем говорится во мнении; тональность – позиция автора относительно упомянутой

темы.

В общем случае, мнение может быть записано кортежем из 5 элементов (e, f, op, h, t):

e – entity – объект тональности;

f – feature – свойство(-а) объекта;

op – orientation/polarity – тональная оценка;

h – holder – владелец(субъект) мнения;

t – time – время, когда было выражено мнение.

Можно выделить подзадачи, которые решаются на этапе проведения анализа тональности и благодаря решению которых получают вышеописанные кортежи: извлечение и классификация сущности (entity); извлечение и классификация свойств сущности (feature); извлечение и классификация субъектов мнения (holder); извлечение и стандартизация времени (time); тональная классификация свойств (feature); генерация пятерок мнений.

Говоря о применении sentiment-анализа, можно выделить несколько основных областей, которые, однако, довольно обширны:

- маркетинг (изучение мнений пользователей относительно продукта). Маркетинговое применение актуально не только для крупных корпораций, желающих оценить необходимость своего продукта, но и рядовых потребителей, желающих ознакомиться с отзывами других пользователей, перед приобретением продукта;

- политика (изучение мнений народных масс с целью влияния). Sentiment-анализ особенно важен и все чаще используется в политических целях, с целью убеждения населения в каком-либо мнении, либо, наоборот, изучении, как население относится к власти;

- мониторинг мнений миллионов пользователей в Сети. Развитие Интернета сделало реальной возможность отслеживания огромного количества мнений без особых затрат: достаточно лишь открыть какой-либо форум и мысли, позиции, оценки тысяч человек относительно определенной темы становятся доступными.

Ниже приведены несколько методов анализа тональности текста.

Методы, основанные на правилах и словарях

В рамках этих методов, текст анализируется на основе заранее составленных тональных словарей. Основная проблема этих методов заключается в трудоемкости составления словаря.

Метод, основанный на теоретико-графовых моделях

Текст изображается в виде графа на основе предположения, что некоторые слова имеют больший вес и, очевидно, сильнее влияют на тональность всего текста. Результат вычисляется как соотношение ко-

личества слов с положительной оценкой к кол-ву слов с отрицательной.

Методы, основанные на машинном обучении

Методы этой группы можно разделить на две категории: обучение без учителя и с учителем. Чаще используются методы из категории «с учителем». Сутью является то, что первоначально машинный классификатор обучается на заранее размеченных текстах, а затем используются для анализа новых документов.

Хотя сентимент-анализ не является «новой» технологией и известен уже достаточно давно, существуют некоторые проблемы, которые требуют решения и тщательного рассмотрения во время проведения анализа, для предотвращения возможных ошибочных результатов: неоднозначность слов; фильтрация эмоций, которые не относятся к основной теме; правильная трактовка многомерных настроений и др.

ЛИТЕРАТУРА

1. М. В. Клевковина, Е.В. Котельников. Метод автоматической классификации текстов по тональности, основанный на словаре эмоциональной лексики. Переславль-Залесский, Россия: конференция – 2012.
2. Bing Liu. Sentiment Analysis and Opinion Mining. Morgan & Claypool Publishers = 2012.
3. Bishop С.М. Pattern recognition and machine learning. Vol. 4, New York = 2006.

УДК 621.967

А.Р. Бакиев, магистрант; А.С. Наркевич, ст. преп. (БГТУ, г. Минск)

АЛГОРИТМЫ И МЕТОДЫ ОПРЕДЕЛЕНИЯ ДВИЖУЩЕГОСЯ ОБЪЕКТА ДЛЯ СОЗДАНИЯ ОБЛАЧНОГО ВИДЕОРЕГИСТРАТОРА

Появление современных облачных сервисов значительно упрощает задачу создания системы видеонаблюдения. При подключении камер к облаку в большинстве случаев не нужен статический IP адрес, а также не приходится возиться с настройками роутера.

Слежение за объектами является важной частью в классе задач компьютерного зрения. Всего существует три ключевых шага в видео анализе:

- обнаружение интересующего движущегося объекта;
- слежение за такими объектами от кадра к кадру;
- анализ объекта слежения для распознавания его поведения.

Таким образом, использование слежения за объектом примени-

мо для таких задач как:

- распознавание на основе движений;
- мониторинг трафика;
- автоматизированное наблюдение, то есть наблюдение за определенной сценой действий для обнаружения подозрительной активности или нежелательных событий.

Для исследования были выбраны следующие методы обнаружения движущихся объектов в видеопотоке:

– метод вычитания фона с использованием смеси Гауссовых распределений;

– алгоритм Лукаса-Канаде.

Исходя из полученных данных, можно выделить сильные и слабые стороны каждого из методов:

– алгоритм Лукаса-Канаде для построения оптического потока довольно устойчив к изменениям освещенности, яркости и контрастности кадров видеопоследовательности. Недостатками данного метода являются неустойчивость к воздействию шума, а также неэффективность обнаружения объектов при медленных движениях (медленнее, чем 1 пиксель за кадр).

– главным недостатком метода вычитания фона является возможная классификация фоновых пикселей как переднеплановых. Это возникает при появлении на видеопоследовательности листьев деревьев, снега и так далее. Алгоритм не устойчив к изменению разрешения видео-данных. Преимущества данного метода: достаточная устойчивость к воздействию шума, простота реализации.

В рамках подготовки магистерской работы были проанализированы существующие методы определения движущегося объекта в видеопотоке. Относительно полученных данных разрабатывается модифицированный алгоритм Лукаса-Канаде для получения точных данных.

ЛИТЕРАТУРА

1. Б. Яне, «Цифровая обработка изображений», стр. 15-28.
2. Wiki – Техническое зрение [Электронный ресурс]. Режим доступа: <http://wiki.technicalvision.ru/index.php/>
3. Способы классификации движущихся объектов на видео [Электронный ресурс]. Режим доступа: <https://moluch.ru/archive/122/33749/>
4. Скрипкина, А.А. Обзор методов обнаружения движущегося объекта по видеоизображениям / А.А. Скрипкина // Перспективы развития информационных технологий. – 2011. – № 3-1. – С. 126-127

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ JAVA ДЛЯ ЦИФРОВОЙ ПОДПИСИ ЭЛЕКТРОННОГО ДОКУМЕНТА

Приложения, которыми будут пользоваться большое количество пользователей, или крупные компании, имеют серьезные требования к безопасности. Пользователи должны быть уверены, что данные, проходящие через приложения, не были изменены, не были украдены, пришли от конкретного человека или дошли до конкретного человека или организации. Если предприятие небольшое, то все эти условия могут быть соблюдены при выполнении общих правил безопасности. Однако, с ростом компании таких мер становится недостаточно. Ситуация становится еще более сложной, когда для передачи данных требуется выход за пределы локальной сети.

Основой для безопасной работы с данными является криптография. Использование криптостойких алгоритмов шифрования, хэширования и электронной подписи обеспечивает безопасность при использовании электронного документооборота.

Java позволяет использовать криптографию для написания приложений поддерживающих безопасность электронного документооборота (ЭДО) как в виде встроенной функциональности, так и в виде сторонних библиотек. Помимо этого, при разработке криптографической части java, была предусмотрена возможность расширения встроенных возможностей в виде использования криптографических провайдеров. Любой разработчик имеет возможность написать свой криптографический провайдер, в котором будут реализованы механизмы криптографии, и предоставлять этот провайдер конечным пользователям, независимо от самого языка.

Стандартная реализация языка включает в себя провайдер, который предоставляет наиболее распространенные преобразования для шифрования и хеширования, например, DSA, RSA, MD5, SHA и т.п. Для платформы Java предоставляется API. Оно включает в себя криптографию, аутентификацию, инфраструктуру открытых ключей, защищенные коммуникации и контроль доступа. Данное API придерживается следующих принципов:

- независимость реализации;
- совместимость;
- расширяемость алгоритмов.

Независимость имплементации говорит нам, что приложения не должны сами реализовывать криптографические алгоритмы. Java включает в себя набор широко используемых криптографических алгоритмов. Однако, для некоторых приложений требуется специальная реализация криптографических алгоритмов. Java расширяема т.к. поддерживает установку «кастомных» провайдеров.

Криптографический провайдер ссылается на пакет, который предоставляет конкретную реализацию какого-либо криптографического алгоритма. Класс `java.security.Provider` (JCA) инкапсулирует непосредственно сам провайдер. Он определяет имя провайдера и перечисляет сервисы, которые он реализует. При этом есть возможность настроить несколько провайдеров и определить их приоритет. Когда приложение запрашивает какой-либо сервис, то используется реализация того провайдера, которые имеет наивысший приоритет.

Система JCA позволяет реализовать библиотеки в виде криптопровайдеров `java`. При этом разработчик, который будет использовать данные криптопровайдеры, сможет легко подключить криптостойкие ЭЦП на базе криптографических хеш-функций семейства SHA-2 и SHA-3. Если требуется интегрировать новый криптопровайдер с ЭЦП в уже существующую систему, то не потребуется никакого изменения кода, кроме замены криптопровайдера. Существуют готовые библиотеки в `java` для электронной цифровой подписи (ЭЦП) и разработчик может подключать их в своем решении:

- Java включает в себя криптопровайдер SUN с решением для создания ЭЦП;
- Apache Santuario – в составе библиотеки присутствуют алгоритмы DSA, RSA, ECDSA;
- Bouncy Castle – DSA, RSA, ECDSA;
- Cryptix – DSA, ElGamal, RawDSA, RSA;
- FlexiProvider – RSA, DSA, ECDSA, ECNR. ECNR.

ЛИТЕРАТУРА

1. Koret, J. The Antivirus Hacker's Handbook / J. Koret, E. Bachaalany – John Wiley & Sons, Inc., Indianapolis, Indiana. – 2015. – P. 165-175.

2. Kaspersky Security Bulletin. Overall statistics for 2017 [Electronic resource]. – 2017. – Mode of access : http://media.kaspersky.com/jp/pdf/pr/Kaspersky_KSB2017_Statistics-PR-1045.pdf. – Date of access : 15.01.2019

УДК 621.383.29:621.514.015

В. И. Никитенок, доц., канд. техн. наук (БГУ, г. Минск);
С. С. Ветохин, зав. кафедр., канд. физ-мат. наук (БГТУ, г. Минск);
А.М. Бахарь, первый зам. нач. военного факультета (БГУ, г. Минск);
Е. В. Терешко (БГТУ, г. Минск)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ПРОВЕРКИ ПРОСТОЙ ГИПОТЕЗЫ О ПАРАМЕТРЕ ЭКСПОНЕНЦИАЛЬНОГО РАСПРЕДЕЛЕНИЯ

Экспоненциальный закон распределения широко используется в различных областях науки и техники. К примеру, в зависимости от анализируемых выборочных значений стационарный пуассоновский поток (СПП) событий представим законом Пуассона или экспоненциальным законом распределения интервалов между соседними событиями. Оба представления имеют право на практическое применение. Вместе с тем, СПП имеет достаточно большое число приложений. Отмечается, что этими математическими схемами описываются самые различные модели физических явлений: в области радиофизики, аэрокосмических радиоэлектронных и информационных систем и технологий, физики, прикладной математики и информатики, радио- и оптической локации (прием слабых (на уровне фотонов) оптических сигналов), физико-химических методов сертификации продукции.

Известно, что оптимальный алгоритм проверки гипотезы о параметре экспоненциального распределения вероятностей сводится к сравнению среднего арифметического m выборочных значений с порогом правила решения. Другой известный оптимальный алгоритм, получаемый из первого, включает сравнение суммы выборочных значений с соответствующим порогом правила решения.

Для нахождения показателей качества алгоритмов (условных вероятностей ошибок первого и второго рода) в первом случае используется хи-квадрат распределение с $2m$ степенями свободы, в другом – гамма-распределение. Известно, что хи-квадрат распределение является частным случаем гамма-распределение (оба распределения медленно сходятся к нормальному при увеличении объема выборки). Вместе с тем сравнительный анализ показателей качества алгоритмов (при использовании указанной аппроксимации) выявил следующее: при очень близких и близких гипотезе и альтернативе относительные расхождения величин мощностей правила решения либо отсутствуют, либо допустимы. С увеличением расстояния между гипотезой и альтернативой это расхождение оказывается неприемлемым.

Казимова Д.А., проф., канд. пед. наук;
Тусупхан А.Т., магистрант; Оскенбай А., магистрант;
Ермекова Д., студ. (КарГУ имени академика Е.А. Букетова)

ПОДГОТОВКА ИТ-СПЕЦИАЛИСТОВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ КАЗАХСТАНА

В настоящее время инфраструктура Казахстана становится основным фактором развития социально-экономических капиталов страны, а внедрение цифровых образовательных технологий способствует интеграции информационной инфраструктуры образования Республики Казахстан в мировую образовательную среду.

В Государственной программе «Цифровой Казахстан», отмечено, что развитие отрасли образования способствует внедрению инноваций, обеспечивает молодежь необходимыми знаниями и навыками, необходимыми для конкурентоспособности на современном рынке труда и является одной из ключевой движущей силой экономического роста [1].

Переход к цифровизации требует от системы образования решения принципиально новой проблемы подготовки ИТ-специалистов, приспособленных к быстро меняющимся реалиям окружающей действительности, способных не только воспринимать, хранить и воспроизводить информацию, но и продуцировать новую, управлять большими данными и эффективно их обрабатывать. Изменение требований к подготовке ИТ-специалистам продиктовано появлением новых типов теоретических и практических задач, отличающихся системным и междисциплинарным характером, нестандартностью, глобальностью возможных последствий.

В настоящее время профессиональные кадры в области информационных технологий являются одними из наиболее востребованных на рынке труда развитых стран, в том числе и в Казахстане.

К настоящему времени сформировался достаточно устойчивый список наиболее распространенных трендовых специальностей ИТ-сфере.

На сегодняшний день имеется «Атлас новых профессий» проект российских ученых, где показаны перспективные отрасли и профессии на ближайшие 15–20 лет. Он поможет понять, какие отрасли будут активно развиваться, какие в них будут рождаться новые технологии, продукты, практики управления и какие новые специалисты по-

требуются работодателям[2].

В разработке профессиональных стандартов Казахстана наиболее преуспела АО «Национальный инфокоммуникационный Холдинг «Зерде», которая совместно с представителями ведущих ВУЗов разработали профессиональные стандарты по большинству профессий в области информационно-коммуникационных технологий, это такие как: проектировщик ПО; системный и сетевой администратор; специалист по администрированию баз данных; специалист по тестированию ПО; бизнес-аналитик; специалист по сопровождению ПО; системный-аналитик. Если проанализировать эти профессиональные стандарты, то можно сделать вывод, что для большинства IT-профессий требуется практически один и тот же базовый набор компетенций [3].

В казахстанских вузах начали разработку новых образовательных программ по ИТ-сектору, такие как: разработчик/тестирующий ПО; специалист по трехмерной графике; разработка моделей BIG DATA; архитектор информационных систем; искусственный интеллект, робототехника и др.

Таким образом, можно утверждать, что важнейший итог обучения и образования студента в вузе подготовка к профессиональной деятельности. Она определяется системой требований, которые предъявляет общество к специалисту. Характер требований обусловлен условиями процесса цифровизации. Задача вуза состоит в том, чтобы всей системой учебно-образовательной работы обеспечить подготовку ИТ-специалистов к будущей работе, наиболее полно соответствующей данным требованиям.

ЛИТЕРАТУРА

1. Государственная программа «Цифровой Казахстан» на 2017-2020 года. Режим доступа: <http://zerde.gov.kz>. Дата обращения: 15.01.2019 г.
2. Атлас новых профессий. Режим доступа: <http://atlas100.ru> Дата обращения: 20.01.2019 г.
3. Профессиональные стандарты. Режим доступа: <http://atameken.kz> /542-profstandart. Дата обращения: 10.01.2019 г.

К ВОПРОСУ О СУЩНОСТИ ПОНЯТИЯ «АЛГОРИТМ»

Процесс решения задачи может быть записан на некотором языке, и следовательно может быть рассмотрен как некоторый информационный процесс. Алгоритм как информационная модель осуществляет управление формальным исполнителем: ведет его от начального объекта к конечному. Этот момент особенно важен при рассмотрении автоматизации процесса решения задачи.

Анализ научной литературы констатирует разнообразие подходов трактовки понятия «алгоритм». Одни исследователи определяют алгоритм как конечную систему правил, другие — как организованную последовательность действий, третьи – как способ решения задачи. Некоторые ученые истолковывают алгоритм как описательно-проектировочную знаково-символьную модель.

По мнению И.Н Фалиной [1], алгоритм – это точная конечная система правил, определяющая содержание и порядок действий исполнителя над некоторыми объектами (исходными и промежуточными данными) для получения (после конечного числа шагов) искомого результата. Н.А. Криницкий утверждает, что «алгоритм – это правило, сформулированное на некотором языке и определяющее процесс переработки допустимых исходных данных в искомые результаты» [2].

Понятие алгоритма подразумевает сформулированную цель, язык, описывающий порядок действий, и возможно, физическое устройство, реализующее алгоритм. Вместе с тем алгоритм является способом решения вычислительных и других задач, который точно приписывает, как и в какой последовательности получить результат.

Н.А. Криницкий утверждает, что алгоритмы – это богатство науки и техники. По мнению ученого, алгоритмы являются: 1) формой изложения научных результатов; 2) руководством к действию при решении уже изученных проблем и, как следствие: 3) средством, позволяющим экономить умственный труд; 4) необходимым этапом при автоматизации решения задач; 5) средством (инструментом), используемым при исследовании и решении новых проблем (особенно это касается математических алгоритмов); 6) одним из средств

обоснования математики; 7) одним из средств описания сложных процессов[2].

Большая ценность алгоритмов обуславливает интерес к ним. Естественно, что специалисты каждой отрасли науки и техники все время ищут алгоритмы решения различных задач. Каждый новый алгоритм немедленно включается в «золотой фонд» науки. При этом интересны как новые алгоритмы, так и алгоритмы для решения вновь поставленных проблем.

По мнению В.Л. Малоряна, современная цивилизация – это цивилизация алгоритмов. Алгоритмы управляют ключевыми моментами жизни человека и общества. Неалгоритмизируемые, творческие моменты существуют параллельно с ними, оттеняя, дополняя и проявляясь на фоне алгоритмических. При этом последние составляют как бы основу, поток действительности, ее массовую компоненту, рутину, фон [3].

Следует отметить, что алгоритм является интегративным понятием, которое рассматривается в различных сферах человеческой деятельности и давно уже стало привычным не только для естественных наук, но и для гуманитарных, так как является концептуальной основой разнообразных процессов обработки информации.

Алгоритмы способствуют деятельности человека в самых различных областях, причем, в большинстве случаев результат деятельности человека зависит от того, насколько четко он осознает алгоритмическую сущность своих действий: что должен делать в каждый момент времени, в какой последовательности, каким должен быть результат и т.п. Все это определяет особый аспект культуры мышления человека, характеризующийся умением составлять и использовать различные алгоритмы. Вместе с тем понимание языковых и алгоритмических аспектов общения с компьютером составляет необходимый элемент культуры современного человека.

ЛИТЕРАТУРА

- 1 Фалина И.Н. Элементы теории алгоритмов // Информатика, 2003. - №46. –С. 18-19.
- 2 Криницкий Н.А. Алгоритмы вокруг нас. - М: Наука, 1984. – 224 с.
- 3 Малорян В.Л. Компоненты алгоритмической культуры и задача ее формирования ВУЗом // Материалы десятой Украинской на-

уч.-метод. конф. «Новые информационные технологии образования в учебных заведениях Украины». - Одесса, 2003. - Ч.1. - С. 39-46.

УДК 004

А.И. Демиденко, канд. техн. наук, доц.
О. В. Ременюк, магистрант
(БГТУ, г. Брянск)

ПЕРСПЕКТИВНОСТЬ И АКТУАЛЬНОСТЬ ПРИМЕНЕНИЯ МОБИЛЬНОЙ ПЛАТФОРМЫ «1С:ПРЕДПРИЯТИЯ» В РАЗРАБОТКЕ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Без раздумий можно сказать, что все сферы нашей жизни определяются информационными технологиями. Технологии передачи информации совершенствуются каждый год, превращая не только персональный компьютер, но и смартфоны в цифровой комбайн [3].

Опираясь на опыт разработки расширения для карманных компьютеров, фирмой 1С было принято решение разработать мобильную платформу «1С:Предприятия», которая использует ту же среду разработки (Конфигуратор) и те же методики разработки, что и обычные приложения на платформе «1С:Предприятие».

Приложения, созданные на мобильной платформе, могут обмениваться данными с информационными базами типовых решений "1С:Предприятия", расположенных в облачном сервисе или локально.

Фирма "1С" выпустила ряд приложений, которые разработаны на мобильной платформе "1С:Предприятия". Данное ПО предназначено для использования на планшетах и смартфонах под управлением операционных систем iOS, Android и Windows [2].

Вместе с готовым к работе мобильным приложением фирма "1С" выпускает также версию для разработчиков – типовое решение, на основе которого средствами мобильной платформы "1С:Предприятия" может создаваться новое прикладное решение.

Это хороший шаг фирмы "1С" в сторону мобильности и кросс-платформенности. Данное направление принесет много пользы, в случае активного развития в дальнейшем. Можно выделить кладовщикам планшеты, использовать встроенные камеры, а также перестать использовать устройства считывания. Любой просканированный камерой документ или объект будет распознан в самом смартфоне одной из уже установленных программ (Qrscanner, FineReader и т.д.) и ис-

пользован для учетных целей. Появится возможность трекинга перемещения водителей и грузов и в самой учетной программе, без нужды в дополнительном физическом и аппаратном обеспечении.

Мобильная платформа "1С:Предприятия" позволяет оформлять документы, представляющие какие-то внешние действия, работать с нормативно-справочной информацией, просматривать отчеты, связываться с внешним миром через интернет-сервисов и многое другое. По сути, разработчик способен создать вполне функциональное ПО, к примеру, программу для торговли на выезде, ПО домашняя бухгалтерия и так далее [3].

Помимо стандартного функционала, который есть на платформе для ПК, мобильная платформа обязана обеспечивать работу со нестандартными возможностями, которые не присущи ПК, но присущи мобильным приложениям: геопозиционирование, мультимедийные возможности, сканирование штрих-кодов, контакты, телефония, SMS / MMS, Push и локальные уведомления, покупки и реклама, озвучивание текста и многое другое [5].

Некоторые возможности скорее всего будут недоступны на определенных устройствах. Для того чтобы узнать, что же можно делать на устройстве, на котором запущено мобильное ПО, предусмотрены специальные методы. Эти методы позволяют узнать реализацию и доступность функционала на данном устройстве, к примеру, возможность вызова номера.

Существует очень множество вариантов использования данной технологии. Возможно это именно то, что необходимо рынку мобильных устройств в данный период развития. Важным является то, что собранные с мобильных устройств данные будут находиться в одной информационной среде с общей информацией в компании. С ними будет очень удобно работать руководителям и заказчикам, ведь теперь есть возможность использовать весь функционал на единой платформе, хоть и программа "1С:Предприятия" пока может использоваться ограниченно.

ЛИТЕРАТУРА

1. Демиденко И.А., Демиденко А.И., Создание инфраструктуры инновационного развития на предприятиях // Материалы VII международной научно-практической конференции «Фундаментальные и прикладные науки сегодня», NorthCharleston, USA, 2016 г. 199-203 с.

2. Демиденко А.И., Демиденко И.А., Исаев А.А., Цифровизация управления инновационными ресурсами предприятия и развитие сетевых организационных структур. Монография.

Издательство: Брянский государственный технический университет, Брянск, 2018 г.

3. Хрусталева Е.Ю., Знакомство с разработкой мобильных приложений на платформе 1С: Предприятие 8, М.: 1С-Паблишинг, 2017 г. 225-316 с.

УДК 004.414.22

К. Э. Рейзенбук, ст. преп.; А. А. Иванов, магистрант
(КузГТУ, г. Кемерово)

АВТОМАТИЗАЦИЯ ПРОЦЕССА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ КРЕДИТОВАНИИ ФИЗИЧЕСКИХ ЛИЦ

Жизнь современного человека неразрывно связана с финансовой сферой. Автоматизация данной сферы является одним из приоритетных направлений развития для современных ИТ-технологий. Любые покупки, перечисление зарплат, денежные переводы и кредитование в современных странах производятся с помощью электронного оборудования специального программного обеспечения. Разрабатываемая информационная система поможет оптимизировать и обезопасить работу с деньгами, в частности, в сфере кредитования [1].

Если рассматривать банковское кредитование, как самый распространенный случай кредитования, то его определение можно представить, как самостоятельная и лицензированная предпринимательская деятельность, направленная на извлечение прибыли кредитной организации, которая включает в себя привлеченные вклады денежных средств клиентов на условиях срочности, платности и возвратности.

Если рассматривать банковское кредитование, как один из важных аспектов финансовой стороны жизни, то кредитование является деятельностью, в которой замешаны определенные риски потери средств физического или юридического лица, а так риски потери средств кредитной организации. Большинство кредитных организаций используют кредитный скоринг для того, чтобы отсеивать «неблагонадежных» клиентов и сфокусироваться на «хороших» клиентах.

Кредитный скоринг является важным инструментом, который используют финансовые организации для минимизации рисков. В кредитный скоринг входят определенные правила, благодаря которым можно определить, к какому типу клиентов относится проверяемое лицо [2].

Имея определенный список правил, данный вид проверки можно автоматизировать, и свести время проверки отдельного человека до минимума. К такому виду программного обеспечения относятся системы поддержки принятия решений.

Система поддержки принятия решений (СППР) – это интерактивная компьютерная система, обеспечивающая пользователю доступ к моделям и данным для решения слабоструктурированных и неструктурированных задач. Такие системы позволяют агрегировать большое количество данных и, пользуясь ими, принимать решение по поставленной задаче, с которой пользователь в обычных условиях либо не справился бы полностью, либо затратил на ее решение неприемлемое количество времени. За основу методики принятия решений при кредитовании физических лиц берется кредитный скоринг.

Разрабатываемая система поддержки принятия решений при кредитовании физических лиц может автоматически обрабатывать большой поток кредитных заявок в реальном времени и принимать по ним решение в течение нескольких минут. Используя статистику по предыдущим заявкам, оператор может корректировать работу системы, изменяя модель принятия решений и повышая эффективность ее работы.

ЛИТЕРАТУРА

1. Иванов, А.А. Информационная система поддержки принятия решений при кредитовании физических лиц // Информационно-телекоммуникационные системы и технологии (ИТСиТ-2018): Материалы Всеросс. научно-практич. конференции, г. Кемерово, 11-13 октября 2018 г.; Кузбасс. гос. техн. ун-т им. Т.Ф. Горбачева. – Кемерово, 2018. – С. 167.
2. Тикота, И. Руководство по кредитному скорингу / И. Тикота, Э. Мейс, Д. Вороненко.–М. :ГревцовПаблшер, 2016. – 464 с.
3. Иванов, А.А. Алгоритмическое и программное обеспечение системы поддержки принятия решений при кредитовании физических лиц // Современные технологии принятия решений в цифровой экономике: сборник трудов Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. – Томск: Изд-во Томского политехнического университета, 2018. – С. 201-203.

ПУТИ ВНЕДРЕНИЯ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

В статье рассматриваются варианты внедрения медицинских информационных систем (МИС), выявляются проблемы, связанные с внедрениями и подбираются альтернативные варианты для их решений.

Процесс внедрения информационных систем в различные сферы жизни уже запущен. В частности, в ближайшем будущем абсолютно все медицинские учреждения будут оборудованы электронными регистрами, проще будет получить больничный, т.к. он электронный. Это облегчит работу не только больницы, но и контролирующих и связующих организаций[3].

Для того, чтобы произошло удачное внедрения МИС необходимо выполнение всех задач, которые ставит перед собой организация. К задачам, которые должна выполнить медицинская информационная система относятся:

- МИС должна выполнять медицинскую деятельность;
- МИС должна выполнять административную деятельность (документооборот, учет сотрудников);
- МИС должна выполнять финансовую деятельность (вести бухгалтерию учреждения, организацию лечебного питания и другое).

Очень важно, чтобы при внедрении были выполнены все необходимые условия:

- техническое обеспечение
- сетевое обеспечение
- системное обеспечение
- программное обеспечение
- техническое обслуживание
- программное сопровождение[1].

И последнее менее важное условие- информационная безопасность.

Невыполнение одной из составляющих нарушит механизм внедрения медицинских информационных систем.

Когда медицинское учреждение выбирает информационную систему, главное внимание уделяется в первую очередь программному продукту. Но даже самые лучшие технологические решения не будут востребованы, если не будет квалифицированных сотрудников, которые способны научить работе конечного пользователя. Проблема

не только в том, чтобы организовать обучение на непосредственно работе за ПК. Существуют более значительные проблемы[2]:

- 1) Ранее неудачный опыт внедрения.
- 2) Бессистемный подход к автоматизации, внедрения «сверху».
- 3) Психологическая проблема медицинского персонала.
- 4) Переоценка или недооценка возможностей МИС.
- 5) Незнание или непонимание возможностей, предоставляемых современными средствами автоматизации[4,с.16].

В процессе подготовки и планирования проекта очень важно учитывать данные позиции:

- Сформировать предварительный план необходимых требований при выборе поставщика и программного продукта.
- Сформировать техническое задание к системе.
- Организационно-кадровые решения, или формирование команды проекта со стороны медицинского учреждения.
- Выявление «сильных» и «слабых» сторон проекта внедрения. Расстановка приоритетов. Успех внедрения во многом обусловлен качеством подготовки и планирования проекта.

Таким образом, создание необходимой инфраструктуры, поставка самых современных, надежных и хорошо отработанных решений и даже проведение обучения – это не более половины пути в решении задачи полноценного внедрения МИС.

ЛИТЕРАТУРА

1. Граванова Ю.В. Сбор, учет и архивирование в медицинских учреждениях URL: /reviews/free/national2016/articles/sbor/
2. Кононов М.В., С.П. Радченко. Информатика в медицине URL:http://www.rpd.univ.kiev.ua/downloads/abitur/cikavo/inf_in_med.doc
3. Лапрун И. А.Эффективность внедрения медицинских информационных систем PC WeekDoctor №1 (1), март 2018
4. Тишук Е.А. Современные проблемы информационного обеспечения управления здравоохранением. Врач и информационные технологии; №7 2018
5. Симпозиум «Медицинские информационные системы», 2017г. г. Кондопога, Карелия - Гусев А. В., Романов Ф. А., член-корреспондент РАМН Дуданов И. П. «Обзор МИС на Отечественном рынке в 2017 году»

Д. Б. Шатько, доц., канд. техн. наук;
В. В. Крюкова, доц., канд. техн. наук
(КузГТУ, г. Кемерово)

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ ТЕХНОЛОГИИ В СИСТЕМЕ МЕНЕДЖМЕНТА КАЧЕСТВА ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Процессный подход на основе международного стандарта ISO 9001:2015 [1] предполагает возможность повышения результативности системы управления качеством (СМК) образовательного процесса через учет и анализ требований потребителя.

В этой связи, внедрение информационно-аналитических технологий (ИАТ) с реализацией аналитического модуля на основе математических методов обработки информации и современных технических средств в рамках информационной системы управления в СМК является актуальной задачей образовательной организации.

Цель работы – анализ практических аспектов внедрения ИАТ в СМК образовательной организации на примере Кузбасского государственного технического университета имени Т.Ф. Горбачева (КузГТУ).

Исследование существующих подходов к совершенствованию СМК образовательных организаций [2- 5] выявил основные направления автоматизации задач (функций) в СМК – анализ и оценка удовлетворенности потребителей и внедрение системы управления задачами (СУЗ, поручениями).

Проведенный аналитический обзор публикаций по использованию в образовательных организациях информационных платформ для разработки систем управления задачами (поручениями) и готовых программных продуктов, позволил выделить наиболее популярные: Microsoft Outlook, Битрикс24, Мегаплан, LeaderTask, Руководитель.

Сравнительный анализ возможностей показал, что каждая система обладает определенными достоинствами и недостатками. Общим недостатком является относительно высокая стоимость программного продукта и затраты на приобретение лицензии.

Для разработки системы управления задачами (поручениями) в КузГТУ была использована система Руководитель в качестве информационной платформы, которая обладает следующими достоинствами:

- возможность установки, как на собственных внутренних серверах, так и на большинстве распространённых интернет-хостингах;
- базовая бесплатная часть продукта Руководитель является полнофункциональным программным средством, без каких-либо ограничений на количество пользователей, проектов и др.;
- возможность гибкой настройки уровней доступа пользователей и др.

В общем случае в СУЗ КузГТУ реализованы следующие функции: выдача поручения, исполнение поручения, обсуждение результатов, корректировка (при необходимости), контроль исполнения. Кроме того, для обеспечения функционирования СУЗ разработана соответствующая локальная нормативная база (методические инструкции, памятки и др.).

Система оценки удовлетворенности потребителей – это программная разработка КузГТУ. В системе реализован модуль Опросы, в котором размещены анкеты для обучающихся, сотрудников, абитуриентов и выпускников. Ежегодно проводятся опросы всех категорий потребителей на предмет их удовлетворенности услугами, оказываемыми КузГТУ. Статистическая обработка результатов осуществляется в автоматическом режиме. По результатам принимаются управленческие решения. Разработана соответствующая нормативная документация.

Таким образом, использование ИАТ в системе менеджмента качества КузГТУ позволило повысить эффективность управления основных процессов и университета в целом за счет автоматизации задач, контроля процессов и реализации обратной связи с потребителями.

ЛИТЕРАТУРА

1. ISO 9001:2015 «Системы менеджмента качества. Требования». – Режим доступа: <http://docs.cntd.ru/document/1200124394>. – Загл. с экрана (дата обращения 18.12.2018).

2. Верховцева А.В. Оценка удовлетворенности потребителей образовательных услуг в системе менеджмента качества образовательной организации. Вестник Российской академии естественных наук. – 2014. – № 18(2). – С. 60–63.

3. Парсегова Т.А., Парфеньева И.Е. Оценка удовлетворенности потребителей в системе менеджмента качества организации // Инновации в науке: сб. ст. по матер. LXII междунар. науч.-практ. конф. № 10 (59). – Новосибирск: СибАК, 2016. – С. 75-84.

4. Абдукаримов В. И. Оценка труда и контроль исполнения поручений в системе менеджмента. Вестник ТГУ. – 2011. – № 12 (104). С. 524-528.

5. Вениг С. Б., Соловьева В. А. Трансформация образовательного пространства под влиянием информационных технологий. Информатизация образования и науки – 2017. – № 1(33). – С. 73-88.

УДК 004.056.5

А.И. Демиденко, доц., к.т.н.; Е.П. Николаенко, магистрант 2 курса
(БГТУ, г. Брянск)

ВЛИЯНИЕ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Цифровая экономика всё активнее заменяет старый уклад во многих сферах деятельности. Благодаря этому повышается эффективность всех отраслей, ведь использование современных информационных технологий активно этому способствует.

Информационная безопасность как одна из важнейших составляющих общей безопасности определяет экономическую и общую безопасность на всех уровнях.

Сегодня руководство любого промышленного предприятия имеет дело с корпоративной информацией, которая должна соответствовать требованиям актуальности, целостности, достоверности, структурированности, и, при необходимости, конфиденциальности.

Такая информационная зависимость привела к существенному увеличению влияния уровня безопасности информационных систем на успешное ведение бизнеса, а иногда и просто возможность его функционирования. Исходя из этого, можно сделать вывод о том, что безопасность информационных систем является одним из важнейших аспектов, который имеет огромный интерес для аналитиков, инженеров и других специалистов в области информационной безопасности.

В рекомендациях стандарта ГОСТ Р ИСО/МЭК 27005-2010 отмечается, что для оценки рисков можно использовать как существующие, так и разрабатывать новые методики. В связи с этим, изучив достоинства и недостатки существующих методик, была разработана новая методика оценки рисков.

Основная задача данной методики заключается в том, чтобы определить численный показатель рисков ИБ с целью принятия эффективных мер по защите информации и других критически важных активов организации. Предлагаемая методика оценки рисков позволяет

выполнить полноценный анализ и оценку рисков без привлечения высококвалифицированных специалистов.

При определении вероятности реализации угрозы необходимо учитывать, что если существует несколько средств нейтрализации, и их эффективности имеют разный уровень, то эффект нейтрализации не суммируется, а берется в итоге равный самому эффективному средству.

Высокий темп роста развития технологий передачи и обработки информации позволило рассматривать её в разрезе ценнейших ресурсов. Тяжело оспорить тот факт, что сегодня информация обладает уникальной ценностью, при этом являясь одним из критически важных для человека ресурсов, ведь это и коммерческие и производственные тайны, новые идеи и т.д. Это затронуло и сферу ведения бизнеса. Информация активно применяется для принятия весомых стратегических заключений и от результата, т.е. от того насколько она будет являться достоверной, правдивой и актуальной, будет зависеть дальнейшая работоспособности представленной компании. Потеря конфиденциальности информации: разглашение или утечка коммерческой тайны могут повлечь значительные убытки для предприятия, в том числе и финансовые, а также негативно отразиться на имидже компании. Устранение одного или же нескольких информационных ресурсов может на длительный срок остановить работу всего промышленного предприятия. Важность вопроса обеспечения информационной безопасности уже не вызывает сомнений, в ближайшее время вопросы управления рисками информационной безопасности будут являться ключевыми проблемами бизнеса.

ЛИТЕРАТУРА

1. Демиденко А.И., Лазуткин А.Н. оценка затрат на внедрение системы обеспечения информационной безопасности предприятий // Материалы II Международной научно-практической конференции профессорско-преподавательского состава, магистров и студентов факультета экономики и управления. Брянск, БГТУ, 2015, 215-218 с.

2. Кваша Е.П. Управление ИТ-инфраструктурой как сервис // Материалы международной мультидисциплинарной научно-практической конференции студентов, магистрантов и аспирантов "ЭМПИ - экономика, менеджмент, прикладная информатика и новые яркие идеи и решения". Брянск, БГТУ, 2016, 349-353 с.

3. Лазуткин А.Н., Демиденко А.И. Построение эффективной системы информационной безопасности // Материалы международной научно-практической конференции профессорско-преподавательского состава. Брянск, БГТУ, 2017, 557-562 с.

4. Лазуткин А.Н., Демиденко А.И. экономические аспекты защиты информации на предприятии // Материалы III Всероссийской научно-практической конференции профессорско-преподавательского состава и магистрантов факультета экономики и управления. Брянск, БГТУ, 2017, 173-177 с.

5. Демиденко А.И., Кваша Е.П. Управление рисками информационной безопасности предприятий // РОССИЙСКАЯ НАУКА: АКТУАЛЬНЫЕ ИССЛЕДОВАНИЯ И РАЗРАБОТКИ. Сборник научных статей V Всероссийской научно-практической конференции: в 2 частях. Самара, 2018, 18-21 с.

УДК 659.18

А.В. Крамарь, студ.; А.И. Демиденко, доц., канд. техн. наук
(БГТУ, г. Брянск)

ОДНОСТРАНИЧНЫЙ САЙТ КАК ИНСТРУМЕНТ ПРЕДОСТАВЛЕНИЯ ИНФОРМАЦИИ КОМПАНИИ

В цифровом мире бизнесы стремятся продавать товары и услуги через Интернет. Пользователи делают заказы с помощью смартфона где и когда им удобно. Продавать в Интернете – тренд. Поэтому появляется конкуренция. Обратиться на себя внимание пользователя становится сложнее. Предпринимателям приходится улучшать свой сайт. Чтобы покупателю требовалось меньше действий и раздумий для совершения покупки. Люди не привыкли тратить время на поиск нужной информации. Если пользователям необходимо поискать ответы на вопросы на сайте, они уходят.

Для того, чтобы продвигать компанию, необходимо рекламировать себя. Каким образом? Давать объявления, размещать баннеры на сайтах, рекламировать себя в выдаче по запросам. В рекламе используется ссылка, которая ведет пользователя на сайт.

Компании продают группы товаров и на каждую из них необходимо делать рекламу. Реклама ведет на страницу с товаром, который ищет покупатель. То есть под разные заголовки рекламы разные товары. Было бы непрактично добавлять для каждого рекламного объявления странички на сложные сайты, которые пишут программисты. Зачастую этот процесс занимает 2 месяца. И за это время рекламная компания может стать неактуальной.

Таким образом, одностраничные сайты становятся эффективным и удобным инструментом для продвижения информации об услугах и предложениях компании.

Что такое одностраничный сайт?

Это современный сайт, состоящий из одной страницы и направ-

ленный на выполнение одной определенной задачи: сбор контактов, оформление заявки на участие в вебинаре, заказ подробной информации о предлагаемом продукте, загрузка электронной книги и т.д. В отличие от многостраничного сайта, одностраничник направлен на получение быстрого и конкретного результата. Такие сайты еще называют лендингом, посадочной, продающей или целевой страницей.

Рекламно-информационная страница предоставляет посетителю максимум полезной информации о продвигаемой услуге или продукте. Затем направляет человека туда, где этот продукт или услугу можно заказать.

Главная задача посадочной страницы – получение конверсии. Для того, чтобы выполнять эту задачу необходимо применять следующие принципы:

1) Минимализм в оформлении – чтобы не отвлекать посетителя от совершения главного действия.

2) Смысловая структура – каждый блок одностраничного сайта является продолжением предыдущего и ведет к нужному действию.

3) Отсутствие сложных графических элементов – они затрудняют работу страницы и усложняют восприятие информации.

Лендинги повышают продажи уже известных товаров или услуг. Для этого используются специальные элементы, чтобы человек совершил определенное действие здесь и сейчас. Акции с таймером ограничивают действие выгодного предложения и помогают клиенту быстрее решиться на покупку.

Также удобнее воспользоваться одностраничным сайтом, когда на рынок выводится новый товар или услуга. Их сложнее продавать сразу, потому что люди вначале изучают предложение. А лендинги предоставляют потенциальному покупателю всю информацию и выгодно подчеркивают преимущества товара или услуги.

Одностраничные сайты создают на платформах – конструкторах. Где сайт собирается из блоков. В целом предоставляет порядка 400 штук. Наиболее известные программы – uLanding, TOBIZ, Wfolio и Tilda. Среди них есть бесплатные, платные с пробным периодом пользования.

По мнению интернет-маркетологов, форматлендинга позволяет максимально привлечь внимание посетителей к его тематике.

Таким образом, одностраничные сайты являются удобным инструментом в предоставлении информации покупателю о своих услугах и предложениях.

ЛИТЕРАТУРА

1. Автоматизированные системы сбора и обработки информации: учеб.пособие / Ю. Ю. Громов [и др.]. - Воронеж: Науч. кн., 2016. 108 с.

2. Влацкая И.В. Распределенная обработка информации :учеб.пособие / И.В. Влацкая, С.И. Сормов. - Оренбург: ИПК ГОУ ОГУ, 2014. 146 с

УДК 330.47

М.А. Мамошина, магистрант;
А.И. Демиденко, доц., канд. техн. наук
(БГТУ г. Брянск)

ИСПОЛЬЗОВАНИЕ ГИПЕРКОНВЕРГЕНТНОЙ АРХИТЕКТУРЫ КАК СПОСОБ УПРОЩЕНИЯ ИТ- ИНФРАСТРУКТУРЫ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

Традиционные ИТ-инфраструктуры предприятий и облаков строились на основе отдельных аппаратных составляющих: серверных вычислителей (обычно блейд-серверов), внешних систем хранения данных (СХД) и быстрой сети между ними (обычно FiberChannel). Отказоустойчивость и производительность обеспечивалась за счет дублирования и специального оборудования корпоративного класса с высокой удельной стоимостью на получаемую мощность вычислителя/объем хранения данных. При этом наращивание (масштабирование) производительности вычислений и/или емкости СХД связано с высокими и нелинейными расходами с большим минимальным шагом. Более того, после 3–5 лет эксплуатации стоимость сопровождения такого устаревшего оборудования и ПО возрастает, и потребность в его модернизации часто приводит к созданию новой системы. Все это выливается в высокую стоимость владения, недостаточную гибкость построенной по таким принципам ИТ-инфраструктуры и снижение конкурентоспособности предприятий. Все это стало предпосылками к появлению гиперконвергентной архитектуры, основной смысл которой сводится к отказу от отдельного специализированного оборудования (блейд-серверов, СХД, FC-сетей и т. п.) и объединению виртуализации вычислений, хранения данных и сетевых функций в особом программном обеспечении, работающем на «обычных» (commodity) серверах. Это позволяет существенно уменьшить затраты

и сроки как построения новых систем, так и их постепенного обновления и масштабирования. Перенос функций обеспечения отказоустойчивости и производительности с «железа» на программное обеспечение, работающее на распределенной ферме «обычных» серверов позволяет использовать недорогое оборудование, при этом повышая степень его полезного использования, взаимозаменяемость узлов и уровень управляемости полученной системой. В отличие от классической архитектуры, в случае с гиперконвергентной системой достаточно подключить новые простые узлы для масштабирования системы. Система сама их определит и начнет эксплуатировать в соответствии с настроенной стратегией. Перераспределение задач и нагрузки произойдет автоматически.

Такой подход несет в себе принципиально другую модель проектирования и эксплуатации ИТ-инфраструктур, позволяя оперировать на уровень выше вычислителей, сетевого оборудования, сети хранения – все это становится программно-определяемыми компонентами, а система сама решает, на каких узлах их физически разместить, следит за «здоровьем» составных частей, выводит из эксплуатации непригодные и подключает новые компоненты. Администратор только задает основные параметры конфигурации, а система самостоятельно определяет, какие физические ресурсы из доступных для этого использовать. Наконец, единое управление ключевыми функциями обработки и хранения данных позволяет интегрировать контроль и над всеми смежными задачами – резервным копированием, защитой от вирусов, блокчейн-нотариатом целостности данных

ЛИТЕРАТУРА

1. Демиденко А.И., Казулин А.Л., Влияние информационно-телекоммуникационных технологий на социальную и экономическую сферу деятельности человека Материалы международной научно-практической конференции «Экономическое развитие регионов и приграничных территорий Евразийского экономического союза (ЕАЭС), Брянск, БГТУ, 2017, 327-328 с.

2. Демиденко И.А., Демиденко А.И., Создание инфраструктуры инновационного развития на предприятиях // Материалы VII международной научно-практической конференции «Фундаментальные и прикладные науки сегодня», NorthCharleston, USA, 2016 г. 199-203с.

3. Демиденко И.А., Демиденко А.И., Управление конкурентоспособностью предприятий региона // III Международная научно-практическая конференция «Инновационно-промышленный потенциал развития экономики регионов», Брянск, БГТУ, 2016, 310-313 с.

4. Кваша Е.П. Управление ИТ-инфраструктурой как сервис // Материалы Международной мультидисциплинарной научно-практической конференции студентов, магистрантов и аспирантов "ЭМПИ - экономика, менеджмент, прикладная информатика и новые яркие идеи и решения". Брянск, БГТУ, 2016, 349-353 с.

5. Измалкова С. А., Внедрение высоких технологий в деятельность промышленно-экономических систем: интегрированный подход. Орел: ФГБОУ ВПО «Государственный университет-УНПК», 2017

УДК 004.93.1

С.А. Кульмамиров, и. о. доцента
(Казахский национальный университет им. аль-Фараби);
Г.К. Ордабаева, ст. преп.; А.С. Кыдырбекова, ст. преп.
(Казахский национальный аграрный университет Алматы, Казахстан)

ИССЛЕДОВАНИЕ БИОМЕТРИЧЕСКОГО СПОСОБА РАСПОЗНАВАНИЯ ЛИЧНОСТИ

Аннотация: В статье рассмотрены результаты авторских исследований по биометрической аутентификации и идентификации личности. Исследованный способ аутентификации используется для удостоверения личности людей в их биометрических данных (по овалу лица человека). Описан процесс доказательства и проверки подлинности личности через предъявление пользовательского биометрического образа. Аппаратное средство состоит из биометрических сканеров и терминалов. Оно фиксирует биометрический параметр (отпечаток пальца, радужную оболочку глаз, рисунок вен на ладони или пальце). Их полученных изображений составляется цифровая модель. Специальная программа обрабатывает данные, сортирует и сравнивает с изображениями из базы данных. Результаты аутентификации и идентификации личности выдает решение, кто представился перед сканером.

Ключевые слова: БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ЛИЧНОСТИ, АУТЕНТИФИКАЦИЯ ПО ЛИЦУ, ИДЕНТИФИКАЦИЯ, БИОМЕТРИЧЕСКАЯ СИСТЕМА, ТЕРМИНАЛ, ЦИФРОВАЯ ОБРАБОТКА, ИДЕНТИФИКАТОР.

В настоящее время биометрическая аутентификация и идентификация личности являются способом аутентификации, использующим для удостоверения личности людей в их биометрических данных [1].

В статье излагается результаты исследований одного из биометрического способа распознавания личности по овалу лица. В этом способе процесс доказательства и проверки подлинности личности может осуществляться через предъявление пользователем своего биометрического образа. Далее путем преобразования этого образа в соответствии с заранее определенным протоколом биометрической системы аутентификации.

Рассматриваемая биометрическая система состоит из двух частей: аппаратных средств и специально написанной программы. Аппаратные средства включают в себя биометрические сканеры и терминалы. Они фиксируют тот или иной биометрический параметр (отпечаток пальца, радужную оболочку глаз, рисунок вен на ладони или пальце) и преобразуют полученную информацию в цифровую модель, доступную компьютеру для проведения соответствующей обработки. Специальной программой эти данные подлежат цифровой обработке, результаты обработки сортируют и сравнивают с типовыми изображениями базы данных. В случае положительного решения программа выдает решение, кто предстал перед сканером[2].

Для того, чтобы специальная программа биометрической системы смогла в дальнейшем идентифицировать личность, в ней необходимо учитывать исходные сведения с ненулевыми начальными условиями о его идентификаторах [3].

Биометрическая система как прототип типовой информационной системы (ИС) хранит не изображения реальных идентификаторов, а их цифровые модели. Когда специальная программа повторно обращается к системе, вновь формируется модель его идентификатора, и она сравнивается с моделями, уже занесенными ранее в базу данных (рисунок 1).

Приведем самый простой пример функционирования биометрической системы аутентификации и идентификации личности: человек поднимается по лестнице, и заходит в лифт, он знает, на какой этаж ему нужно. Далее двери в квартиру перед человеком сами открываются. Компьютер и телефон «узнают» личность и не требуют ввода пароля.

Вот таким образом сейчас входят в общественную жизнь цифровые биометрические системы [4]. Автомобили, социальные сети, магазины - все приветствуют человека после биометрического сканирования, обращаются к нему по имени и предугадывают каждый его шаг.

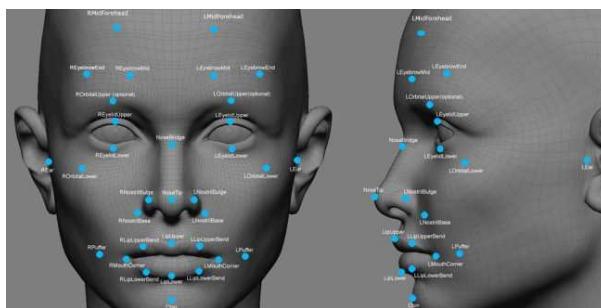


Рисунок 1 - Цифровая модель биометрической системы распознавания личности по лицу

Так работает алгоритм распознавания личности человека в биометрической системе. На первый взгляд может показаться, что любая организация или общественность, которая может себе позволить иметь биометрическую систему, следит за каждым шагом человека. Но в наше время сложно представить, как широко технологии распознавания личности распространились по всему миру и какие мощные перспективы обещают такие методы и технологии.

Помимо выше приведенного примера, биометрические системы распознавания лиц, например в образовании и обществе, позволяют делать такие простые или сложные вещи:

- подтверждение личности обучающегося во время онлайн-экзаменов;
- определение личности из «черного списка» на входе на стадионы и ночные клубы;
- оплата товаров по желанию конкретно известного человека;
- сохранение места личности в очереди при посещении парка аттракционов;
- разблокировка телефона или компьютера личности.

Также общеизвестно, что в одной только Москве уже работает сеть из более 150 000 камер наружного видеонаблюдения. От них никуда не скрыться, и это заставляет людей задумываться, но масштабы «слежки» не настолько велики. Сеть использует мощную систему распознавания лиц, но для ее работы необходимо много энергии, поэтому в режиме реального времени работают всего 2-4 тысячи камер. Массовым слежением за населением пока только пугают, поэтому стоит сосредоточиться на реальных плюсах работы биометрической технологии.

Авторы статьи проводят ряд исследований по изучению свойств биометрической системы распознавания лиц. Исследование началось после постановки актуальной задачи по распознаванию типового лица сознанием человека, т.е. его мозгом. После познания этих свойств биометрии ставилась вторая задача: как это делает компьютер?

Конечно, у человеческих лиц есть определенные свойства, которые легко описать[5]. Расстояние между глазами, положение и ширина носа, форма надбровных дуг и подбородка - все эти детали мозг человека подмечает бессознательно, когда он смотрит на другого человека. Компьютер же делает все это с определенной последовательностью и идентифицирующей точностью. Далее совмещая все эти метрики, получается математическая формула человеческого лица[6].

Также в исследованиях были попытки анализа существующих биометрических систем, чтобы выяснить насколько хорошо работает

система распознавания лиц в настоящее время. Разбор аналитических ситуации и цифровых данных показали, что созданные биометрические системы работают вполне неплохо, но они иногда ошибаются.

Если рассмотреть известную программу распознавания лица на Facebook или на другой социальной сетевой платформе, то в авторских исследованиях были заметны забавные и положительные и отрицательные результаты. И все же, хотя известные биометрические технологии не работают со 100-процентной точностью, они достаточно хороши и эффективны, чтобы найти широкое их применение в промышленных и экономических целях.

Пол Хоуи из NEC говорит [4], что их система распознавания лиц сканирует лица на предмет индивидуальных идентификаторов (рисунок 2).

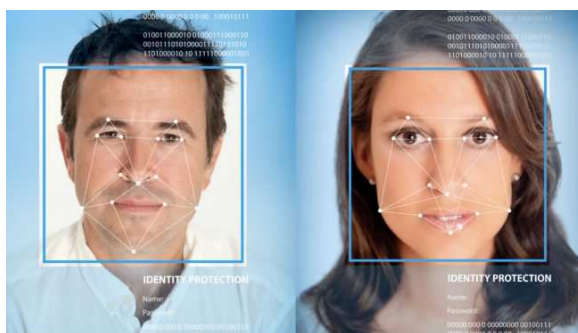


Рисунок 2 – Функционирование системы распознавания лиц человека

В статье лучше привести результаты его исследований, чем лишний раз их комментировать: «... к примеру, многие считают расстояние между глазами уникальной характеристикой. Или же это может быть расстояние от подбородка до лба и другие компоненты. Мы, в частности, учитываем 15-20 факторов, которые считаются важными, а также другие факторы, уже не настолько значимые. Создается трехмерное изображение головы человека, поэтому даже если она частично будет закрыта, мы все равно сможем получить точное соответствие. Затем система берет сигнатуру лица и пропускает ее через базу данных». Вот эти 5 предложений Пол Хоуи сущность работы специальной программы. Это один из первых в мире алгоритмов распознавания лица.

Теперь можно продолжить наши исследования, через совершенствование существующих алгоритмов или программ по аутентификации или идентификации личности. Прежде всего, распознавание лиц - это данные в цифровом формате удобные для формирования базы данных (БД). Данные можно собирать и хранить, зачастую без разрешения. Как только информация собрана и сохранена, она открыта и

для взлома. Это наталкивает на мысль обязательно предусмотреть в таких специальных программах и систему информационной безопасности данных (СИБ). Платформы со специальными программами, распознающим лица, пока не подвергались серьезным взломам, но по мере распространения технологий такие биометрические данные оказываются в руках все большего числа взламывающих людей (рисунок 3).



Рисунок 3 – Обоснование наличия СИБ по мере распространения технологий опознавания личности особенно среди взламывающих лиц

Существуют также вопросы владения описанными БД. Большинство людей не знают, что когда они регистрируются в социальных медиаплатформах, вроде Facebook, их данные с этого момента принадлежат этой самой Facebook. Поскольку число организаций, использующих распознавание лиц, постоянно растет, очень скоро даже не придется загружать собственные фотографии в Интернет, чтобы оказаться скомпрометированным. Они уже там хранятся, и хранятся давно [5].

Специальные программы работают по-разному алгоритмам, но в основе своей используют похожие методы и нейронные сети. У каждого лица человека есть множество отличительных признаков (в мире невозможно найти два идентичных лица).

К примеру, программное обеспечение FaceIt определяет эти признаки как узловые точки [3]. Каждое лицо содержит примерно до 80 узловых точек, схожих с теми, что указаны на рисунках 1 и 2: расстояние между глазами, ширина носа, глубина глазных впадин, форма подбородка, длина челюсти. Эти точки измеряются и создают числовой код – так называемый «отпечаток лица», который затем попадает в состав БД.

В прошлое столетие распознавание лиц опиралось на двумерные снимки для сравнения или идентификации других двумерных снимков из хранилища данных. Для достаточной эффективности и точности изображение должно было быть лицом, прямо смотрящим в камеру, с небольшой дисперсией света и без особого выражения лица.

Такие алгоритмы и способы были не эффективными и не всегда срабатывали положительно. В большинстве случаев снимки не создавались в подходящей среде. Даже небольшое изменение света на изображении могла снизить эффективность системы, что приводило к высоким показателям отказа.

В нашем столетии на смену 2D пришло 3D-распознавание. Эта недавно появившаяся тенденция в программном обеспечении использует 3D-модель, обеспечивающую высокую точность распознавания лица [6]. Запечатлевая трехмерное изображение поверхности лица человека в реальном времени, теперь специальная программа выделяет отличительные черты для идентификации субъекта, где больше всего выдаются жесткие ткани и кость, например, кривые глазного гнезда, носа и подбородка. Эти области отличительных черт уникальны и не меняются со временем (рисунок 4).

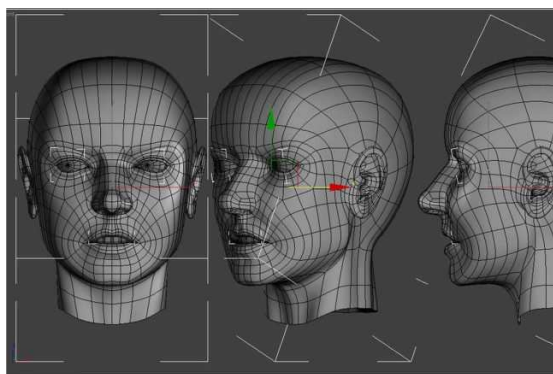


Рисунок 4 - Отличительные черты для идентификации субъекта

Используя глубину и ось измерения, на которые не влияет освещение, система трехмерного распознавания лиц может даже использоваться в темноте и распознавать объекты под разными углами (даже в профиль). Такая специальная программа реализуется выполнением нескольких этапов, идентифицируя человека:

- обнаружение - получение снимка при помощи цифрового сканирования существующей фотографии (2D) или видео для получения живой картинке субъекта (3D);

- центровка - определив лицо, программа фиксирует положение головы, размер и позу;

- измерение- программа измеряет кривые на лице и биометрическая система с точностью до миллиметра и создает шаблон;

- репрезентация - система переводит шаблон в уникальный код. Этот код задает каждому шаблону набор чисел, представляющих особенности и черты лица;

- сопоставление - если снимок в 3D и БД содержит трехмерные

изображения, сопоставление пройдет без изменений снимка. Но если БД состоит из двумерных снимков, трехмерное изображение раскладывается на разные составляющие (словно сделанные под разными углами двумерные снимки одних и тех же черт лица), и они конвертируются в 2D-изображения. И затем находится соответствие в базе данных;

- аутентификация или идентификация - в процессе верификации снимок сравнивается только с одним из снимков в БД (в масштабе 1:1). Если целью обработки изображения является идентификация, то снимок сравнивается со всеми снимками в БД. Это приводит к ряду возможных совпадений снимков в масштабе 1:N. По необходимости применяются тот или иной другой метод биометрической идентификации.

Столетие назад биометрические системы распознавания лиц находили применение в основном в сфере правоохранения, поскольку государственные органы использовали их для поиска случайных лиц в толпе. Некоторые правительственные органы также использовали подобные системы для безопасности и для устранения мошенничества на выборах.

Однако есть много других ситуаций, в которых такая специальная программа становится популярным и востребованным. Биометрические системы становятся все дешевле, их распространение растет. Теперь они совместимы с камерами и компьютерами, которые используются банками, гостиницами и аэропортами. Туристические агентства работают над программой «бывалого путешественника»: с ее помощью они проводят быстрый скрининг безопасности для пассажиров, которые добровольно предоставляют информацию. Очереди в аэропортах будут продвигаться быстрее, если люди будут проходить через биометрическую систему распознавания лиц, сопоставляющую лица с внутренней БД.



Рисунок 5 - Сопоставление лиц в биометрической системе

Другие широкие применения включают банкоматы и терминалы выдачи наличных денег. Специальная программа может быстро проверить лицо клиента. После разрешения клиента банкомат или терминал делает снимок лица. Программа создает отпечаток лица, защищающий клиента от кражи личных данных и мошеннических тран-

закций. Далее банкомат просто не выдаст деньги человеку с другим лицом. Все так просто, даже ПИН-код не потребуется.

Особенно важным и интересным может быть развитие биометрической технологии распознавания лиц в сфере банковских переводов. Из публикации СМИ известно, что недавно российский банк «Открытие» представил собственное уникальное решение, разработанное под технологическим брендом «OpenGarage». Алгоритм бренда состоит: перевод денег по фотографии в мобильном приложении «Открытие.Переводы». Вместо того чтобы вбивать номер карты или телефона, достаточно просто сфотографировать человека, которому нужно сделать перевод. Биометрическая система распознавания лиц банка сравнивает фото с эталонным снимком из БД. Эталонный снимок был сделан банком, когда банк выдавал пластиковую карту. Специальная программа теперь подсказывает клиенту имя и фамилию. Останется только изъять карту с банкомата и ввести требуемую сумму.

Это особенно важно, когда клиенты сторонних банков также могут использовать эту функцию для переводов клиентам «Открытия». Отправитель переводов может пользоваться картой любого российского банка (рисунок 6).

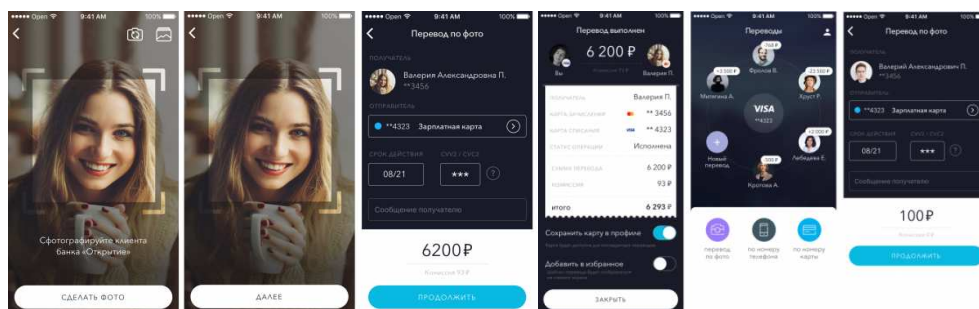


Рисунок 6 - Уникальное решение российского банка «Открытие», представленное под технологическим брендом «OpenGarage»

Здесь уникальностью является использование фотографии клиента вместо номера банковской карты. Это является принципиально новым подходом к онлайн-переводам. Технология основана на использовании нейронной сетевой системы распознавания лиц. Алгоритм биометрической системы банка позволяет с высокой степенью точности идентифицировать клиента по его биометрическим данным. Выгодный для клиентов банка сервис открывает для них совершенно новые жизненные сценарии для выполнения денежных переводов. В настоящее время ни один из участников финансового рынка в мире не предлагает подобного сервиса своим клиентам.

Таким образом, результаты проведенных исследований по био-

метрической аутентификации и идентификации личности показывают, что рассмотренный способ аутентификации используется для удостоверения личности людей в их биометрических данных (по овалу лица человека). Здесь процесс доказательства и проверки подлинности личности осуществляется через предъявление пользователем своего биометрического образа. Исследованная биометрическая система состоит из аппаратных средств и специальной программы. Аппаратные средства включают в себя биометрические сканеры и терминалы, фиксирующие биометрический параметр (отпечаток пальца, радужную оболочку глаз, рисунок вен на ладони или пальце). Эти цифровые устройства преобразуют полученную информацию в цифровую модель, доступную компьютеру для проведения соответствующей обработки. Специальная программа выполняет цифровую обработку данных. Результаты обработки сортируются и сравниваются с типовыми изображениями из базы данных. Своим положительным решением специальная программа выдает результаты аутентификации и идентификации личности, представившейся перед цифровым сканером.

ЛИТЕРАТУРА

1 Milborrow S. Locating facial features with active shape models: Master's thesis. – S. 1.: Faculty of Engineering, University of Cape Town, 2007. – 103 p.

2 Броневич А. Г., Каркищенко А. Н. Вероятностные и возможные модели классификации случайных последовательностей. – Таганрог: ТРТУ, 1996. – 196 с.

3 Кульмамиров С. А., Бейбиткызы Ф. Идентификация ориентира лица человека по ключевым точкам. Сборник трудов ICITE-218 - V-ой Международной конференции «Промышленные технологии и инжиниринг», посвященная 75-летию Южно-Казахстанского государственного университета имени М. Ауэзова и 90-летию академика Сулейменова С.Т. 2018.

4 Броневич А. Г., Гречухин И. А., Каркищенко А. Н. Нечеткая классификация вероятностных распределений в задаче распознавания лиц // Обозрение прикладной и промышленной математики. – 2011. – Т. 18, вып. 6. – С. 530–531.

5 Cootes T. F., Taylor C. J. Technical Report: Statistical Models of Appearance for Computer Vision // The University of Manchester School of Medicine, 2004. – 125 p.

6 Kirby M., Sirovich L. Application of the Karhunen-Loeve procedure for characterization of human faces // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1990. – Vol. 12. – P. 103–108.

ГИС-АНАЛИЗ ОБЕСПЕЧЕННОСТИ НАСЕЛЕНИЯ ГОРОДА МОЛОДЕЧНО ОЗЕЛЕНЕННЫМИ УЧАСТКАМИ В ЖИЛОЙ ЗАСТРОЙКЕ

Озелененность жилой застройки городов является важным показателем качества городской среды. Зеленые насаждения улучшают экологическое состояние жилых микрорайонов, препятствуют сильным ветрам, формируя благоприятный для горожан микроклимат, повышают эстетические качества застройки. Анализ обеспеченности населения озелененными участками в жилой многоквартирной застройке отражает степень благоустройства территории, что представляет интерес как для муниципальных служб и органов архитектуры и градостроительства, так и для рядовых жителей города. Геоинформационные системы (ГИС) позволяют значительно упростить расчет озелененности жилой застройки и представить результаты пространственного анализа в виде карты.

В качестве примера для данного исследования была выбрана территория города Молодечно. На первом этапе было проведено дешифрирование мозаики космоснимков картографического сервиса Bing (пространственное разрешение – 0,5 метра) в программном комплексе ENVI 4.8. Вначале были созданы области интереса, отражающие основные элементы структуры фотоизображения городской территории, которые были использованы в качестве обучающих выборок при классификации изображения способом максимального правдоподобия. Далее полученное изображение было загружено в программный комплекс ArcGIS 9.3, где с помощью инструмента Переклассификация были выделены ячейки растра, закодированные как древесно-кустарниковая растительность. Затем посредством конвертации растра в векторный класс пространственных объектов (инструмент Растр в полигоны) был получен полигональный слой отдешифрованной древесно-кустарниковой растительности территории города Молодечно. Пространственные объекты слоя озелененных территорий были слиты в один объект, а затем разбиты по кварталам жилой застройки. Затем из данного слоя были извлечены не учитываемые в составе озелененных участков жилой застройки зеленые насаждения с ограниченным доступом населения, расположенные в пределах территорий школ и детских садов [1].

Сравнительный анализ площади озелененных участков в жилых массивах и численности их населения (по данным Национального ста-

тистического комитета Республики Беларусь) показал, что, за исключением отдельных кварталов с малоэтажными домами или вкраплениями усадебных участков, только в нескольких микрорайонах, сформированных во 2-ой половине 1950-х – 1-ой половине 1970-х годов, соблюдены нормы по обеспеченности населения средних городов озелененными участками в жилой застройке (15–20 м²/чел.) [2]. Приоритет размещения дополнительных парковочных мест для автомобилей перед размещением древесных насаждений в новых жилых микрорайонах негативно сказывается на микроклимате территории, здоровье и общем уровне удовлетворенности жизнью населения.

ЛИТЕРАТУРА

1 Кравчук, Л.А. Методология оценки уровня структурно-функциональной организации ландшафтно-рекреационного комплекса городов / Л.А. Кравчук // Природопользование: сборник научных трудов. – Минск: Национальная академия наук Беларуси, 2008. – №14.

2 Градостроительство. Населенные пункты. Нормы планировки и застройки: ТКП 45-3.01-116-2008 (02250). – Введ. 01.07.2009. – Минск: Министерство архитектуры и строительства Республики Беларусь, 2009. – 64 с.

УДК. 004

Е.С. Смотриков; А.И. Демиденко, доц., канд. техн. наук
(БГТУ, РФ, г. Брянск)

ИНТЕГРАЦИЯ ERP СИСТЕМ И АСУТП КАК ПЕРВОСТЕПЕННАЯ ЗАДАЧА СОВРЕМЕННОГО ПРОИЗВОДСТВА

Не так давно понятие автоматизации предприятия имело лишь смысл обновление вычислительной техники и программного обеспечения. В настоящее же время быстрыми темпами и широкими масштабами внедряются системы автоматизации предприятий и производств «АСУ» - автоматизированных систем управления (в мировой практике используется название ERP - Enterprise Resources Planning- планирование ресурсов предприятия) и «АСУТП»- автоматизированных системы управления технологическими процессами, так понятие приобрело более широкий смысл, подразумевающий создание единой информационной среды на предприятиях и как следствие устранение информационных барьеров внутри предприятия, повышения управляемости, обеспечение гибкой системы произ-

водства, корректировке производственных заданий, следствием чего является оптимизация различных внутренних технологических и прикладных процессов.[1],[2]

Рациональное и эффективное функционирование современного предприятия – это сложная задача, которая определяет какие организационные и технические факторы ложатся в основу эффективной работы отдельных подразделений на производстве и технологических устоев предприятий.

В отечественной практике довольно продолжительное время складывалась такая тенденция, когда автоматизация на предприятиях осуществлялась по независимым направлениям, одним из которых является внедрение автоматизированных системы управления технологическими процессами, а другим автоматизированные системы управления и планирования ресурсов предприятия. Группы специалистов имели разные конечные цели и идеи, не связанные между собой ни организационно, ни технически. Вопрос интеграции двух систем если и рассматривался, то не доходил до реализации на практике.

Проведя анализ можно говорить о том, что автоматизированная система управления технологическими процессами отдельно функционирующая от системы управления предприятием не может являться эффективной, не имея возможности для уровня руководства предприятия получения данных в реальном времени, служащих, для принятия оперативных и обоснованных управленческих решений, которые бы основывались на объективной оценке текущей ситуации на производстве, именно нехватка прежде всего, технологической информации становится все более актуальной проблемой, влияющей на ход управление производством в целом. Все практически без исключений службы предприятий заинтересованы в получении оперативных и объективных технологических данных, но в абсолютном большинстве случаев, именно отсутствие единого информационного пространства на предприятии ограничивает возможность стандартизации и взаимного обмена данными в реальном масштабе времени между ERP-системами и АСУТП [3]. Решение задачи интеграции таких систем можно считать первостепенной задачей повышения управляемости современных производств. Ликвидация информационных, технических и организационных барьеров между технологическими системами и системами управления, поможет вывести предприятия на новый уровень эффективности.

ЛИТЕРАТУРА

1. Демиденко И.А., Демиденко А.И., Создание инфраструктуры инновационного развития на предприятиях // Материалы VII между-

народной научно-практической конференции «Фундаментальные и прикладные науки сегодня», North Charleston, USA, 2016 г. 199-203 с

2. Смотриков Е.С. Проблемы внедрения автоматизированных информационных систем на современных предприятиях. Труды международной научно-практической конференции «Цифровой Регион: опыт, компетенции, проекты». «Брянский Государственный Инженерно-Технологический Университет» Инженерно-Экономический Институт.2018г

3. Eational Enterprise Management - информационно-аналитический журнал для руководителей и IT-специалистов промышленных предприятий, научных и проектных организаций.

УДК 004.622

А.С. Шульгина-Таращук, ст. преп.; К.М. Турдыбекова, ст.преп.;
Турдыбекова К.К., студ. (КарГУ им. Е.А. Букетова, г. Караганда)

МЕТОДЫ ШИФРОВАНИЯ ИНФОРМАЦИИ

Шифрование может защитить информацию, электронную почту и другие конфиденциальные данные, а также безопасные сетевые подключения. Сегодня существует множество вариантов на выбор, и обязательно нужно найти безопасный и соответствующий вашим потребностям. Вот четыре метода шифрования и что вы должны знать о каждом из них [1].

The Advanced Encryption Standard, AES - расширенный стандарт шифрования, являющийся симметричным алгоритмом шифрования и одним из самых безопасных. Этот метод использует блочный шифр, который шифрует данные по одному блоку фиксированного размера за раз, в отличие от других типов шифрования, таких как потоковые шифры, которые шифруют данные по битам. AES состоит из AES-128, AES-192 и AES-256. Выбранный вами ключевой бит шифрует и дешифрует блоки 128 битами, 192 битами и так далее. Есть разные раунды для каждого ключа бита. Раунд - это процесс превращения открытого текста в зашифрованный текст. Для 128-битного есть 10 раундов; 192-битный имеет 12 раундов; и 256-битный имеет 14 раундов. Поскольку AES - это шифрование с симметричным ключом, вы должны предоставить этот ключ другим лицам, чтобы они могли получить доступ к зашифрованным данным. Кроме того, если у вас нет безопасного способа поделиться этим ключом, и посторонние лица получают к нему доступ, они могут расшифровать все, что зашифровано с помощью этого конкретного ключа.

Triple Data Encryption Standard, 3DES - тройной стандарт шифрования данных, являющийся текущим стандартом и является блочным шифром. Это похоже на более старый метод шифрования, Data Encryption Standard, который использует 56-битные ключи. Однако 3DES - это шифрование с симметричным ключом, в котором используются три отдельных 56-битных ключа. Он шифрует данные три раза, что означает, что ваш 56-битный ключ становится 168-битным ключом. К сожалению, поскольку он шифрует данные три раза, этот метод намного медленнее других. Кроме того, поскольку 3DES использует меньшую длину блоков, легче расшифровывать и пропускать данные. Однако многие финансовые учреждения и предприятия во многих других отраслях используют этот метод шифрования для обеспечения безопасности информации. По мере появления более надежных методов шифрования этот метод постепенно удаляется.

Twofish - это симметричный блочный шифр, основанный на более раннем блочном шифре - Blowfish. Twofish имеет размер блока от 128 до 256 бит и хорошо работает на небольших процессорах и оборудовании. Подобно AES, он реализует циклы шифрования для превращения открытого текста в зашифрованный текст. Тем не менее, количество раундов не меняется, как с AES; независимо от размера ключа всегда есть 16 раундов. Кроме того, этот метод обеспечивает большую гибкость. Вы можете выбрать медленную настройку ключа, но процесс шифрования будет быстрым или наоборот. Кроме того, эта форма шифрования не имеет патентов и лицензий, поэтому вы можете использовать ее без ограничений.

RSA - этот асимметричный алгоритм назван в честь Рона Ривеста, Ади Шамира и Лена Адельмана. Он использует криптографию с открытым ключом для обмена данными по небезопасной сети. Есть два ключа: один публичный и один закрытый. Открытый ключ, как следует из названия: открытый. Любой может получить к нему доступ. Однако закрытый ключ должен быть конфиденциальным. При использовании криптографии RSA вам необходимо использовать оба ключа для шифрования и дешифрования сообщения. Вы используете один ключ для шифрования ваших данных, а другой - для его расшифровки. Согласно Search Security, RSA является безопасным, потому что он учитывает большие целые числа, которые являются продуктом двух больших простых чисел. Кроме того, размер ключа большой, что повышает безопасность. Большинство ключей RSA имеют длину 1024 и 2048 бит. Однако более длинный размер ключа означает, что он медленнее, чем другие методы шифрования.

В то время как существует множество дополнительных методов шифрования, знание и использование самых безопасных из них гарантирует, что ваши конфиденциальные данные остаются в безопасности и вдали от нежелательных глаз.

ЛИТЕРАТУРА

Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование/ С. Н. Никифоров. – Санкт – Петербург: Лань, 2018. – 124 с.

УДК 004.738

Р.И. Допира, ст. преп.; Н.В. Попова, ст. преп.
(Карагандинский государственный университет
имени академика Е.А. Букетова, Караганда, Казахстан)

ФОРМИРОВАНИЕ КОМПЕТЕНЦИЙ ИТ-СПЕЦИАЛИСТА ПРИМЕНЯЯ МЕТОД ПРОЕКТОВ НА ЗАНЯТИЯХ СРСП ДИСЦИПЛИНЫ «ПРОГРАММИРОВАНИЕ НАС++»

Реформирование образовательного пространства предполагает оптимизацию содержания и форм педагогической деятельности, внедрение инновационных технологий в образовательный процесс. Одна из форм педагогической деятельности обеспечивающих профильное обучение – это метод проектов. Метод проектной деятельности активизирует самостоятельную работу обучающихся, направленную на поиск информации и получение практического результата, развивает творческие способности.

Работа над проектами со студентами проводилась на занятиях по дисциплине «Программирование наC++» во время самостоятельной работы студентов под руководством преподавателя. Учащимся было предложено разработать проект, взяв за основу имеющиеся у них знания, полученные за пройденный курс «Технология программирования». Совместно со студентами был разработан план создания проектов, который содержал в себе: формирование состава проектных групп и первичное распределение обязанностей среди группы; формулировка темы проекта, постановка задач, определение конечного вида создаваемого программного продукта, его назначение; выбор программного обеспечения; выделение подзадач для определенных групп учащихся, подбор необходимого материала; непосредственно работа над проектом; подведение итогов.

На первом этапе студенты разбивались на группы, каждая из которых должна разработать собственный проект. Они самостоятельно выстраивали план работы над проектом. На каждом этапе работы обу-

чающийся приобретает опыт (рождение идеи, проверка гипотезы, исследование, оформление результатов, презентация). Студент формирует навыки IT-специалиста, умения использовать теоретические знания на практике и в конечном итоге создает приложение, код программы которого может быть использован при решении других задач программирования.

Знания в области программирования, необходимые для разработки проектов, студенты получили, изучая дисциплины «Технология программирования» и «Программирование на С++», однако студентам предлагалось изучить дополнительную информацию по теме самостоятельно или при помощи консультации преподавателя.

Основную часть проекта студенты создавали сами, однако обращались за консультацией к преподавателю для добавления функций стандартных библиотек. Некоторые студенты заинтересовались реализацией функции и сами разработали нужные функции к проекту.

На защите проектов особое внимание было уделено дизайну и удобству работы с программой. Так как предполагалось, что код программы в дальнейшем будет использован другими программистами, поэтому требования к читаемости кода и простоте использования были первичными.

На этапе реализации проекта преподаватель и студенты сталкивались с различными трудностями. Используя метод проекта, преподаватель воспитывает в своих учениках умение решать текущие проблемы, определять наиболее эффективные способы достижения результата, приобретать навыки, которые способствуют адаптации личности в динамично изменяющемся и развивающемся мире. Результаты работы студентов в проектной деятельности по дисциплине «Программирование на С++» должны иметь практическое значение, если рассматривалась теоретическая проблема, то результатом должен быть алгоритм ее решения, если проблема практическая то разработанное приложение.

Необходимость применения проектной методики в современном образовании обусловлено очевидными тенденциями в образовательной системе к более полноценному развитию личности учащегося, его подготовки к реальной деятельности.

ЛИТЕРАТУРА

1. Полат Е.С. Метод проектов: история и теория вопроса. - М.: изд. центр «Академия», 2010. – 478с.
2. Допира Р.И., Попова Н.В. Использование проектного метода при проведении занятий по дисциплине «Программирование на С#». Международный электронный журнал: Устойчивое развитие: наука и практика. – Дубна, 2016. - № 1 (16). - С. 140-144.

О.В. Крупица, ст. преп.;
А.С. Бихдрикер, доц., канд. техн. наук
К.К. Панайотов, доц., канд. техн. наук
(Луганский национальный университет им. В.Даля, г. Луганск)

ЗАЩИТА ОБЛАЧНОЙ АРХИТЕКТУРЫ НА ОСНОВЕ ТЕХНОЛОГИИ ОТКРЫТЫХ КЛЮЧЕЙ

Облачные технологии являются удобной виртуальной средой, которая используется для хранения и обработки информации. Использование облачных технологий помогает довольно быстро реагировать на появление новых бизнес-задач, снижает затраты и увеличивает эффективность предприятий и их подразделений.

При использовании облачных технологий особенно актуальным является защита информации. Одним из способов повышения эффективности защиты информации является применение единой инфраструктуры открытых ключей. При этом остро стоит вопрос конфиденциальности информации. Криптографические методы защиты являются одним из надежных методов обеспечения такой конфиденциальности.

Практика показывает, что пароли несложно расшифровать, используя технические методы или методы социальной инженерии. Администраторы облачных сервисов требуют от пользователей применение более длинных и сложных паролей, например, использование специальных символов, комбинаций букв обоих регистров, обязательного использования цифр. Это повышает надёжность пароля, но вызывает другую проблему. Пользователи в этом случае часто забывают пароль.

Цифровые сертификаты — это альтернативный способ идентификации пользователя в системе. При практической реализации технологии инфраструктуры открытых ключей (PKI-Public Key Infrastructure) требуется наличие персональных носителей ключевой информации в виде смарт-карт или USB-токенов, на которых хранятся соответствующие закрытые ключи и цифровые сертификаты. Для учета и контроля смарт-карт и токенов в рамках инфраструктуры открытых ключей используются системы класса Card Management, предназначенные для управления жизненным циклом ключевых носителей [2].

Цифровые сертификаты являются частью инфраструктуры открытых ключей, поэтому они обязательно содержат в себе данные об открытом ключе.

Закрытый ключ, который ассоциирован с этим открытым ключом, хранится отдельно от сертификата в защищенном хранилище. Соответственно к ассоциированному закрытому ключу имеет доступ только его владелец. Выделим основные принципы, на которых построены открытые и закрытые ключи [1]:

1. Владея открытым ключом, нельзя получить доступ к закрытому ключу и наоборот.

2. Если данные зашифрованы открытым ключом, то расшифровать их можно только ассоциированным с ним закрытым ключом.

3. Если данные зашифрованы закрытым ключом, то их может прочитать любой пользователь – это так называемая цифровая подпись. Цифровую подпись может создавать только владелец ключа.

Задачу внедрения защищённых файловых хранилищ с шифрованием можно реализовать на базе Windows Server 2016 с помощью службой File classification Infrastructure (FCI). Для реализации обязательного шифрования всех файлов, хранящихся на файловом сервере можно использовать службы FCI и Active Directory Right Management Services (AD RMS) или серверную роль File Server Resource Manager (FSRM). С помощью механизма FCI находят все файлы, которые необходимо защитить, и присваивают им определенные метки, затем для файлов с данными метками создаётся специальное задание RMS Encryption.

Таким образом, используя технологию открытых ключей, можно организовать защищённый обмен информацией между подразделениями предприятия.

ЛИТЕРАТУРА

1. Крупица, О.В., Бихдрикер, А.С. Использование инфраструктуры открытых ключей для защиты облачной архитектуры // Материалы II Республиканской научно-практической Интернет-конференции «Информационные технологии в экономике». Луганск: ЛНУ им. В.Даля, 2018. С. 87-90.

2. Инфраструктура открытых ключей (PKI) [Электронный ресурс]. URL:https://indeed-id.ru/infrastruktura_otkrytyh_kljuchej_pki.html (дата обращения 16.03.2018)

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В АГРАРНОМ СЕКТОРЕ

Технология Blockchain имеет универсальные особенности, так как на сегодняшний день она применяется не только для создания различных криптовалют. На данный момент эксперты в сфере информационных технологий предсказывают хорошее будущее этой инновации в аграрной отрасли.

Blockchain-технология – это метод сохранения информации, цифровой реестр любых транзакций, соглашений или стартовых контрактов, что позволяет накапливать любую информацию: данные о выданных кредитах или о договорах аренды на землю, финансовую отчетность по затратам на гектар (топливо, агрохимия, удобрения, семена), статьи расходов по закупке материально-технических ресурсов, агротехнологические операции и договора по закупке (семена, техники), по реализации продукции и т.д. [1]. Она представляет распределенную систему данных, при которой у каждого участника процесса сохраняется полная информация обо всех операциях, которую невозможно подделать, сломать, изменить или украсть, поскольку используются алгоритмы математического вычисления. Также исключается «человек» и человеческий фактор при принятии решения системой.

Все транзакции в Blockchain хранятся в едином реестре, составляющих децентрализованную структуру для принятия коллективных решений. Поскольку операции полностью упорядочены по времени, текущее состояние системы определяется исключительно этим реестром транзакций. Блоки в базе создаются постоянно, причем каждый новый блок содержит группу накопленных за последнее время и упорядоченных транзакций.

Blockchain поможет агропромышленному комплексу в создании прозрачной и надежной цепочки производства и поставки продуктов, гарантирует пищевую безопасность. Потребители хотят знать о происхождении пищи и готовы переплачивать, если смогу узнать все подробности о товаре. Сейчас соблюдения стандартов гарантирует сертификация, но она дорогая. Другая проблема сертификации в том, что результаты проверок можно изменить задним числом за взятку. Blockchain устраняет эту проблему. Технология не позволит незаметно ввести записи, поскольку их содержание и дата останутся неизменными. Например, наклеив отметку с QR-кодом, покупателю предоставляется возможность проследить все, что происходило с товаром:

когда родилась корова, в каких условиях жила, как ее кормили, чем она болела, когда ее забили, на каком заводе тушу превратили в консервы, как эти консервы транспортировались и хранились. При такой отлаженной системе вся история продукта будет отображаться на экране смартфона потребителя. Государство тоже сможет пользоваться преимуществами цепочки. Санитарные органы смогут отследить, как распространялась эпидемия. Если человеку стало плохо после съеденного, врач сможет моментально узнать, какого качества продукт съел пострадавший [2].

Так, к примеру, в Украине Министерство аграрной политики совместно с Государственным агентством электронного управления и Transparency International Украина презентовали обновленный Государственный земельный кадастр, который отныне будет работать на технологии Blockchain [3]. Внедрение этой технологии позволит обеспечить надежную синхронизацию данных, сделает невозможным их подмену в результате внешнего вмешательства, а также даст возможность осуществлять общественный контроль за системой. Данная сеть имеет самую высокую степень защиты и способна усилить прозрачность земельных отношений, тем самым повышая уровень требований к обеспечению сохранности данных [4].

Для Украины Blockchain является идеальным средством, сможет обеспечить полную прозрачность данных земельного кадастра и завоевать безусловное доверие к ним со стороны населения страны, поскольку технология сочетает в себе внутреннюю безопасность и общественный контроль.

ЛИТЕРАТУРА

1. Блокчейн: революция в агросекторе или авантюра? [Электронный ресурс] - Режим доступа: goo.gl/vtfR9q.
2. Блокчейн плюс сельское хозяйство: как изменится жизнь потребителя и бизнеса [Электронный ресурс] - Режим доступа: goo.gl/QVV4yR.
3. Государственный земельный кадастр перешел на технологию Blockchain [Электронный ресурс] - Режим доступа: goo.gl/oT1nmo.
4. Технология Blockchain в системе Государственного земельного кадастра [Электронный ресурс] - Режим доступа: goo.gl/Sq8VKj.

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ИНТЕГРАЦИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПСИХОЛОГИЮ

Такие сферы как психология и информационные технологии достаточно разной направленности. Нередко обсуждается пагубное влияние технологий на психическое состояние человека. Однако информационные технологии можно использовать во благо процветания такой науки как психология. В мире технологий и инноваций необходим баланс данных сфер.

Современные информационные технологии достаточно расширили возможности статистической обработки имеющихся данных во всех сферах исследований. Относится это и к психологии. Это позволило психологам использовать ныне доступные современные средства обработки данных.

Благодаря этому стали доступны формирование и предъявление тестируемому гораздо большего количества стимулов, их контекстная коррекция в зависимости от сделанного выбора. Значительно упрощается хранение и обработка ответов респондента, при этом одновременно снижается вероятность ошибок на данном этапе диагностики, которые при ручной обработке практически неизбежны. Таким образом появляется возможность минимизировать влияние человеческого фактора, который играет не последнюю роль в процессе диагностики⁵.

Интеграция информационной системы тестирования можно рассматривать с двух сторон. Необходимо грамотно организовать процесс взаимодействия психолога с программными средствами, реализующими тест на экране монитора и последующими процедурами его обработки и сохранения результатов. С другой - это особенности взаимодействия проходящего тестирование человека как с собственно компьютером, так и с материалом теста. В наше время уже существует множество компьютерных систем психодиагностики. Их можно классифицировать по таким показателям, как количество методик в составе системы и возможность изменения методик¹.

Умение грамотно владеть современными средствами обработки данных дает возможность психологу структурировать и качественно интерпретировать результаты психологических экспериментов; создавать и использовать различные виды тестирования, применять авторские методики, разработанные под специфику своей области

исследования; математически моделировать психологические процессы; разрабатывать новые психодиагностические методики.

С помощью применения компьютерных технологий увеличивается эффективность, а именно качество и скорость работы, так как появляется возможность проводить тестирование одновременно целой группы испытуемых; существенно уменьшить рутинную бумажную работу и повысить точность результатов исследования.

К очевидным преимуществам автоматизированной обработки и представления результатов психологических исследований можно отнести снижение вероятности ошибок при обработке и интерпретации результатов тестирования и значительную экономию времени, выделенного для первичной обработки данных.

Современные компьютерные программы и психодиагностические методы облегчают сбор эмпирических данных и лечения, на основе которого намного легче и точнее формировать индивидуальное заключение психодиагностического состояния и анализировать средние показатели тенденции в определенной группе.

Нередко хранение и структурирование информации является большой проблемой в психологии. Поскольку данные клиента не являются публичными, нужно позаботиться о способах хранения. В наше время тестирование проходит на листках и в этом же виде хранят за редким исключением, когда дублируют данные в электронном виде. Информационная система должна иметь возможность защиты от проникновения, для надежного хранения данных клиента.

Таким образом, основными преимуществами интеграции информационных технологий является снижение временных затрат на проведение и обработку тестирования, а так же исключение человеческого фактора.

Зачастую работа школьного психолога сводится к проведению тестирования учеников на профориентацию, на психологическое состояние учеников, уровень стресса и т.п. Стоит упомянуть, что в школах данные исследования проводятся вручную. Сбор информации со всех классов, в которых более 20 учеников, расчет результатов и их интерпретация требует колоссальных труда и времени. Именно поэтому внедренная информационная система для проведения подобных исследований упростила и ускорила бы работу школьного психолога.

Такая система так же может провести простой для ученика тест, который должен проводиться с каждым учеником индивидуально. Суть данного теста заключается в том, что пользователю дается определенный набор цветов, из которых он выбирает наиболее приглянувшийся, данный цвет исчезает из представленного набора, затем

пользователь выбирает цвет из оставшихся. Такие действия совершаются до тех пор, пока не останутся два финальных цвета. Провести этот тест массово "на листках" не получится, т.к. важен факт исчезновения выбранного цвета, иначе он будет мешать дальнейшему выбору.

Определенная последовательность цветов дает обобщенную характеристику внутреннего эмоционального состояния. Такие тесты полезно проводить в периоды сдачи контрольных и экзаменов для определения общего эмоционального фона класса, для проведения определенных мероприятий по его улучшению, если это необходимо.

Таким образом, внедрение данной системы также увеличивает число возможных исследований, которые при проведении вручную для школьного психолога отнимут как минимум одну учебную четверть. Данная трата временных ресурсов не рациональна, именно поэтому данная система необходима для работы школьного психолога⁴.

Такие системы можно подстроить под более игровое восприятие учеников младших классов, вместо тестовых вопросов можно использовать видео, ученик так же может выбирать вместо тестового варианта картинку, соответствующую определенному варианту ответа. Гибкость настройки может сделать интерфейс более приятным для восприятия учеников разных возрастов.

Основными источниками финансирования инновационной деятельности до сих пор являются бюджетные средства; внебюджетные фонды; собственные средства.

Свыше 70% организаций научно-технической сферы в настоящее время находятся еще в государственной собственности. Сегодня доля России в общем объеме мирового рынка наукоемкой продукции невелика и составляет всего 0,3%, однако уже можно отметить некоторую положительную динамику в развитии инноваций в нашей стране. В России с 2010 года по 2018 год количество выданных патентов выросло на 51%, в том числе количество заявок на изобретения за последние 5 лет выросло более чем на 9%².

С 2005 года по 2018 год затраты на исследования и разработки выросли почти в 6 раз и составили более 523 млрд рублей. Вместе с тем в рейтинге ВОИС и INSEAD, по данным доклада "Глобальный индекс инноваций-2015", Россия заняла 51-е место в списке из 141 страны, поднявшись на шесть позиций выше по сравнению с предыдущим годом. А среди стран БРИКС Россия занимает второе место после Китая. («Российская Газета»).

На стадии разработки решения самой частой проблемой является, когда пользователи не могут описать, что они хотят, потому что они не знают, что возможно. Они также не говорят на том же языке, что и программисты, которые будут разрабатывать систему, тем са-

мым практически обеспечивая несоответствие между тем, что хочет пользователь, и тем, что будет строить инженер³.

Описать проблемы, процессы и алгоритмы психологической сферы очень трудно, поскольку ей соответствуют такие характеристики, как контекстное значение какого-либо признака, постоянная динамика средств и методик. При разработке системы нужен человек, который обладает достаточной компетенцией в обеих этих областях для корректной интерпретации пожеланий конечных пользователей на "программный язык".

Еще одной распространенной проблемой является нежелание руководителей организаций тратить средства на обучение персонала. По статистике, данная доля вложений составляет около 3% от капитала фирмы. Однако пробелы в обучении пользования системой выливаются в ошибки управлением конкретным бизнес-процессом. Обучение пользователей системы производится слишком поздно и недостаточно. Это может повлечь за собой ошибки в ведении учета, на некоторых стадиях проведения тестирования, что может повлечь за собой некорректные ответы клиента, интерпретировав которые психолог в конечном итоге может получить совершенно далекие от реальности результаты.

Использование современной компьютерной техники предоставляет качественно новые возможности для проведения диагностики личности и группы. Это относится ко всем этапам и стадиям процесса диагностики.

ЛИТЕРАТУРА

1. Демиденко А.И., Казулин А.Л. Влияние информационно-телекоммуникационных технологий на социальную и экономическую сферу деятельности человека // Материалы международной научно-практической конференции «Экономическое развитие регионов и приграничных территорий Евразийского экономического союза (ЕАЭС), Брянск, БГТУ, 2017, 327-328 с.

2. Афолина Ю.А., Демиденко А.И. Перспективы развития отечественного ПО в России в условиях экономических санкций // Материалы Международной научно-практической конференции профессорско-преподавательского состава, Брянск, БГТУ, 2017, 504-507 с.

3. Бирюкова В.А. Перспективы импортозамещения в сфере ИТ на примере Брянской области // Материалы Международной мультидисциплинарной научно-практической конференции студентов, магистрантов и аспирантов, Брянск, БГТУ, 2016, 346-349 с.

4. Афолина Ю.А., Демиденко А.И. Внедрение системы интерактивного контроля состояния здоровья в РФ // Материалы международной мультидисциплинарной научно-практической конференции студентов, магистрантов и аспирантов, Брянск, БГТУ, 2016, 343-346 с.

5. Электронный журнал психолога [Электронный ресурс]. – Режим доступа: <http://psihologschool.ucoz.ru/publ/6-1-0-70>– Дата доступа 6.01..2019.

УДК 004.056

С.К. Жумагулова, ст.преп.; С. С. Копбалина, ст. преп.;
Б.М. Нурланова, ст.преп. (КарГУ им.Е.А.Букетова)

НЕКОТОРЫЕ ВОПРОСЫ ОБРАБОТКИ ДАННЫХ

Обработка является одной из основных операций, выполняемых над информацией и главным средством увеличения ее объема и разнообразия. Для осуществления обработки информации с помощью технических средств ее представляют в формализованном виде - в виде «информационных объектов», представляющих собой некоторую абстракцию фрагмента реального мира.

Абстракция подразумевает выделение наиболее существенных с точки зрения задачи обработки свойств и связей. Так, например, информация о студенте, необходимая для учета его успеваемости, может быть представлена набором таких идентифицирующих данных, как фамилия, имя, отчество, номер учебной группы [1].

Обработка информации – это получение одних «информационных объектов» из других путем выполнения некоторых алгоритмов. Исполнитель алгоритма - абстрактная или реальная система, способная выполнить действия, предписываемые алгоритмом. Для автоматизации процесса обработки информации и вычислений, выполняемых в соответствии с заданным алгоритмом, используют различные типы вычислительных машин [2].

ЛИТЕРАТУРА

1. Бабич, А.В. Эффективная обработка информации/А.В. Бабич. - М.: Бином, 2014. - 223 с.

2. Остроух, А.В. Ввод и обработка цифровой информации: Учебник для нач. проф. образования / А.В. Остроух. - М.: ИЦ Академия, 2013. - 288 с.

С.К. Жумагулова, ст.преп.;
Е.А. Спирина, доц., канд. пед. наук;
М.А. Смирнова, ст.преп. (КарГУ им.Е.А.Букетова)

СОЗДАНИЕ ПРОГРАММЫ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ

Современное общество все в большей степени становится информационно-обусловленным, успех любого вида деятельности все сильнее зависит от обладания определенными сведениями и от отсутствия их у конкурентов [1].

В настоящее время особо актуальной стала оценка уже используемых криптоалгоритмов.

В созданном программном приложении происходит шифрование исходной информации методом прямой замены. Целью создания программного приложения является шифрование текстовой информации методом прямой замены. В системе должны быть предусмотрены средства контроля входной и результирующей информации, обновления данных в информационных массивах [2]. На рисунке 1 представлена главная загрузочная форма программы.

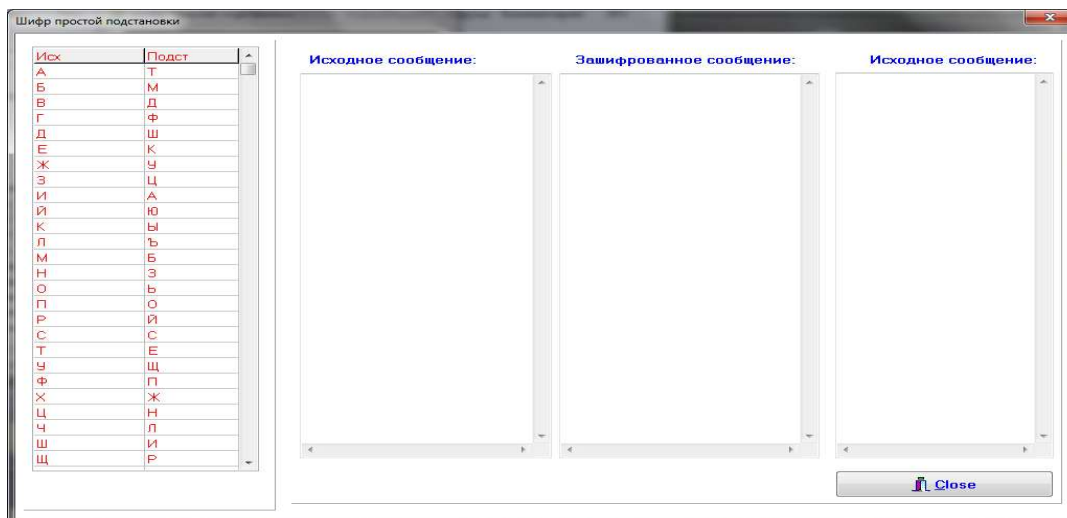


Рисунок 1 - Интерфейс программы

ЛИТЕРАТУРА

1. Петров, А.А. Компьютерная безопасность: криптографические методы защиты./ А.А.Петров. - Москва: ДМК, 2010. – 448 с.
2. Фаронов, В.В. Delphi 2011 Язык, среда, разработка приложений./ В.В.Фаронов. - Санкт-Петербург, 2011. – 322с.

ДЕШИФРИРОВАНИЕ ЛЕСНОЙ РАСТИТЕЛЬНОСТИ НА ОСНОВЕ СПЕКТРАЛЬНЫХ ИНДЕКСОВ

В настоящее время применение мультиспектральных данных дистанционного зондирования Земли (ДЗЗ) в совокупности с их соответствующей цифровой обработкой позволяет получать достоверную и подробную информацию о классах земной поверхности.

Цель наших исследований заключалась в выполнении анализа и оценке возможностей дешифрирования породного состава лесных насаждений по индексным изображениям, рассчитанным по данным ДЗЗ, полученным Белорусским космическим аппаратом (БКА).

Объектом исследования была выбрана территория биологического заказника «Оброво», расположенного в Ивановском районе Брестской области. Около 90% территории заказника занято естественной лесной растительностью. В структуре породного состава лесных сообществ доминирует сосна. К повышениям приурочены дубово-грабовые леса, в понижениях встречаются черноольховые и берёзовые леса. В исследованиях использовались космические снимки БКА с уровнем обработки спутниковых данных «С» - ортотрансформированные изображения в проекции UTM и системе координат WGS-84. (таблица 1).

Таблица 1 – Характеристика используемых материалов

Снимок	Спутник	Дата съёмки	Количество спектральных диапазонов	Пространственный охват	Пространственное разрешение
4047182-0220-MUL-C-1-1-1137973-160630T092525-VY	БКА	30.06.2016 г.	Синий – 0,45 – 0,52 Зеленый – 0,51 – 0,61 Красный – 0,64 – 0,70 Бл. ИК – 0,73 – 0,86	20 км	10,5 м

Имеющийся набор каналов позволяет производить расчет ограниченного количества индексных показателей. Однако, среди всего множества спектральных индексов наибольший интерес для интерпретации растительности представляют вегетационные индексы (ВИ), расчет которых базируется на двух наиболее стабильных участках кривой спектральной отражательной способности растений - красной и ближней ИК. В красной области спектра находится максимум поглощения солнечного излучения хлорофиллом растений, а в ближнем ИК диапазоне – область максимального отражения клеточных струк-

тур листа. Таким образом, здоровая, фотосинтезирующая растительность характеризуется меньшим отражением в видимой красной зоне и большим в ближней ИК. Отношение этих показателей друг к другу позволяет четко отделять растительность от прочих природных объектов.

Расчет индексных показателей производился в программном пакете EXELIS ENVI 5.2 при помощи инструмента алгебры каналов – Toolbox – Band Algebra – Band Math.

Всего по снимку БКА было получено 10 ВИ: разностный ВИ (DVI), относительный ВИ (Simple Ratio), преобразованный относительный ВИ (TSR), нормализованный разностный ВИ (NDVI), преобразованный нормализованный разностный ВИ (TNDVI), индекс глобального мониторинга окружающей среды (GEMI), ВИ устойчивый к влиянию атмосферы (ARVI), расширенный индекс озеленённости (EVI), почвенный ВИ (SAVI), модифицированный почвенный ВИ (MSAVI2) [1].

Общим для всех рассчитанных индексных изображений является четкая дифференциация лесной растительности на хвойную и лиственную (за исключением индекса ARVI). Перспективными с точки зрения выделения породного состава по данным БКА по результатам проведённого исследования являются индексы GEMI, Simple Ratio и TSR. – Индекс глобального мониторинга окружающей среды (GEMI) обладает большим разбросом значений (от +1,5 до -21000). Лесная растительность находится в интервале от -5000 до -14500. Значительная ширина диапазона позволяет путем эталонирования установить промежутки, наиболее характерные для определённых пород.

Относительный ВИ (Simple Ratio), а также преобразованный относительный ВИ (TSR) характеризуются поступательным уменьшением значений яркости при переходе от широколиственной к мелколиственной и хвойной растительности.

Таким образом, выполненные исследования показали, что по мультиспектральному снимку БКА наличие четырех спектральных каналов позволяет рассчитать 10 вегетационных индексов различной информативности, использование которых может способствовать повышению эффективности распознавания породного состава лесной растительности по данным БКА.

ЛИТЕРАТУРА

1. Жиленев, М. Ю. Обзор применения мультиспектральных данных ДЗЗ и их комбинаций при цифровой обработке / М. Ю. Жиленев // Геоматика. – 2009. – № 3. – С. 56-64.

УДК 004.9

К.М. Турдыбекова, ст. преп.; А.С. Шульгина-Тарашук, ст. преп.;
К.К. Турдыбекова, студ. (КарГУ им. Е.А. Букетова, г. Караганда)

ВЛАСТЬ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Успехи и достижения в области информационных и коммуникационных технологий показывают уровень развития страны в целом. Эта область нуждается в постоянном прогрессе, так как если мы не будем двигаться вперед и создавать все новые, более совершенные продукты, все нововведения вскоре станут обычными.

Информационные и коммуникационные технологии полностью изменили наш образ жизни. Появились новые рынки для поддержки ввода, хранения, обработки, анализа и представления информации, и этот процесс продолжает развиваться [1]. Информационные технологии стали рассматриваться как средство обеспечения позитивных сдвигов в социально-экономических условиях.

В Казахстане на уровне государства проводится большая исследовательская и практическая работа по их внедрению и развитию. Предполагается развитие направлений, которые серьезно изменят жизнь пользователей в ближайшие годы. Если осуществить градацию приоритета, получатся следующие виды технологий: развитие «облачных» вычислений; развитие интерфейса человек-машина; создание искусственного интеллекта; разработка и широкое распространение цифровых устройств на основе встроенных технологий распознавания речи и видеоизображений; развитие функциональных возможностей смартфонов и гаджетов, которые смогут распознавать речь на разных языках; внедрение высокотехнологичного производства, организованного без участия человека, управляемого роботизированными системами; распознавание изображений; развитие беспроводных сетей; виртуальная реальность, которая станет настоящей реальностью.

Интенсивное развитие новых информационных и коммуникационных технологий становится движущей силой экономических, социальных изменений в мире. Это оказывает значительное влияние на отношения между странами на мировом уровне.

Инновационная политика в сфере информационно-коммуникационной деятельности связана с подъемом всей экономики. Необходимо проанализировать информационно-коммуникационную деятельность, чтобы оценить возможные механизмы улучшения позиций страны на мировой арене. Существенную помощь в оценке оказывают статистические методы, использование которых помогает определить решающие факторы развития ИТ в стране, а также их взаи-

мосвязь. Необходимо стимулировать развитие науки, инноваций, использовать самые современные технологии производства, определяющих эффективность экономики.

В последнее время несомненно информационные технологии играют первостепенную роль в нашей жизни. Они обеспечивают конкурентоспособность страны и стабильный экономический рост.

Телекоммуникации, информационные технологии, цифровые медиа во всем мире подвержены постоянным, быстрым, кардинальным изменениям. Индустрия коммуникаций и новых технологий, проникающая во все сферы повседневной деятельности человека, является одной из наиболее значимых по степени влияния на нашу частную и трудовую жизнь, социальную сферу, экономику, имидж и статус страны в мировом сообществе. Международные исследования показывают, что существует тесная связь между развитием информационно-коммуникационных технологий и экономическим благополучием [2].

Прогресс в сфере новых технологий и инновационных услуг, рост информатизации, улучшение качества и удобства общения, появление социальных электронных порталов, доступность многих видов мультимедиа призваны способствовать повышению производительности труда, стимулировать создание новых предприятий и рабочих мест и в целом улучшать социальную сферу и качество жизни населения.

ЛИТЕРАТУРА

1. Илларионов С.И. Власть информации. - М.: ООО «РИЦ «ПрофЭко», 2013
2. Развитие отрасли Информационно-коммуникационных технологий (ИКТ) в России [Электронный ресурс]. - Режим доступа: <http://www.crn.ru/news/detail.php?ID=68520>.

M. Błaszczak, student (Lublin Catholic University, Poland);
 P.P. Urbanovich, prof. (BSTU, Minsk, Belarus)

**SERVER SECURITY OF THE MULTIPLAYER GAME
 «PROJECT I.G.I. 2: COVERT STRIKE»**

Secure of applications for multiplayer games is very important aspect for creators. The more expanded system requires a greater security level.

Often you can find systems of virtual money, payment. This is undoubtedly great opportunity for cybercriminals [1-2].

The modern games have really well protection of data and operations while elder games, which are still of interest to players, are exposed for various attack. The great part of games like those aren't supported by creators. Therefore users acquire control of security and create applications which support protection. The example of a game like that is "Project I.G.I. 2: Covert Strike". Creators stopped support servers of the game and because of that there have been many attacks and modifications which destroy the game.

One of the main ways to attack the server is sending false packet [3-4]. After analysis of a network traffic during the game you can observe the pattern of communication between the server and the gamer.

The following figure (fig. 1) shows an example of the most common packet format. After deciphering the contents of the packet you can easily compile your own data which may be dangerous for the server.

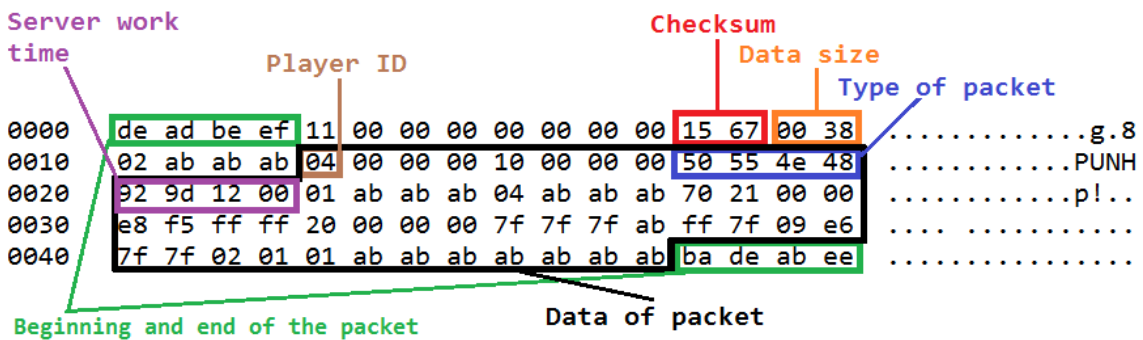


Fig. 1 – An exemplary format of a packet of communication between the server and the player

The most popular way to attack is overflow the buffer of a player name. In the game application user has restricted ability to set the name to 32 characters. However it isn't secure for server application. During sending the packet which is responsible for create the player, you can include

1000 characters long name. The server applications will try save that name in memory but specified character string is going to be too long what will result in a program error.

The next form of attack is “Format string attack”. It is based on misuse of arguments delegated to the following functions in language C which formats characters strings.

It’s hard to secure attacks which have been shown [3-5]. One of the ways to do that is creating system and accurate protection the server by the firewall. One of the elements of the system is application for players which is responsible for registrations, logging in and questions for access to the server.

The next element is application to the server which gives permission for the access, adds an exception to the firewall for a particular gamer and when he ends the game, the exception is going to be deleted. The firewall set to reject all of the packets from the outside is the crucial element.

Activity of the whole system may be show in that way:

- 1) registration with the e-mail address;
- 2) logging in to the application;
- 3) sending questions for the access to the server;
- 4) the application on the server checks players authenticity and adds the exception to the firewall with giving IP address and port which the player connects from;
- 5) after leaving the gave application deletes the exception from the firewall;

Thanks to this solution, the player is not able to send any crafted packets because he has no access. To protect the server more, you can set a server password that changes before each entry to the game. A player does not know it so there is no way to start an attack, because without the first packet in which the server password is sent, other packages will not be analyzed by the program. The extra solution is allocation the unique keys for every single player [4]. If any attack will be detected, you can lock adding access to a server for a player with the particular key. If a player registers again system will recognizes the previously used key and won’t allowed finish registration.

To secure server better you can use the algorithm which can detect the attack and lock it. A program like that one is able to work with servers log, that is a text file which includes register of the servers operations with exact date and hour. When a player enters a game the following line shows in the log:

"[20:30:42] Server info sent to 192.168.1.1:26015".

We download time and wait for the next line:

"[20:30:42]
[192.168.1.1:26015]".

NETWORKPACKET_TYPE_CLIENTCONNECT

If the time of saving in log is the same or there is one second difference it means sending packets by the attacking program. In a regular screenplay of entry to the game the difference of the time between those lines is minimum three seconds but mostly over 5 seconds.

The next proof for sending packets by the assailant are destination ports. If in both lines ports are different, it means that attacking packets were sending. This is due to the fact that the program created to attacks like that after each sending the packets is closed by the nest, this results in a change of port. The player who enters a game by the application sends all packets through the same port. Similar algorithm you can use during the analysis of network traffic which works faster.

In conclusion it must be said that to secure a server it is necessary to stock up on a system to control players. As an extra function it may be checking originality of the files to the game because there are a lot of modifications which disturb during playing the game.

REFERENCES

1. Pieprzyk, J. Teoria bezpieczeństwa systemów komputerowych/ J. Pieprzyk, T. Hardjano, J. Seberry. – Wydawnictwo Helion, 2003. – 595 s.
2. Paweł Urbanowicz, Marek Smarzewski. Bezpieczeństwo w cyberprzestrzeni a prawo karne/ Księga pamiątkowa ku czci Księdza Profesora Andrzeja Szostka MIC. – Lublin: Wydawnictwo KUL, 2016. – S. 489-496.
3. Urbanovich, P. P. Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii/ P.P. Urbanovich: ucheb.-metod. posobiye dlya stud. – Minsk: BGTU, 2016. –220 s.
4. Ochrona informacji w sieciach komputerowych / pod red. prof. P. Urbanowicza. – Lublin: KUL, 2004. – 150 s.
5. Makas, S. B. License Protection of a component of web-applications on .Net framework / S. B. Makas, P. P. Urbanovich // New Electrical and Electronic Technologies and their Industrial Implementation: proc. of the 5-th Intern. Conf., Zakopane, Poland.– Lublin. 2007. – P. 99.

P. Raб, student (Lublin Catholic University, Poland);
P.P. Urbanovich, prof. (BSTU, Minsk, Belarus)

METHODS, SOFTWARE AND HARDWARE TOOLS FOR CRYPTOCURRENCY TECHNOLOGIES

Cryptocurrency has been created and is managed by computer software and does not exist physically in any way. In other words, it is a currency used within software and created thanks to software as opposed to a specific physical currency [1].

The cryptocurrency market is growing stronger every year.

Bitcoin is one of the oldest and most popular cryptocurrencies. There is no owner or central control, here – all users are equal, in contrast to, for example, the general banking system, where there is a client-manager relationship. The source currency code is open and available to everyone.

Bitcoin is the first use of blockchain technology. The network is based on the digital record of transactions in the form of blocks of data, thus creating an identical database of transactions is distributed on many computers. Each computer that is a node in a peer-to-peer network (also referred to as P2P – can act as a client and server), has a copy of the collective transaction book in digital form. The verification consists in checking the value of the result with the value of input data by all network nodes and does not require as many resources as finding a solution that approves a given block containing transactions and attaches them to the block chain (fig. 1 [2]).

The idea behind the security of a distributed blockchain register is rewards in the form of cryptocurrencies for transaction authentication. The authentication process is also the process of assigning a new cryptocurrency to the owner and is called mining.

There are two types of algorithms for extracting cryptocurrencies: *Proof of Work* and *Proof of Stake*.

To present and analyze the basic methods of functioning of the most popular cryptocurrencies, based on blockchain technology, a web-application was created.

The site uses the most popular pattern for creating websites such as Model-View-Controller. The application consists of many functionalities such as: briefcase creation, adding new transactions, adding new network nodes and thus simulating the P2P network operation on which the Bitcoin cryptocurrency is based. To generate a wallet, we need a public and a private cryptographic keys [3-4].

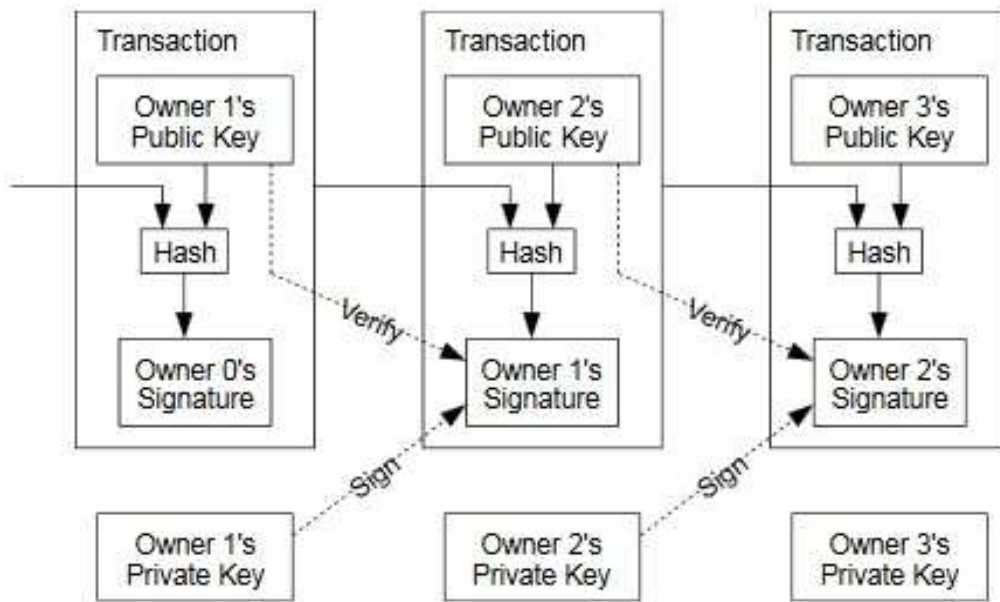


Fig.1 The blockchain technology implementation scheme [2]

When someone wants to send any cryptocurrency, they need a public key of the recipient, and more specifically a public address. Everyone can share it freely, because the only function that it fulfills is the ability to send funds from another wallet to it.

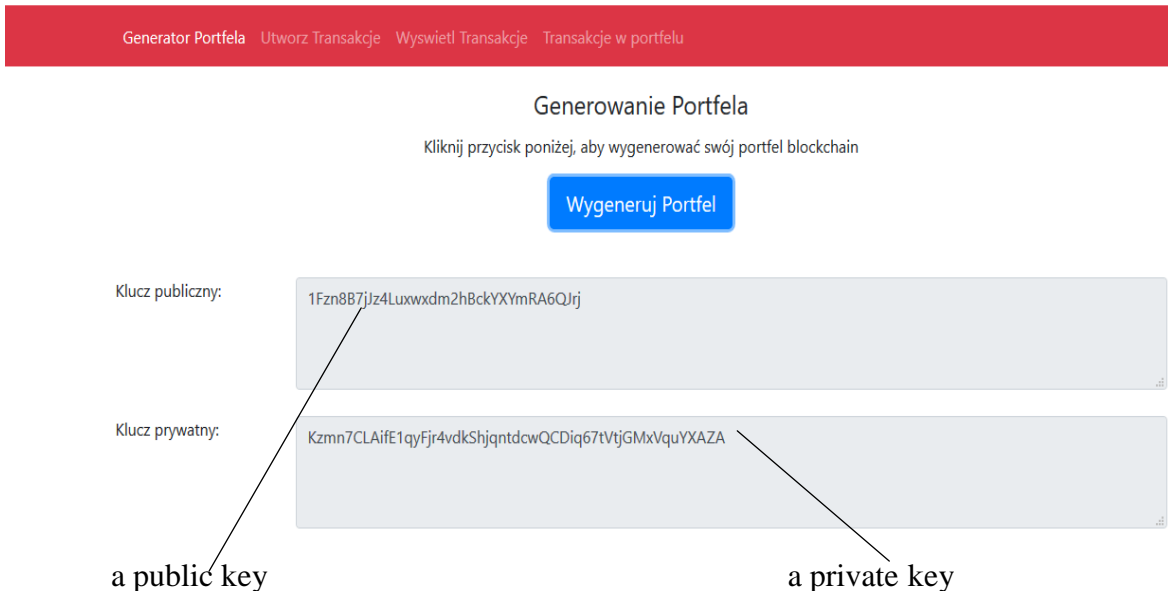


Fig.2 The screenshot of «The Briefcase Generation»

The private key, in addition to being our password, also serves to sign each transaction. Assuming that such a key should not be shared with anyone, the entire blockchain network is sure that the funds have been sent

by the owner of a given wallet. Figure 2 shows the appearance of the wallet page view.

A RSA algorithm was used to generate a pair of keys [3]. Another functionality is creating transactions that are saved in a blockchain. If the user wants to send to another person, some amount must have the recipient's public key. In the transaction, he must also provide his own public and private key.

Fig. 3 presents the appearance of the page for creating transaction

The last important functionality is the ability to trace the entire register of all transactions that have been recorded in the entire network.

Generator Portfela Utworz Transakcje Wyswietl Transakcje Transakcje w portfelu

Wprowadz szczegoly transakcji i wcisnij klawisz wygeneruj transakcje

Adres Wyslajacego:

Adres wysylajacego klucz prywatny:

Adres odbiorcy:

Kwota do wyslania:

Oplata za wydobycie:

Generuj transakcje

Fig.3 The screenshot of «The transaction Generation»

This register consists of the following information: recipient's address, sender's address, amount, transaction date, and block number.

REFERENCES

1. [Electronic resource]: <https://pl.dailyforex.com/forex-articles/2017/12/>. – Access date: 20.02.2019.
2. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system/ S. Nakamoto. – [Electronic resource]: <https://bitcoin.org/bitcoin.pdf>. – Access date: 20.02.2019.
3. Urbanovich, P. P. Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii/ P.P. Urbanovich: ucheb.-metod. posobiye dlya stud. – Minsk: BGTU, 2016. – 220 s.
4. Ochrona informacji w sieciach komputerowych / pod red. prof. P. Urbanowicza. – Lublin: KUL, 2004. – 150 s.

Научное издание

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
Материалы докладов 83-й научно-технической конференции
профессорско-преподавательского состава,
научных сотрудников и аспирантов
(с международным участием)
Электронный ресурс

В авторской редакции

Компьютерная верстка:
Н.А. Жиляк, Е.О. Черник

Усл. печ. л. 7,15. Уч.-изд. л. 7,38.

Издатель и полиграфическое исполнение:
УО «Белорусский государственный технологический университет».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий
№1/227 от 20.03.2014
Ул. Свердлова, 13а, 220006, г. Минск.