Секция
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

УДК 004.5; 159.937.7

Студ. Д. М. Талапина
Науч. рук. ст. преп. Н. И. Потапенко
(кафедра информатики и веб-дизайна, БГТУ)

ИСПОЛЬЗОВАНИЕ СИНЕСТЕЗИИ В ДИЗАЙНЕ

Синестезия – нейрологический феномен, при котором раздражение одной сенсорной или когнитивной системы ведёт к автоматическому, непроизвольному отклику в другой системе (раздражение одного органа чувств вызывает ощущения, соответствующие другому органу чувств).

Есть несколько распространенных видов синестезии, которые создают мультисенсорные ощущения при чтении, восприятии цвета, прослушивании музыки. Так же считается, что к синестезии склонен каждый человек, просто степень проявления данного феномена отличается из-за свойств психики и мозга человека, отсюда и вытекает идея данного исследования. Как наполнить свой веб-дизайн так, чтобы он стал более запоминающимся, благодаря мультисенсорным ощущениям?

Графемно-цветовая синестезия – восприятие буквы или цифры дополняются ощущением цвета [1]. Существует множество таблиц наиболее частых пар символ-цвет. Пример показан на рис. 1.

Рисунок 1 – Пример таблицы соотношения цветов и символов

Также нужно учитывать факт того, что различные начертания и гарнитуры могут вызывать различные синестезические ощущения (рис. 2).

Рисунок 2 – Пример мультисенсорного ощущения гарнитур

Мы также должны включить в наше понимание синестезии то, что она не связана с опытом или ассоциациями, поэтому не стоит опираться на основную теорию цветового восприятия. В отличие от фантазии и когнитивного бессознательного опыта, синестезия возникает непроизвольно и не меняется с годами. При проектировании своего

продукта исследователи рекомендуют избегать излишне агрессивных гарнитур (Trashka TYGRA, HussarLance-Bold, v_DirtyEgo, JK_Cold Night for Alligators и пр.), если вашей целью не является эмоциональное давление на пользователя. Применяйте правила копирайтинга и анализа текстовой информации (избегайте слов с большим количеством согласных или гласных подряд). Расположение текста в блоке так же имеет значение, придерживайтесь правил набора и верстки (трекинг и кернинг). Для начертания самих букв лучше использовать максимально нейтральные и привычные цвета, такие как: черный, белый, серый, синий. Яркие цвета должны уравновешиваться, согласно правилам.

Хроместезия – особенность восприятия, в результате которой звук окрашивается восприятием цвета [1]. Наиболее распространенной закономерностью при данном типе восприятия является соотношение частоты звуков и цветовых гамм. При проектировании своего медиа продукта необходимо учесть, что более низкие диапазоны ассоциируются с темной гаммой и могут вызывать нагнетающее или же успокаивающее действие на психику, а высокие частоты вызывают ощущение светлых и ярких цветов. Данные закономерности выведены не только среди синестетов, но и среди обычных людей.

В практической части работы будет использована хроместезия нейросети для подбора изображения, согласно цветовому разложению музыкальной волны, для создания видео (рис. 3).

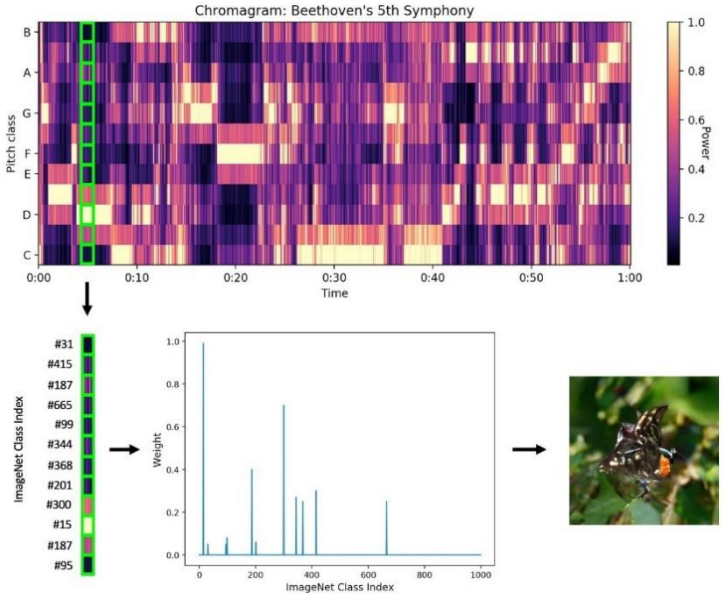


Рисунок 3 – Пример хроматографического разбиения 5-й симфонии Бетховена

Нейросеть [2] синхронизирует высоту звука с вектором класса изображений, а громкость и темп с вектором шума, так что высота звуковой волны управляет объектами, формами и текстурами в каждом кадре, а громкость и темп управляют движением между кадрами. В каждый момент времени в музыкальной композиции хроматограмма (диаграмма, полученная путем разделения сигнала по функции времени) двенадцати нот определяет вес каждой ($0 \leq 1$) для двенадцати классов изображений в векторе шума.

Помимо основных параметров видео (разрешение, длительность) для глубинной нейросети можно установить чувствительность к изменению темпа ($0 \leq 1$), она определяет скорость изменения вектора шума, соответственно большая чувствительность порождает более быстрое изменение изображений. Изменение параметра чувствительности к высоте звукового сигнала – это изменение вектора класса изображений к изменениям высоты звукового сигнала. При более высокой чувствительности к высоте волны мы получаем более быстрое и точное изменение основных параметров изображения (тона, текстуры и объектов). Для работы с данной нейросетью будем использовать модуль с открытым исходным кодом (взаимодействие со всеми классами и параметрами), написанный на языке программирования Python (visualize.py). Пример установки входных параметров с помощью консоли:

```
python visualize.py --beethoven.mp3--duration 60
--pitch_sensitivity 290 --tempo_sensitivity 0
```

Количество классов изображений (1-12) позволяет ограничить типы изображаемых объектов, которые будет обрабатывать нейросеть, для получения видео с использованием каких-то конкретных изображений. Классы синхронизируются с высотами в хроматическом порядке (A, A #, B…). Пример передачи параметров изображений с заданием приоритета встречаемости в видео:

```
python visualize.py --song cold.mp3 --duration 10
--pitch_sensitivity 260 --tempo_sensitivity 0.8 --
num_classes 2
--classes 985 107 --sort_classes_by_power 1
```

Наиболее важным параметром для визуализации быстрой современной музыки является характеристика длины кадра. Длина кадра – это количество сэмплов (небольших оцифрованных звуковых фрагментов) на видеокадр. Длина кадра 512 (по умолчанию) дает частоту кадров видео 43 кадров в секунду. Уменьшение длины кадра увеличи-

вает частоту кадров, поэтому изображение обновляется чаще (но рендеринг видео займет больше времени).

Таким образом, после ввода всех параметров и обработки нейросетью мы получаем готовое видео, которое можно считать хромосенестезическим воплощением некоторой музыкальной композиции. В дизайне данные видео полезно использовать для привлечения внимания пользователей, концентрации их внимания. Данный вид дизайна позволяет подарить мультисенсорные ощущения от увиденного и услышанного, что повышает эмоциональный отклик пользователя и позитивно сказывается на лояльности к нашему медиа продукту.

ЛИТЕРАТУРА

1. Шон Д. «Синестезия. Фундаментальные вопросы теории, искусства и науки». – Гранада, 2012. – 14 с.

2. Обучение GAN для синтеза естественных изображений с высокой точностью [Электронный ресурс]: статья. Режим доступа: https://arxiv.org/abs/1809.11096. – Дата доступа: 03.03.2020.

УДК 003.26

Магистрант М. Г. Савельева
Науч. рук. зав. кафедрой Д. М. Романенко
(кафедра информатики и веб-дизайна, БГТУ)

ОСАЖДЕНИЯ ИНФОРМАЦИИ В РАСТРОВЫЕ ИЗОБРАЖЕНИЯ МЕТОДАМИ СТЕГАНОГРАФИИ

Актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации. Современные компьютерные технологии, прогресс в области глобальных компьютерных сетей и средств мультимедиа обеспечивают возможность разработки и реализации новых методов, предназначенных для обеспечения компьютерной информационной безопасности. Компьютерные технологии придали новый импульс развитию и совершенствованию нового направления в области защиты информации – компьютерной стеганографии. Одна из самых новых горячих точек в исследованиях безопасности – это сокрытие информации. Она обусловлена двумя важнейшими проблемами информационной эпохи – защитой авторских прав и государственным надзором.

Помимо того, что сокрытие информации важно для защиты авторских прав и для любого долгосрочного решения спора о криптографических и правоохранительных органах, сокрытие информации также важно для конфиденциальности. Задача защиты информации от несанкционированного доступа решалась во все времена на протяже-

нии истории человечества. Можно выделить две причины популярности исследований в области стеганографии в настоящее время: ограничение на использование криптосредств в ряде стран мира и появление проблемы защиты прав собственности на информацию, представленную в цифровом виде. Первая причина повлекла за собой большое количество исследований в духе классической стеганографии (то есть скрытия факта передачи информации), вторая – еще более многочисленные работы в области так называемых водяных знаков. Цифровой водяной знак (ЦВЗ) – специальная метка, незаметно внедряемая в изображение или другой сигнал с целью тем или иным образом контролировать его использование [1].

Стеганография является эффективным программно-техническим методом сокрытия данных и защиты их от несанкционированного доступа. Но все же это лишь один из способов защиты информации. Эффективное использование стеганографии совместно с другими методами защиты информации обеспечит многоуровневую безопасность [2].

Цифровая стеганография – относительно молодая отрасль знаний, развитие которой принято отсчитывать с 90-х годов прошлого века. Несмотря на это, цифровая стеганография представляет несомненный интерес для специалистов, изучающих вопросы защиты информации, инженеров-проектировщиков средств защиты информации, а также специалистов в области теории информации и цифровой обработки сигналов.

По способу встраивания информации в изображения стегоалгоритмы можно разделить на линейные (аддитивные), нелинейные и другие. Алгоритмы аддитивного внедрения информации заключаются в линейной модификации исходного изображения, а ее извлечение в декодере производится корреляционными методами. При этом ЦВЗ обычно складывается с изображением-контейнером, либо «вплавляется» (fusion) в него. В нелинейных методах встраивания информации используется скалярное либо векторное квантование. Среди других методов определенный интерес представляют методы, использующие идеи фрактального кодирования изображений [3].

Одним из наиболее популярных методов встраивания информации в изображения является метод LSB. LSB (Least Significant Bit, наименьший значащий бит (НЗБ)) – суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека [4]. Выделяют два метода внедрения: LSB-R и LSB-M. LSB-R метод состоит в простой замене наименее

значащих битов яркости цветовой компоненты пикселя на информационный бит. Таким образом, в одном пикселе изображения при стандартной работе алгоритма мы сможем сохранить 3 бита. В случае с LSB-M идет не простая замена наименее значащего бита, а прибавление или вычитание единицы от байта компоненты цвета. Такая модификация предназначена для того, чтобы обходить автоматические проверки контейнеров на наличие в них скрытой информации.

Самый простой способ сокрытия информации в последовательности двоичных чисел – замена младшего значащего бита (LSB) каждого элемента одним битом секретного сообщения *m*. В арифметике с плавающей запятой вместо него можно использовать младший значащий бит мантиссы. Поскольку обычно размер скрытого сообщения намного меньше, чем количество бит, доступных для скрытия информации ($l(m) << l(c)$), остальная часть LSB может быть оставлена без изменений. Среди недостатков этого метода можно выделить следующие:

– скрытое сообщение легко разрушить, например, при сжатии;

– не обеспечена секретность встраивания информации. Точно известно местоположение зашифрованной информации. Для преодоления этого недостатка можно встраивать информацию не во все пиксели изображения, а лишь в некоторые из них, определяемые по псевдослучайному закону в соответствии с ключом, известным только законному пользователю.

За последние несколько лет предложены различные стеганографические методы, большинство из которых можно рассматривать как системы замещения. Такие методы пытаются заменить избыточные части сигнала секретным сообщением; их главный недостаток – относительная слабость против модификаций контейнера [1].

Существует множество гибких и простых методов встраивания информации в шумы каналов связи. Однако контейнеры и сообщения, как правило, имеют уникальные паттерны, которые мог бы использовать стеганалитик. Большинство простых приемов может быть нарушено тщательным анализом статистических свойств шума канал. Изображения и многие другие сигналы подвергались квантованию, фильтрам, преобразованиям, преобразователям формата и т. д. Большинство этих методов оставляют в данных своего рода «отпечатки пальцев».

Исходя из вышеперечисленного, направлением работы была выбрана модификация метода LSB. А именно, изменение компонента яркости цветового пространства YCbCr при работе с растровыми изображениями формата JPEG. Это обосновано тем, что при сжатии изображение преобразуется из цветового пространства RGB в YCbCr. После преобразования RGB → YCbCr для каналов изображения Cb и

Cr, отвечающих за цвет, может выполняться «прореживание». Таким образом, канал Y в данном случае не изменяется и подходит для осаждения информации. Интересным также является осаждение информации в виде относительных, а не абсолютных величин. Так, например, могут быть использованы различные методы яркостных преобразований (линейные, степенные), в результате чего будет увеличиваться (уменьшаться) разность значений яркости пикселей на границах объектов. Данные преобразования должны применяться для целой группы пикселей. При таком подходе стеганографическая система станет многоключевой: ключ, определяющий адреса пикселей, подлежащих изменению (аналогично методу LSB); ключ, задающий математическую зависимость, применяемую при выполнении яркостных преобразований; ключ, задающий среднее значения разности яркостей пикселов, входящих в область контрастирования; ключ, задающий минимальные (максимальные) отклонения от начальных (средних) значений яркости, которые будут восприниматься как 0 или 1. Предполагается, что для осаждения 1 бита информации будут использованы значения нескольких бит изображения.

ЛИТЕРАТУРА

1. Information Hiding Techniques for Steganography and Digital Watermarking. Ed. Stefan Katzenbeisser, Fabien A. P. Petitcolas. – London: Artech House, Inc., 2000. – P. 213.

2. Information Hiding – A Survey. Petitcolas, F. A. P., R. J. Anderson, and M. G. Kuhn. Proceedings of the IEEE, vol. 87, no. 7, Jul. 1999, pp. 1062–1078.

3. Хорев, А. А. Способы и средства защиты информации/ А. А. Хорев. – М.: МО РФ, 2000. – 316 с.

4. Урбанович П. П. Защита информации методами криптографии, стеганографии и обфускации / П. П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

УДК 004.9

Студ. Е. Р. Смирнов
Науч. рук. зав. кафедрой Д.М. Романенко
(кафедра информатики и веб-дизайна, БГТУ)

ОСОБЕННОСТИ РАЗРАБОТКИ ПРИЛОЖЕНИЯ «STUDYGO» НА ПЛАТФОРМЕ NODEJS

В наше время среди студентов популярностью пользуются сайты факультетов. Популярность данных сайтов достигается тем, что их использование очень помогает студентам в поиске новостей о жизни факультета, а также актуальной информации преподавателей факультета.

Для реализации веб-приложения используются следующие технологии и методы.

– Для разработки внешнего вида и логики сайта, должна быть использована библиотека React в связке с Redux и препроцессор Sass.

– Для хранения данных использовать MongoDB.

– Для связи визуальной части веб-сайта с серверной использовать платформу NodeJS в связке с фреймворком ExpressJS.

React – это инструмент для создания пользовательских интерфейсов. Его главная задача – обеспечение вывода на экран того, что можно видеть на веб-страницах. React значительно облегчает создание интерфейсов благодаря разбиению каждой страницы на небольшие фрагменты, называемые компонентами.

Компонент React – это, участок кода, который представляет часть веб-страницы. Каждый компонент – это JavaScript-функция, которая возвращает фрагмент кода, представляющего часть страницы [1]. Компоненты делятся на: «умные» и «глупые». Глупые служат для отображения статического контента страницы. «Умные» же компоненты служат для хранения и работы с состояниями.

По сути Redux – это инструмент управления как состоянием данных, так и состоянием интерфейса в JavaScript-приложениях. Redux предлагает хранить все состояние приложения в одном месте, называемом «store» («хранилище»). Компоненты «отправляют» изменение состояния в хранилище, а не напрямую другим компонентам. С Redux все компоненты получают свое состояние из хранилища. Можно отметить следующие ключевые моменты при работе с Redux:

1. Хранилище (store): хранит состояние приложения.

2. Действия (actions): некоторый набор информации, который исходит от приложения к хранилищу и который указывает, что именно нужно сделать. Для передачи этой информации у хранилища вызывается метод dispatch().

3. Reducer: функция (или несколько функций), которая получает действие и в соответствии с этим действием изменяет состояние хранилища [2].

Для разработки backend использовалась платформа Node.js [3]. С Node легко организовать масштабирование. При одновременном подключении к серверу тысяч пользователей Node работает асинхронно, то есть ставит приоритеты и распределяет ресурсы грамотнее.

Для веб-приложения «StudyGo» был выбран стиль material. Материальный дизайн – стиль графического дизайна интерфейсов программного обеспечения и приложений, разработанный компанией Google. Стиль расширяет идею «карточек», появившуюся в Google Now, более широким применением строгих макетов, анимаций и переходов, отступов и эффектов глубины (света и тени).

Перед созданием прототипов приложения «StudyGo», макетов и версткой страниц веб-сайта, необходимо разработать его структуру, определить необходимое количество страниц и систему связей между ними. Структура представлена на рис. 1. Приложение имеет древовидную структуру. Большое количество новостей и принуждает создать множество страниц, что может негативно отразиться на удобстве потребителя, если максимально точно не продумать структуру. В данном случае помогают различные фильтры, которые позволяют найти нужного собеседника в своих диалогах или выбрать нужное лабораторное занятие преподавателю, для выставления отметки за защиту лабораторной.

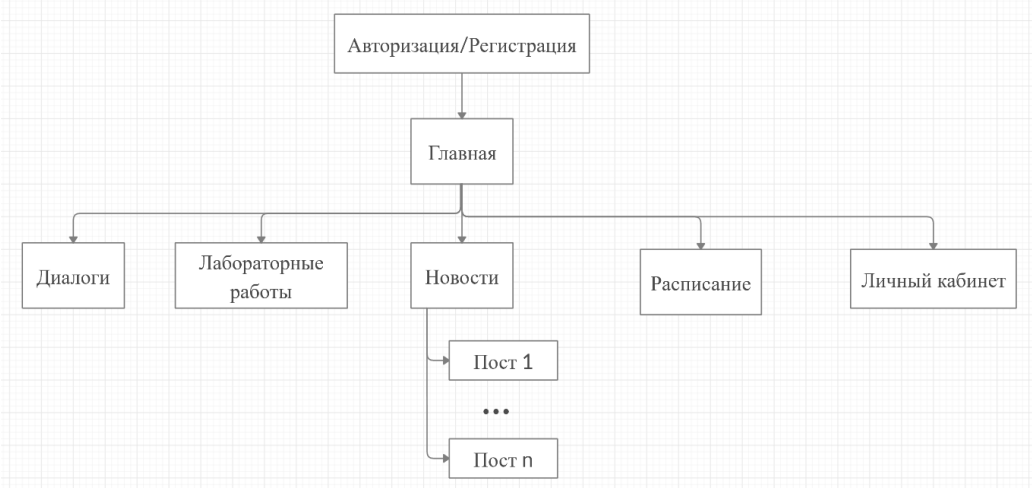


Рисунок 1 – Структурная схема веб-приложения «StudyGo»

При разработке веб-приложения использовалась база данных MongoDB [4]. База данных представлена в виде физического хранилища коллекций. Каждая БД имеет свой собственный набор файлов в файловой системе. Обычно, один MongoDB сервер имеет несколько БД (рис. 2).

Рисунок 2 – База данных веб-приложения «StudyGo»

В соответствии с поставленными задачами была разработана Use-case диаграмма для веб-сайта «StudyGo», представленная на рис. 3. В данной диаграмме имеется четыре актера: студент, преподаватель, декан, администратор.

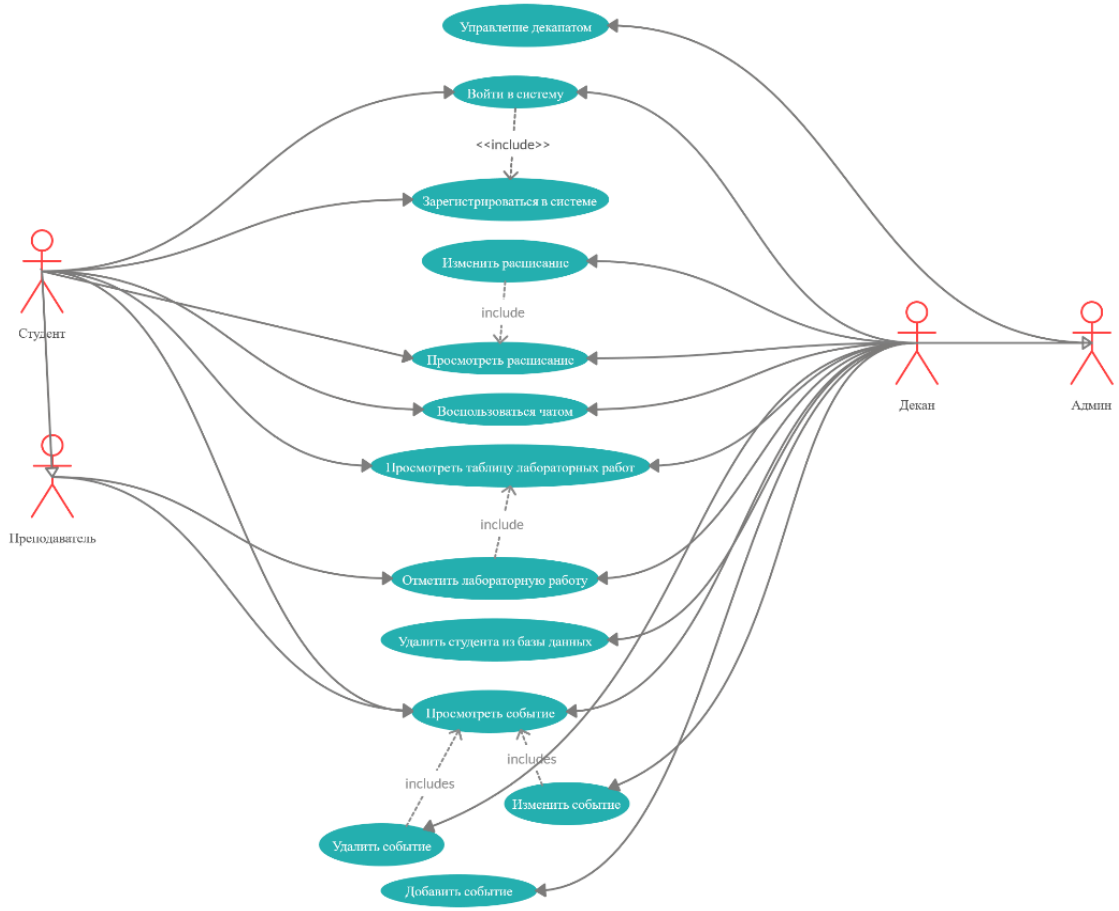


Рисунок 3 – Use-case диаграмма

Исходя из диаграммы, можно заметить, что доступное количество действий у актеров отличается. Студент может только просматривать контент, в то время как администратор может полностью редактировать его.

ЛИТЕРАТУРА

1. Основы React [Электронный ресурс]. / Сайт Habr, 2006-2019. – Режим доступа: https://habr.com/ru/company/ruvds/blog/343022/. – Дата доступа: 24.04.2020.

2. Redux [Электронный ресурс]. – 2014-2018. – Режим доступа: https://getinstance.info/articles/react/learning-react-redux/. – Дата доступа: 24.04.2020.

3. Что такое Node.js– [Электронный ресурс]. – 2011-2020. – Режим доступа: https://netology.ru/blog/node. – Дата доступа: 24.04.2020.

4. Руководство по MongoDB. – [Электронный ресурс]. – 2015-2020. – Режим доступа: https://proselyte.net/tutorials/mongodb/. – Дата доступа: 24.04.2020.

4. Что такое материальный дизайн. – [Электронный ресурс]. – 2013-2020. – Режим доступа: http://x-site.by/info/material-design. – Дата доступа: 24.04.2020.

УДК 76.021

Студ. Д. М. Талапина
Науч. рук. доц. О. А. Новосельская
(кафедра информатики и веб-дизайна, БГТУ)

ИСПОЛЬЗОВАНИЕ ШТРИХОВЫХ ЛИНИЙ В СОЗДАНИИ ОБРАЗОВ

Линия – протяжённый объект, представляющий собой цепь взаимосвязанных подобъектов, движущихся в пространстве между двумя точками, благодаря чему зритель может визуализировать движение, направление и намерение, в зависимости от того, как линия ориентирована и к какому типу она относится.

Линии описывают контур, детали, позволяют оценить соотношение и динамику объектов, могут быть использованы, чтобы задать, структуру, высоту, глубину, расстояние, ритм, движение и диапазон эмоций, текстуры и поверхности в соответствии с их длиной и кривизной.

Существуют разные типы линий: фактические, подразумеваемые, вертикальные, горизонтальные, диагональные и контурные. Все они имеют разные функции. Линии также являются ситуативными элементами, требующими от зрителя знания физического мира, чтобы

понять их гибкость, жесткость, синтетическую природу или натуралистичность.

В искусстве линия рисуется ручкой, карандашом, кистью или другим инструментом. Она имеет толщину, длину и является непрерывным знаком. Она может быть прямой, изогнутой или пунктирной и может варьироваться по толщине от одного конца к другому. Фактические линии – это те, которые физически присутствуют.

Экспрессивные линии имеют изогнутую форму, добавляя органический, более динамичный характер к произведению искусства. Экспрессивные линии часто округляются и следуют неопределенным путям.

Биоморфные линии – линии, которые воссоздают биологические или органические поверхности. Это негеометрические криволинейные линии используются для описания образов в более абстрактных типах сюрреалистической живописи и скульптуры [1].

Психологический отклик на разные типы линий:

- изогнутые линии предполагают комфорт и легкость;
- горизонтальные линии предполагают расстояние и спокойствие;
- вертикальные линии указывают на высоту и силу;
- неровные линии предполагают беспорядок и беспокойство.

Выразительные качества, определяемые путем рисования линии:

- линии от руки могут выразить личную энергию и настроение;
- механические линии могут выражать жесткий контроль;
- непрерывные линии могут вести глаз в определенных направлениях;
- пунктирные линии могут выражать эфемерное или несущественное;
- толстые линии могут выразить силу;
- тонкие линии могут выражать деликатность.

Линия может передавать тон и форму (рис. 1).

Рисунок 1 – Генри Мур «Овцы»

На рис. 1 лексика набросанных и заштрихованных линий, совместима с предметом. Кружащиеся линии соответствуют текстуре шерсти. Постепенно нарастает плотность линии, чтобы передать более темные тона, и уменьшается, чтобы передать более светлую область тона. На фоне работы используются заштрихованные линии, любое несоответствие их в общем стиле скрывается в плотном потоке кривых. В этой гравюре используется особый стиль многозадачности линий для выражения формы, тона и текстуры. У зрителя создается ощущение что линии сами являются клубком шерсти, который можно распутать взглядом.

Линии могут также передавать текстуру (рис. 2). Для передачи эффекта текстуры художники начинали с отдаленных черт фона, создавая изображение слой за слоем, пока они не закончатся на переднем плане. Дойг, однако, прорисовывает этот плотный узор «вуали» в начале процесса рисования и использует его для упорядочивания заднего плана, привлекая внимание к поверхности работы, развивая «лоскутное одеяло» [2] цвета и текстуры, которое фокусируется на абстрактных и выразительных качествах среды.

Линии часто используются для передачи динамики, движения (рис. 3).

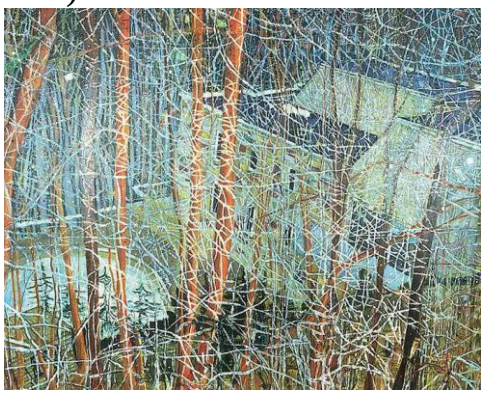


Рисунок 2 – Петер Дойг «Дом архитекторов в ущелье»

Рисунок 3 – Катсушика Хокусай «Великая волна у Канагавы»

На рис. 3 изгиб каждой волны усиливается контурными линиями, которые описывают ее плотность и объем. Сила этого движения еще больше усиливается лодками, которые изображаются спокойными, статичными горизонтальными линиями. Действие останавливается в критической точке для повышения драматичности и напряженности композиции.

Линия также является средством передачи эмоций (например, рис. 4). Зубчатые линии, изломанные формы и кислотные цвета задают отчаянный тон работы. Эмоции женщины усиливаются балансом смелых линий, преувеличенным цветом и упрощенным рисунком.

Пикассо использует яркие темные линии, чтобы объединить фрагментированное изображение и подавить оптический дисбаланс противоположных цветов.

Таким образом, линия хоть и является одним из базовых элементов художественной выразительности, она оказывает наибольшее влияние на создание целостного образа у зрителя, так как помогает объединить многие другие аспекты художественного выражения и усилить их.

В качестве практической части данного исследования были проведены некоторые манипуляции над одним и тем же объектом в программе CorelDraw, для определения того, как параметры инструмента «Художественное оформление» могут повлиять на общий образ, настроение и эмоциональный посыл изображения, при использовании

Рисунок 4 – Пабло Пикассо «Плачущая женщина»

одного и того же контура. Для данной работы был воссоздан контур девушки в профиль, достаточно нейтральный контур. К контуру были применены следующие вариации инструмента «Художественное оформление»: кисть каллиграфическая, кисть художественная, кисть физическая, кисть текстура, кисть разбрызгивание (рис. 5).

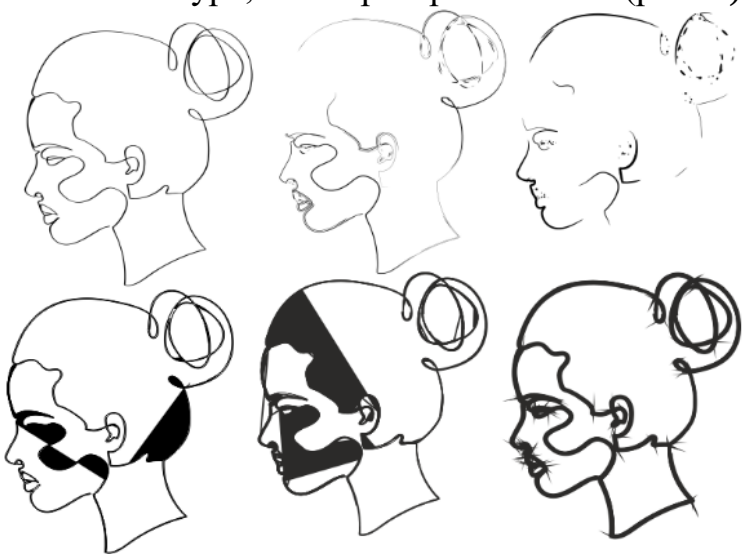


Рисунок 5 – Полученные образы

Первое изображение является оригинальным контуром. Образ характеризуется абсолютной эмоциональной нейтральностью. Образ легкий, за счет непрерывности линии и плавности переходов.

Второе изображение несет явную напряженность и некоторую строгость в лице девушки, за счет того, что некоторые линии стали двойными, в некоторые части добавился объем. Рваные и ритмичные линии придают изображению нарастающее напряжение, усиливающееся к чертам лица.

Третье изображение слегка потеряло свою структуру, из-за того, что линии стали каплеподобными. Из-за невозможности увидеть все черты лица, создается ощущение полуулыбки на лице девушки. Образ стал легче и романтичнее, сам по себе образ композиционно уравновешен.

Четвёртый и пятый образы мрачные, враждебные. Линии возле глаз ассоциируются со слезами. Композиционный вес данных образов намного больше веса оригинального контура, большая часть веса приходиться на лицо, отсюда теряется единство волос и лица, возникает композиционная асимметрия внутри самого контура.

Шестой образ меланхоличный, увесистый. Нет ощущения легкости или пустого пространства внутри контура, композиционно образ цельный и неразрывный, ассоциируется с клубком колючей проволоки.

Таким образом, не только порядок, плавность и ориентация линий в пространстве имеют важное значение для формирования цельного композиционного зрительного образа, но важен и сам тип этих линий.

ЛИТЕРАТУРА

1. Чалабаева, Ж. Линии в искусстве [Электронный ресурс]: лекции по искусству / Веб-сайт ArtBerries. – Режим доступа: https://artberries.kz/lectures/linii-v-iskusstve/. – Дата доступа: 23.03.2020.

2. Белая, Д. Питер Дойг – магия, абстрация, фотография [Электронный ресурс] / Сайт «Beatrice Magazine» – 2017. – Режим доступа: http://beatricemagazine.com/peter-doig/. – Дата доступа: 23.03.2020.

УДК 004.92

Студ. А. С. Леонова
Науч. рук. доц. О. А. Новосельская
(кафедра информатики и веб-дизайна, БГТУ)

РАЗРАБОТКА ВЕБ-САЙТА БРАСЛАВСКОГО ИСТОРИКО-КРАЕВЕДЧЕСКОГО МУЗЕЯ

Мы живем в эпоху стремительного развития информационных технологий. Так, глобальная сеть Интернет стала важной частью культурной жизни в целом и жизни учреждений культуры в частности. Музеи постепенно включаются в этот процесс.

Многие историко-краеведческие музеи, художественные галереи, музеи государственного, регионального, городского значения в стране и мире имеют свои веб-сайты. Это способствует знакомству с экспозицией и предоставляемыми музеями услугам большего количества людей, повышению посещаемости музеев в режиме реального времени. Однако зачастую взаимодействие посетителей с сайтом, поиск нужной информации могут быть затруднительными. Это может быть связано с неграмотно организованной подачей информации, непродуманным пользовательским интерфейсом, устаревшим дизайном и т.д.

Цели и задачи разрабатываемого веб-ресурса. В ходе разработки веб-сайта Браславского историко-краеведческого музея учтены данные моменты. Для разрабатываемого ресурса были поставлены следующие цели:

– знакомство посетителей сайта с экспозицией музея и его историей, численности фондов;

– предоставление информации о местонахождении музея, графике работы, стоимости посещения, вариантах экскурсий и прочих услугах, предоставляемых музеем.

Перед началом разработки был проведен поиск и анализ существующих решений в данной предметной области. Аналитический обзор способствовал формированию для веб-ресурса следующих задач:

– легкость доступа к информации;

– управление через интуитивно понятный интерфейс;

– информация на сайте должна быть тематически структурирована и разделена на отдельные блоки;

– возможность осуществления связи пользователя с администрацией музея посредством контактной формы;

– просмотр пользователями фондов экспозиционных залов музея, т.е. организация виртуального панорамного тура.

Структурная схема. Структуру сайта можно определить, как «Многомерная иерархия». Предусматривается большое количество элементов навигации, это позволяет каждой странице сайта быть доступной отовсюду [1]. Схема веб-сайта представлена на рис. 1.

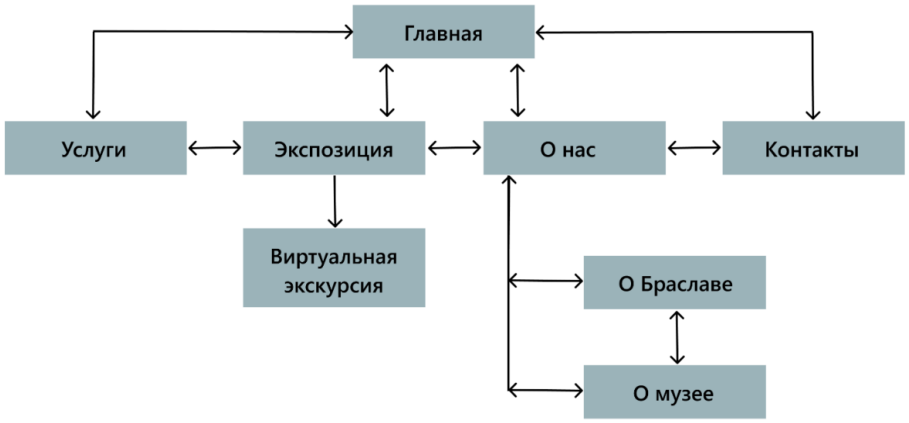


Рисунок 1 – Структурная схема веб-сайта

Веб-сайт музея состоит из следующих страниц: «Главная», «Услуги», «Экскурсии», «О городе», «О музее», «Контакты», а также виртуальный панорамный тур.

Интерактив и мультимедиа на веб-сайте. На сайте присутствуют следующие интерактивные и анимационные элементы: слайдер (страница «Услуги»); увеличивающиеся фотографии (страницы «О музее», «Экспозиция»); всплывающая подсказка (в футере страниц); форма обратной связи (страница «Контакты»); панорамный виртуальный тур по страницам музея (переход осуществляется со страницы «Экспозиция»); анимационный мультфильм о городе Браслав (страница «О Браславе»); видеофон (на странице «Экспозиция»).

Для анимации элементов сайта использовались анимации и трансформации CSS, JavaScript.

Страница «Главная». Содержит меню, состоящее из перечня всех страниц сайта, в футере страницы помещены ссылки на социальные сети, адрес музея со ссылкой на карту местности.

Страница «Услуги» содержит информацию о вариантах проводимых экскурсий, ценах, количестве человек в экскурсионной группе, информацию, о функционировании музея в настоящее время. Для придания странице динамичности, был разработан и размещен трехмерный анимационный ролик здания музея, созданный на основе двумерной фотографии. Ролик создан с помощью возможностей про-

граммного обеспечения для 3D-моделирования, анимации и визуализации Autodesk 3ds Max [2]. На рис. 2 показаны кадры готового анимационного ролика.

Рисунок 2 – Фрагменты анимационного ролика

Страница «О Браславе» содержит сведения об вариантах возникновения названия города, мультипликационный ролик на основании одной из версий. Кадры для анимационного ролика были отрисованы в программе Adobe Illustrator, движение элементов иллюстраций создано в Adobe After Effect, итоговый монтаж кадров и разработка аудиодорожки – в Adobe Premiere Pro. Кадр мультфильма представлен на рис. 3.

Рисунок 3 – Кадр мультипликационного ролика

Страница «О музее». Содержит описание истории музе, численности фондов и т.д., сопровождается фотоматериалами.

Страница «Контакты» содержит контактную информацию (номера телефонов, электронная почта), ссылки на социальные сети, форму для обратной связи, карту, с указанием расположения музея.

Страница «Экспозиция» содержит общее описание экспозиции музея и переходы на страницы экспозиционных залов. С данной страницы можно перейти на виртуальный панорамный тур, кликнув кнопку «Смотреть 3Д-тур». Пользователь попадает на страницу виртуальной экскурсии, где с помощью навигационной панели может осуществлять передвижение по зданию музея. Также организовано звуковое сопровождение, знакомящее пользователей с историей того или иного экспоната. На рис. 4 представлен вид страницы виртуальной

экскурсии экспозиционный зал № 1. Виртуальная экскурсия создана с помощью программного обеспечения Panotour Pro 2 [4].

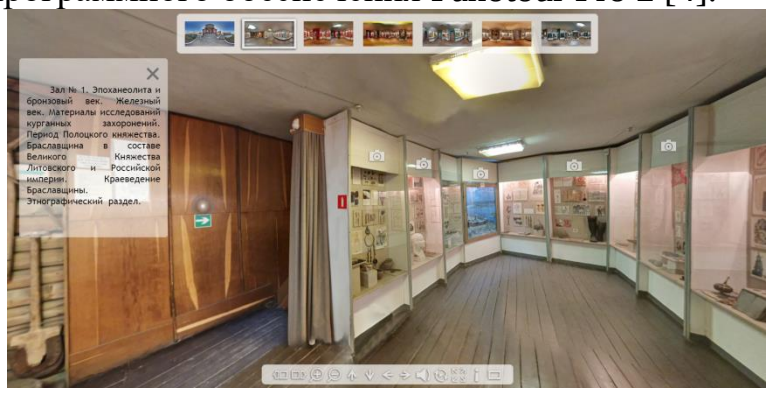


Рисунок 4 – Экспозиционный зал № 1

Заключение. Таким образом, предъявляемые к веб-ресурсу требования – легкость доступа к информации, управление через интуитивно понятный интерфейс, для чего информация на сайте была структурирована и разделена на отдельные блоки, внедрение интерактивных и мультимедийных методов, – полностью выполнены.

Конечно, не стоит забывать о таких достоинствах традиционных музеев, как живое общение с экскурсоводом, неповторимая атмосфера музейных залов, пропитанных духом истории, возможность вживую увидеть удивительные экспонаты. Однако, в случае возникновения непредвиденных обстоятельств, – грамотно организованный сайт музейной организации представляет собой достойную альтернативу посещению традиционного музея.

ЛИТЕРАТУРА

1. Брезгунова И.В. Основы веб-проектирования: учебно-методическое пособие. Мн.: РИВШ, 2013-125 с.

2. Estate [Электронный ресурс] / Трехмерная графика – 2015. – Режим доступа: http://esate.ru/article/cg/dizayn/trekhmernaya_grafika. – Дата доступа: 11.04.2020.

3. Анимация с помощью перекладки. [Электронный ресурс]: Режим доступа: http://nix-studio-edition.ru/tutorials/after-effects/1783-parent-tool-animation.html. Дата доступа: 11.04.2020.

4. Kaddr [Электронный ресурс] / Создание 3D тура в Panotour Pro 2 – 2015. – Режим доступа: http://www.opengl.org.ru/teachpro-web-dizain/ trekhmernaya-grafika.html. – Дата доступа: 12.04.2020.

УДК 004.92

Студ. М.Ю. Радченко
Науч. рук. доц. О.А. Новосельская
(кафедра информатики и веб-дизайна, БГТУ)

ОСОБЕННОСТИ ДИЗАЙНА И РАЗРАБОТКИ ВЕБ-САЙТА СВАДЕБНОГО АГЕНТСТВА «MARY»

Интернет развивается стремительно и сегодня большинство компаний имеют свои сайты. Иметь интернет-ресурс – необходимость современного мира. Сайт свадебного агентства – это не просто дань моде, а мощный и многофункциональный ресурс для развития бизнеса [1].

Свадебное агентство, в отличии от свадебного салона, предоставляет не только выбор платьев для невесты, но также и широкий ассортимент мужской одежды и аксессуаров, услуги уникального декора профессионалами, оригинальных идей флористов, визажистов и фотографов. Веб-сайт свадебного агентства – визитная карточка компании в сети Интернет. Красочное портфолио, современный лаконичный дизайн веб-страниц, наличие подробного описания оказываемых услуг поможет клиенту быстро ознакомится с агентством, понять, насколько ему близок стиль агентства организатора.

Владельцы свадебного агентства также должны понимать, что созданный единожды сайт со статичным контентом будет приносить пользу лишь на первых порах. Для поддержания конкурентоспособности сайта необходимо, чтоб его контент был актуальным, то есть обновляемым – возникает необходимость в панели администратора, в которой будет возможность управлять контентом.

Процесс разработки веб-сайта включает в себя следующие этапы: постановка целей и задач; создание, проработка технического задания на разработку сайта; прототипирование; создание макета дизайна сайта; верстка; программирование; наполнение контентом; тестирование; сдача готового проекта клиенту.

Каждый ресурс компании должен тем или иным способом приносить деньги фирме, и веб-сайт не является исключением. Таким образом цели веб-проекта свадебного агентства прямым или косвенным образом отвечают именно за увеличение прибыльности компании.

Целями создания веб-проекта свадебного агентства являются:

– привлечение большего количества клиентов агентства;
– формирование клиентской базы;
– представление компании в интернете;
– формирование положительного имиджа в интернет-сообществах;

– увеличение количества продаж товаров и услуг;
– упрощение обратной связи и процесса представления услуг;
– возможность неограниченной демонстрации.

Важным этапом разработки является анализ конкурентов, который помогает понять ситуацию в отрасли, найти свою нишу и понять, в каком направлении развиваться. Проанализировать удачные решения и ошибки конкурентов, можно определить, что в данном сегменте рынка пользуется популярностью и что нового можно предложить, оценить потенциал интернет-проекта как инструмента получения прибыли [2].

Изучив современные тенденции в дизайне, можно сделать вывод, что в последнее время наблюдается уход от явно выраженных сложившихся стилей к эклектике – смешению, соединению разнородных стилей, идей, взглядов и т. п. Веб-проект свадебного агентства также не является типичным шаблоном какого-либо направления в веб-дизайне, он включает в себя элементы различных стилей.

Сайт содержит элементы классического стиля: хедер с логотипом, названием агентства, краткими контактными данными; горизонтальное меню; футер, содержащий меню, информацию о правах, контактную информацию.

Так как основные ассоциации, возникающие со словом свадьба, – это легкость, воздушность, счастье, то большое внимание при дизайне проекта уделяется негативному пространству, которое сможет обеспечить «легкость» сайта. С понятием негативного пространства граничит такой стиль веб-дизайна как минимализм. Важно уловить грань между свободным пространством и пустотой. В процессе разработки дизайна сайта происходит отказ от анимации, большого количества фонов и текстур, слишком широкой цветовой палитры и тому подобного.

Для создания прототипов используется программа Axure RP Pro 7.0 – самая известная и популярная программа по созданию прототипов веб-сайтов и приложений. В процессе создания макетов были учтены свойства композиции. Каждая из страниц оформлена в едином стиле.

Разработки дизайна веб-проекта включает в себя разработку логотипа агентства, выбор шрифтов и цветовых схем, написание правил их использования. На рис. 1 представлен разработанный логотип на допустимых фонах в соответствии с выбранной цветовой схемой.

Рисунок 1 – Допустимые цветовые вариации логотипа и фона

Этап дизайна завершается разработкой дизайн-макетов в программе Adobe Photoshop. На рис. 2 представлен фрагмент дизайн-макета страницы «О нас».

Функционал веб-сайта свадебного агентства «Mary» включает: отображение общей информации об агентстве, контактных данных, списка предоставляемых услуг и их описание с фотографиями, красочное портфолио, слайдер с фотографиями и видео, форму обратной связи для записи на оказание услуг агентства, новостной блог статей по теме свадебных торжеств, визуализацию выбора свадебного наряда для невесты. К функционалу панели администратора относится: просмотр всех статей, отзывов, свадеб (единиц портфолио), а также создание нового контента, редактирование и удаление существующего, просмотр сообщений, отправленных через форму обратной связи.

Рисунок 2 – Фрагмент дизайн-макета страницы «О нас»

Для разработки адаптивного веб-сайта свадебного агентства и панели администратора для его управления используются следующие веб-технологии:

– язык гипертекстовой разметки HTML для определения структуры страниц веб-сайта, которую пользователь видит в окне браузера;

– каскадные таблицы стилей CSS для определения стилей документов, в том числе дизайна, верстки и вариаций макетов сайта для различных устройств и размеров экрана [3];

– JavaScript для написания сценариев;

– AngularJS для такой функциональности, как Ajax, управление структурой DOM, анимация, шаблоны, маршрутизация и так далее;

– библиотека JQuery для добавления интерактивности и анимацию на веб-сайт;

– язык PHP для динамического формирования страниц на основе информации из базы данных;

– MySQL для создания базы данных, в которой будут хранится все необходимые для корректного функционирования веб-сайта данные, для ее управления и выборки записей из базы.

Таким образом, созданный веб-сайт имеет хорошо структурированный контент, единую стилистику всех страниц, он привлекателен и приятен для пользователей. Сайт понятен и прост в изучении, расположение блоков интуитивно понятно. Перечисленные выше факты способствуют увеличению количества посещений сайта, а, следовательно, и увеличению клиентов агентства. Сайт разработан с возможностью расширения информации и добавления нового контента.

ЛИТЕРАТУРА

1. Колисниченко Д. Н. Интернет от «чайника» – к пользователю: 3-е изд., перераб. и доп./ Д. Н. Колисниченко – СПб: БХВ-Петербург, 2012. – 512 с.

2. Зачем нужен анализ конкурентов в вебе [Электронный ресурс] / Независимый проект брендингового агентства Depot – 1998-2020. – Режим доступа: https://www.sostav.ru/publication/soperniki-kak-luchshie-pomoshchniki-v-postroenii-strategii-18349.html. – Дата доступа 20.03.2020.

3. Зачем нужен CSS? [Электронный ресурс] / MDN web docs. 2005–2020. – Режим доступа: https://developer.mozilla.org/ru/docs/Web/Guide/CSS/ Getting_started/Why_use_CSS. – Дата доступа: 12.04.2020.

УДК 004.5; 766

Студ. А. А. Корделюк, Т. А. Коротыш
Науч. рук. ассист. С. А. Осоко
(кафедра информатики и веб-дизайна, БГТУ)

НОВЫЕ ТЕХНОЛОГИИ В WEB

В индустрии веб-разработки все меняется очень быстрое. Сегодня одна технология на пике развития, а завтра она уже не востребована. Поэтому необходимо следить за тенденциями разработки новых платформ, элементов, технологий и других инструментов, набирающих популярность, имеющий наибольший потенциал и перспективы роста.

На сегодняшний день, представителями таких технологий являются: PWA, боты, искусственный интеллект, блокчейн, MotionUI, PHP 7, SSL протокол и HTTPS и многие другие.

Progressive Web Apps (PWA – прогрессивные веб-приложения). Прогрессивные веб-приложения нового поколения (PWA) собрали информацию о лучшем пользовательском опыте и воплотили это в мобильных приложениях. PWA – это веб-приложения, которые по ощущениям и пользовательскому опыту напоминают мобильные приложения. Они собирают новейшие веб-технологии в удобной для пользователей форме, доступ к которым пользователь может получить в любое время с помощью закладок (URL) или панели расширений любого современного браузера. Благодаря работе сервисных служб, не зависят от состояния сети, а с предварительным кэшированием они доступны пользователям даже в автономном режиме.

Недостатками этой технологии является высокая стоимость разработки и много усилий, которые прилагаются к их созданию.

Чат боты (chatbot) и искусственный интеллект – это компьютерная программа, основанная на достижениях машинного обучения и обработки естественного языка, помогающая людям в выполнении определенных задач и имитирующая взаимодействие с реальным собеседником. Типичными задачами, с которые могут помочь боты, являются покупка, поиск определенной информации или заказ услуги. Боты оказывают помощь в форме «вопрос-ответ», создавая ощущения общения с человеком. Рассмотрим несколько примеров:

– Nikabot – инструмент для контроля рабочего процесса. Он опрашивает сотрудников, чем они занимаются, и на основе полученных данных создает для руководства информативный интерактивный отчет о проделанной работе.

– Geekbot – более продвинутая версия ассистента для организации рабочих совещаний. Бот задает ряд вопросов о рабочем статусе и распознает взаимосвязи сотрудников между задачами. Недостатком, по сравнению с Nikabot, является отсутствие подробного анализа проделанной работы.

– Ace. Удобный и функциональный планировщик задач. умеет составлять списки задач, и делегировать задачи другим сотрудникам и проводить командные опросы. Чтобы поставить задачу, достаточно написать в начале предложения слово todo.

В настоящее время боты преобладают в работе мессенджеров, таких как Facebook Messenger (более 100 тысяч ботов), Telegram, Kik, Skype, WeChat и т. д. У некоторых крупных компаний есть свои боты, (H & M, Sephora, Hilfiger и др.). Включение ботов считается будущим мобильных приложений. Крупные игроки создали свои бот-платформы и инструменты с открытым исходным кодом, чтобы сделать создание бота еще более доступным.

Блокчейн (blockchain) – это быстро развивающаяся технология, которая трансформирует всю суть бизнеса. Первоначально эта технология поддерживала цифровую валюту Bitcoin, но теперь для нее нашли много других применений, и она стала действительно революционной.

Суть технологии блокчейн заключается в использовании общей базы данных, которая постоянно согласовывается. Миллионы компьютеров содержат записи базы данных, которые обновляются каждые десять минут. Поскольку данные разбросаны по большому количеству компьютеров, и нет никакой команды, контролирующей, невозможно испортить или нарушить функционирование системы. Чтобы уничтожить блокчейн, требуется уничтожать все ПК, которые могут хранить данные или же отключать Интернет.

Блокчейны позволяют создавать цепочки поставок, обеспечивают децентрализованное хранение файлов и автоматическую защиту интеллектуальной собственности. Они открывают новые перспективы для онлайн коммерции и краудфандинга.

Motion UI – анимация и переходы. Библиотека Motion UI позволяет мгновенно анимировать пользовательский интерфейс вашего сайта используя motion-дизайн.

Пакет библиотеки включает в себя файл CSS с готовыми эффектами, а также файлы, которые позволяют вам создавать собственные анимации. Библиотека позволяет пользователям перемещать элементы сайта (наложения, меню и т. д.). Кроме того, возможно использовать эффекты перехода для создания одиночных анимаций CSS и даже ряды и группы анимаций.

PHP 7. PHP работает на 82,4% всех сайтов. В 2017 году вокруг него поднялся шум в связи с выпуском PHP 7.

В версии PHP 7 появились новые операторы и функции, классы, интерфейсы и глобальные константы. В нем были внесены изменения в функции и модули SAPI. Эти изменения позволили:

– значительно увеличил производительность. Он компилирует код в машинный язык, используя быстродействующий движок Just In Time (JIT). С этим движком он в 2 раза быстрее, чем PHP 5.6. В то же время с PHP 7 база кода использует гораздо меньше памяти;

– использует новые описания типов (дескрипторы). Это значительно упрощает чтение и понимание кода;

– не выдает пользователям белый экран, если они сталкиваются с ошибкой. Вместо этого он генерирует исключение без остановки всего скрипта.

SSL протокол и HTTPS (Secure Socket Layer) – это технология, которая обеспечивает установление зашифрованного соединения между браузером и веб-сервером, что обеспечивает целостность данных, шифрование и аутентификацию.

Переход на SSL-сертификат приносит следующие преимущества:

– защищает конфиденциальную информацию пользователей и позволяет им совершать транзакции без риска потери данных. Поэтому он повышает доверие пользователя и помогает вам получать максимальный доход;

– позволяет исключать предупреждения браузера, которые сообщают пользователям, что их данные не защищены на вашем сайте;

– повышает репутацию вашего бизнеса в глазах поисковиков (Google отдает преимущество сайтам на HTTPS);

– уменьшает риск фишинга и других кибератак.

Сегодня набирают популярность такие технологии как нейронные сети, голосовое управление, интернет вещей, виртуальная и дополненная реальности, машинное обучение. Однако с течением времени эти технологии продолжат развиваться, поэтому необходимо постоянно отслеживать этот процесс.

ЛИТЕРАТУРА

1. Новости, тенденции и тренды веб разработки в 2020 году [Электронный ресурс]: статья. – Режим доступа: https://www.moto-cms.com/blog/ru/trendy-web-razrabotki/. – Дата доступа: 03.03.2020.

2. Тренды веб разработки 2020 [Электронный ресурс]: статья. – Режим доступа: https://merehead.com/ru/blog/web-development-trends-in-2020/. – Дата доступа: 03.03.2020.

УДК 004.5

Студ. М. И. Гундарева, А. А. Виленская
Науч. рук. ст. преп. Т. В. Кишкурно,
(кафедра информатики и веб-дизайна, БГТУ)

ЮЗАБИЛИТИ ИНТЕРФЕЙСОВ СОЦИАЛЬНЫХ СЕТЕЙ

Благодаря развитию компьютерных и мобильных технологий социальные сети прочно вошли в нашу повседневную жизнь. Каждый раз, переходя из одного приложения в другое, из одной вкладки социальной сети в другую мы так легко находим нужные пункты, ссылки или настройки в совсем разных социальных сетях. Неужели мы все так быстро запоминаем, несмотря на то, что не можем запомнить простую тему по предмету в университете или это дело привычки? Конечно, мы не исключаем привычные движения, но что говорить, когда вы легко разбираетесь или регистрируетесь в совершенно незнакомой социальной сети, почему вам так легко адаптироваться и понять ее интерфейс? Мы постараемся ответить на эти вопросы. Для нашего исследования мы взяли четыре социальные сети: Твиттер, Facebook, ВКонтакте, LinkedIn.

При разработке интерфейса на всех этапах проектирования важно знать и не забывать, что как пользователь видит интерфейс, так он и воспринимает весь продукт в целом. Таким образом, если программа не удобна, то она и бесполезна во всех проявлениях, особенно это важно для социальных сетей и игр, где конкуренция очень велика.

По мнению Якоба Нильсена, удобство использования, или юзабилити, определяется пятью ключевыми компонентами: обучаемость, эффективность, запоминаемость, ошибки, удовлетворенность.

Для повышения юзабилити в этих критериях используются уже понятные или сформированные представления об определенных ссылках и понятиях. Так, например, для профиля используется уже привычный кружок с фотографией или инициалами (табл. 1), которые распространены почти повсеместно.

Таблица 1 – Вид изображения профиля в соцсетях

							
Твиттер	Facebook	ВКонтакте	LinkedIn	Google	Яндекс	Яндекс почта	Instagram

Другой пример – значок «сообщения», который очень хорошо ассоциируются с конвертом или «диалогом» между людьми (табл. 2). Стилизацию картинок-конвертов используют многие электронные почты: Яндекс Почта, Gmail, Mail.ru и т.п.

Таблица 2 – Примеры значков сообщений

						
Твиттер	ВКонтакте	LinkedIn	Facebook	Mail.ru	Gmail	Яндекс Почта

Неизменным и почти не стилизованным остается еще один раздел – уведомления. В рассматриваемых нами социальных сетях роль иконки для уведомления играет колокольчик. Но на первые три критерия юзабилити влияют не только очень похожие иконки, но и расположение отдельных элементов, таких как строка поиска, кнопка выхода, панель меню, основная лента, логотип сети, количество колонок и многое другое. Так, например, во всех браузерах при поиске нужной страницы строка поиска расположена в самом верху страницы. Эту черту переняли и социальные сети, у которых строка поиска расположена в шапке на одной линии с логотипом, причем логотип находится левее строки поиска. Можно с уверенностью сказать, что никто не любит делать ошибки, как в реальной жизни, так и в виртуальной. Поэтому чтобы избежать мелких ошибок – дизайнеры стараются просчитать их при проектировании и сделать все более понятным и удобным. Но даже при таком условии ошибок избежать практически невозможно. Для того, чтобы минимизировать количество ошибок, нужно плавно обучать пользователей в процессе работы и снижать чувствительность системы к ошибкам. Т.к. последнее очень сложно достижимо и проводится на стадии разработки, то проще постараться обучить пользователей.

Для обучения можно использовать несколько подходов: составить бумажную документацию, сделать справки и подсказки, использовать метафоры и стандарт. Для социальных сетей чаще используется стандарт. Это самый мощный способ обучения. Например, продукты Adobe. Хоть программы продукта Adobe выполняют разные функции, но пользовательский интерфейс одинаковый. Социальные сети построены по тому же признаку: в рассматриваемых социальных сетях используется одинаковое количество колонок, названия разделов соответствует во всех социальных сетях своим функциям, расположение строки поиска, меню, ссылки на страницы, расположение новостной ленты и многое другое.

О пятом критерии (удовлетворенности) мы не можем говорить определенно. Ведь сколько людей, столько мнений и предпочтений. Но легкость и простата никогда не выходят из моды. Так простой и красивый синий цвет не раздражает взгляд, может принести приятное спокойствие пользователям. Данный цвет также способствует физическому расслаблению и создает атмосферу безопасности и доверия. В

дизайне социальных сетей присутствует также и скругленные углы блоков, строки поиска и логотипа, что говорит о безопасности, привычности (округлые формы встречаются чаще острых). Ну и конечно минимальное количество оттенков и излишних деталей.

Во время написания работы мы провели опрос, в котором предлагали участникам стать дизайнерами новой социальной сети. Им предлагалось выбрать цвет, расположение некоторых деталей (логотип, кнопка выхода, строка поиска, меню), форму картинки профиля, количество колонок и то, какие разделы они бы хотели видеть в социальной сети.

Мы заметили, что на критерии выбора никак не влияли пол и возраст участников опроса. И так – почти 77% выбрало круглую форму для картинки профиля (аватарки), что свидетельствует о привычке и удобстве такого профиля. Мы почти не были удивлены, когда все участники опроса выбрали расположение поисковой строки в самом верху страницы, как мы и упоминали раньше, говоря о стандартах и частоте использования тех же поисковых страниц (как эталона). Почти 48% выбрало расположение логотипа слева около строки поиска и 28% – просто левый верхний угол страницы. Мы упоминали выше о скругленных формах, и 97% выбрало круглые и скругленные формы и только 3% квадратные. При выборе цвета будущей социальной сети, 62% выбрало синий цвет, 28% – черный, 7% – зеленый и только 3% – желтый, но вот более агрессивные цвета (красный и фиолетовый) никто не выбрал.

Мы можем сделать вывод, что при проектировании новой сети для легкости восприятия и обучения необходимо использовать общепринятые нормы, часто используемые формы, картинки и привычки. Не стоит изобретать велосипед заново, проще изменить то, что будет доступно многим, если конечно вы не задумали изменить вообще представление обо всем.

ЛИТЕРАТУРА

1. Брусенцова, Т. П. Проектирование интерфейсов пользователя: пособие для студентов специальности 1-47 01 02 «Дизайн электронных и веб-изданий» / Т. П. Брусенцова, Т. В. Кишкурно. – Минск: БГТУ, 2019. – 170 с.

2. Судольский Р. 15 самых популярных социальных сетей мира [Электронный ресурс] / Интернет-журнал AIN.UA. – 1999-2020. – Режим доступа: https://ain.ua/2014/06/09/15-samyx-populyarnyx-socialnyx-setej-mira/. – Дата доступа: 12.03.2020.

3. Лина Стопятюк. 5 основных цветов в веб-дизайне [Электронный ресурс] / Интернет-издание о творчестве Say hi – 2020. Режим доступа: https://say-hi.me/design/web-design/5-osnovnyx-cvetov-v-veb-dizajne.html. – Дата доступа: 12.03.2020.

УДК 004.5

Студ. Э. И. Хорова
Науч. рук. ст. преп. Т. В. Кишкурно
(кафедра информатики и веб-дизайна, БГТУ)

БЕЗБАРЬЕРНЫЙ ДИЗАЙН

Интернет-пространство развивается в геометрической прогрессии. Пользователи перенасыщены уникальными дизайнами и сложным функционалам. Разработка и проектирование веб-сайтов с каждым годом всё больше соответствует принципам usability, однако красота и удобство не единственные факторы, на которые стоит обратить внимание в 21 веке. Одним из принципов проектирования становится доступность интернет-среды.

Безбарьерный дизайн – термин применяется к элементам визуальной среды, в которой могут свободно ориентироваться и использовать люди с физическими, сенсорными или интеллектуальными нарушениями. Если говорить о веб-ресурсах, то наиболее уязвимой группой являются люди, с нарушением зрительного аппарата.

По статистике Республики Беларусь на сегодняшний день насчитывается около 50 тысяч инвалидов по зрению. В мире социальной коммуникации сложно представить жизнь без возможностей всемирной паутины, но, к сожалению, около 70% веб-сайтов не соответствуют нормам доступности.

Доступность веб-ресурсов должна закладываться при проектировании интерфейса, однако существуют способы повышения доступности на уже готовых, функционирующих сайтах. Далее рассмотрим несколько правил повышения доступности на веб-сайтах.

Первое правило – реализация масштабируемой вёрстки сайта. Этот способ актуален не только для инвалидов по зрению, но и для плохо видящих людей. Масштабируемая верстка будет полезна и для массовых пользователей – например, когда они заходят на сайт с устройства с маленьким экраном. Увеличить масштаб сайта на экране компьютера или телефона – самый простой способ повысить видимость информации. Масштабируемая верстка придает эстетичность верстке, а также является одним из проводников доступности.

Далее следует правило контрастности текстовой информации и фона. Важно, чтобы основной текст на сайте можно было легко прочитать с экранов разной яркости и качества. Также существует множество людей с различными нарушениями зрения. Например, пользователи с расстройствами цветового зрения просто не увидят текст или смогут разглядеть его с большим трудом, если он не будет контрастен

фону. Часто при разработке не принимают во внимание эту рекомендацию в погоне за красивым дизайном, моно-стилем, а потом оказывается, что текст на сайте сложно читать.

Удовлетворительной доступности можно достичь без исправления верстки всего сайта. Одним из таких решений является панель для слабовидящих, которая решает вопрос с контрастностью и размером шрифта. С помощью нее можно добавить функции, которые удовлетворят потребности людей с ограниченными возможностями – например, возможность настроить отображение цвета на сайте поможет людям с дальтонизмом, а увеличение интервалов между буквами и строчками, а также настройка шрифта с засечками – людям с дислексией, для которых рядом стоящие буквы меняются при чтении местами.

Такие панели достаточно просто внедрить в функционирующие сайты, не прибегнув к большим затратам, или вовсе бесплатно. Важно помнить, что кнопка «Версия для слабовидящих» должна быть видна и очевидна для всех пользователей, иначе какой смысл, если попросту её не найдет в визуальной среде.

Для анализа доступности интернетной среды были выбраны государственные веб-ресурсы Республики Беларусь. К сожалению, на государственных сайтах разработчики плохо позаботились о видимости кнопок для перехода на облегченную версию сайта. Так, например, на сайте министерства здравоохранения Республики Беларусь присутствует лишь функция увеличения шрифта на сайте (рис. 1). Контрастность кнопок нарушена, такая функция может остаться незамеченной, если пользователю с плохим зрением придется воспользоваться веб-ресурсом самостоятельно.

Рисунок 1 – Сайт Министерства здравоохранения РБ

Негативно отличился и сайт фонда защиты населения. Разработчики сделали текстовую кнопку нейтрально-серого цвета, которая сливается с белым фоном даже для хорошо зрячих людей (рис. 2).

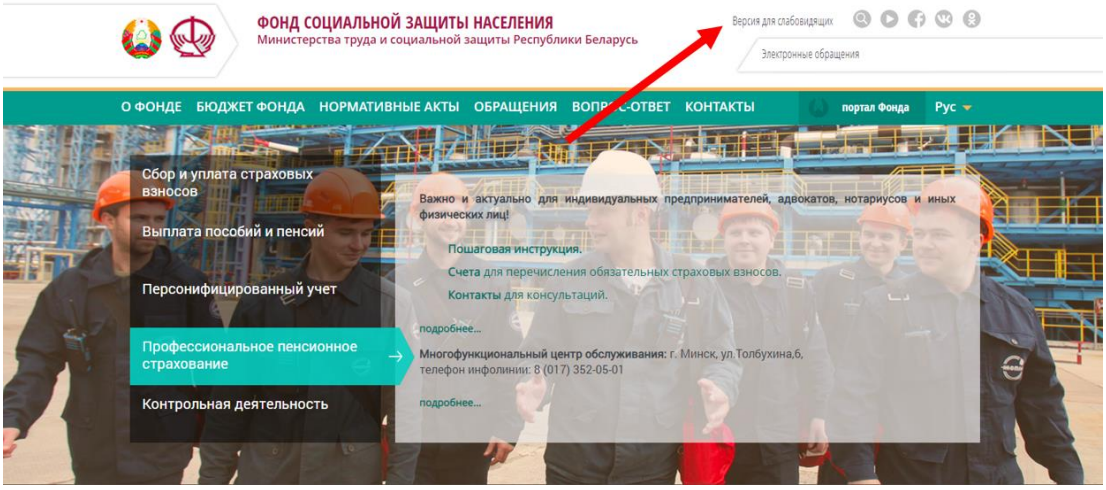


Рисунок 2 – сайт Фонда социальной защиты населения

Однако, при анализе государственных сайтов Республики Беларусь были обнаружены веб-ресурсы, вовсе не оснащенные никакими решениями для плохо видящих людей. К ним относятся Национально-правовой интернет-портал Республики Беларусь и Детский правовой портал Республики Беларусь. К сожалению, эти важные сайты не адаптированы под современные требования к веб-проектам, тем самым лишают возможности самостоятельного посещения плохо видящим людям.

При проектировании и разработке веб-сайтов важно помнить о том, что интернет – это возможность для всех, а увеличение доступности веб-сайта – это хороший шаг на встречу своим пользователям.

ЛИТЕРАТУРА

1. Сервис, предоставляющий статистику Республики Беларусь. [Электронный ресурс] – Режим доступа https://minsk.belstat.gov.by – Дата доступа: 10.03.2020.

УДК 004.021

Магистрант И. А. Литвинович
Науч. рук. ст. преп. А. С. Наркевич
(кафедра программной инженерии, БГТУ)

ОЦЕНКА СКОРОСТИ ВЫПОЛНЕНИЯ АЛГОРИТМОВ ПОИСКА ПРОФИЛЕЙ

В рамках исследовательской работы по изучению и разработке алгоритмов и методов оптимизации поиска профилей в социальных сетях,

были исследованы существующие методы обхода пользовательских профилей. При проведении исследований использовались алгоритмы, описанные в [1].

В ходе проведения опытов лидером оказался подход с использованием социального графа как структуры, позволяющей производить обход максимально эффективно. В социальном графе вершинами являются профили пользователей определенной социальной сети, а ребрами – социальные связи. В ходе исследований сравнивался подход итеративного обхода всех профилей и алгоритм, основанный на социальном графе.

Первый подход основан на последовательном итеративном переборе всех существующих объектов в базе данных. При использовании данного подхода среднее время поиска доходило до 10 минут и количество пройденных пользователей приближалось к десятимиллионам даже при условии близких социальных связей искомого профиля с ищущим. При использовании социального графа для обхода пользовательских профилей было достигнуто увеличение скорости в десятки раз и прирост составил в среднем тысячу пользователей при учете близких социальных связей.

Близкие социальные включают в себя людей, которые:

- живут в одном городе;
- работаю на одном предприятии;
- учатся в одном университете;
- имеют общие интересы.

У таких пользователей более вероятно наличие общих друзей и, таким образом, поиск на основе социального графа дает лучшие результаты.

Вычисление средней скорости работы алгоритмов производилось на различных количествах записей в базе данных. Алгоритм запускался по десять тысяч раз для каждой из тридцати тысяч записей в БД. Результаты вычисления средней скорости выполнения алгоритмов для каждой порции данных представлены в таблице.

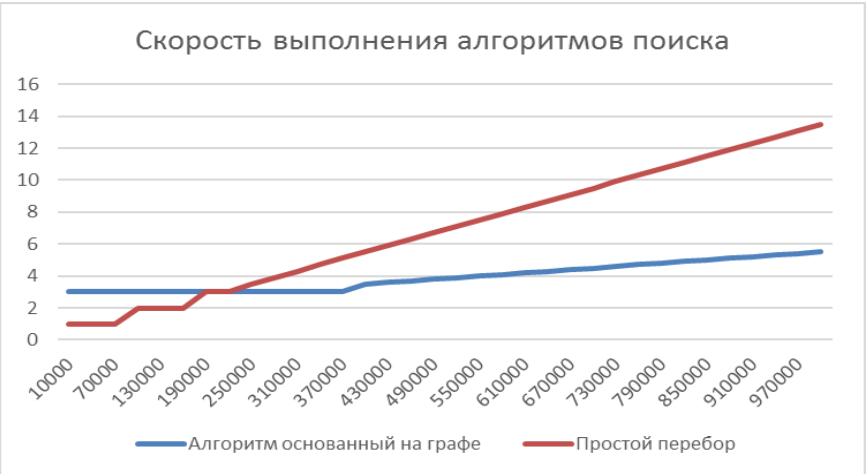
Таблица – Средняя скорость выполнения алгоритмов

Количество записей в БД	Алгоритм, основанный на графе	Простой перебор
1	2	3
10000	3	1
40000	3	1
70000	3	1
100000	3	2
130000	3	2
160000	3	2

Продолжение таблицы

1	2	3
190000	3	3
220000	3	3
250000	3	3.5
280000	3	3.9
310000	3	4.3
340000	3	4.7
370000	3	5.1
400000	3.5	5.5
430000	3.6	5.9
460000	3.7	6.3
490000	3.8	6.7
520000	3.9	7.1
550000	4	7.5
580000	4.1	7.9
610000	4.2	8.3
640000	4.3	8.7
670000	4.4	9.1
700000	4.5	9.5
730000	4.6	9.9
760000	4.7	10.3
790000	4.8	10.7
820000	4.9	11.1
850000	5	11.5
880000	5.1	11.9
910000	5.2	12.3
940000	5.3	12.7
970000	5.4	13.1
1000000	5.5	13.5

На графике представлена зависимость средней скорости нахождения искомого профиля для алгоритма, построенного на графовой структуре и алгоритма, основанного на простом переборе профилей.



Исходя из данных, представленных на графике, можно судить о том, что алгоритм простого перебора является эффективным для по-

иска в очень небольших объемах исходных данных (менее 200 тысяч), что может быть полезно для организации поиска внутри организаций с небольшим количеством сотрудников. Алгоритм основанный на социальном графе, учитывающий социальные связи при поиске и обработке профилей в социальных сетях, является предпочтительным, так как позволяет задействовать меньшие вычислительные мощности для поиска в больших объемах информации.

ЛИТЕРАТУРА

1.Литвинович, И. А. Разработка и оптимизация алгоритмов поиска профилей пользователей социальной сети по фотографии / И. А. Литвинович, А. С. Наркевич // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. – Минск: БГТУ, 2020. – № 1 (230). – С. 92-95.

УДК 004.22-021.453

Студ. Д. Э. Юрашевич
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

ИСПОЛЬЗОВАНИЕ СИСТЕМНЫХ СВОЙСТВ И ПАРАМЕТРОВ ФАЙЛОВ В СТЕГАНОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

Стеганографические методы стали важным и эффективным средством тайной передачи информации и защиты контента от несанкционированной модификации [1]. Для формального описания процессов используются разнообразные математические модели (см., например, [2, 3]).

Цель нашей работы: провести анализ свойств и параметров текстовых документов, получение их значений и задание значений свойств в плане возможности использования этих свойств в стеганографии. У документа можно выделить основные свойства, значение которых может получить любой пользователь с помощью проводника Windows. А также установить значения для некоторых из полученных свойств. Некоторые из них приведены в таблице.

В результате выполненного анализа были найдены свойства, которые не подвергаются изменению. Также найдены типы характеристик для всех системных свойств документа. Наибольшее количество имеет тип данных *String*, наименьшее – *IntPtr*. Были найдены свойства, в которые есть возможность устанавливать значение определенный длинны без изменения размера документа. Всего обнаружено 202 свойства.

Таблица – Основные свойства текстового документа

Свойство	Тип значения	Возможность изменения
Название	String	Да
Тема	String	Да
Теги	String[]	Да
Категории	String[]	Да
Комментарии	String	Да
Авторы	String[]	Да
Кем сохранен	String	Нет
Имя программы	String	Нет
Дата создания	Date	Нет
Язык	String	Да
Размер	Integer	Нет
Компьютер	String	Нет

Устанавливать значение свойств возможно только после открытия и изменения содержимого документа. В ходе исследования было выявлено, что не все свойства обладают возможностью фактического изменения. При изменении свойства, которое не поддается изменению, исполняющий файл не завершает свою работу ошибкой, а продолжает работу в штатном режиме, тем не менее, значение свойства не меняется. Это обусловлено тем, что есть такие свойства, при изменении которых, документ утратит свою работоспособность, например, свойство *ItemNameDisplay*.

В ходе исследования был доказан тот факт, что какое бы значение из 202 свойств не изменялось, хеш-сумма в любом случае поменяется. Также стоит отметить, что при модификации свойства, которое не подлежит изменению, хеш-сумма меняется, но значение свойства не меняется.

Еще одним фактом, о котором нельзя умолчать, является случай изменения свойства документа до того, как в него будет записана какая-либо информация. В таком случае запись в свойства файла невозможна. Некоторыми из списка таких свойств являются: *FileCount, FileAllocationSize, FileName, DateCreated, AppUserModel, ContentType, FileFRN, FreeSpace, ItemFolderPathDisplay*.

При изменении текстовых свойств файла размер файла увеличивается на 240-270 бит. Среда передачи документа не влияет на размер. Тестированию подвергались: электронная почта, социальная сеть Facebook, Bluetooth, съемные носители с файловыми системами NTFS.

Исследование атрибута документа показало, что его изменение никак не влияет на хеш-сумму документа. В завершении исследования был получен полный список свойств документа и их подробное опи-

сание. Направление дальнейших исследований – использование полученных результатов для разработки новых стеганометодов.

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учебно-метод. пос. для студ. вузов / П. П. Урбанович. – Минск: БГТУ, 2016. – 219 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. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си/ Б. Шнайер. – М.: Триумф, 2003. – 806с.

УДК 004.056+003.26

Студ. М. Е. Алексеев
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

ТЕКСТОВАЯ СТЕГАНОГРАФИЯ С ИСПОЛЬЗОВАНИЕМ КОНТЕЙНЕРА ФОРМАТА PDF

На сегодняшний день стеганографические методы сокрытия информации с использованием контейнера формата PDF исследованы в меньшей степени в сравнении с методами для других типов форматов [1, 2]. Цель данной работы: провести сравнительный анализ существующих методов PDF-стеганографии, а именно: метода инкрементных обновлений, метода выравнивания текста, метода использования пробельных символов и метода с использованием межсимвольных интервалов.

PDF (Portable Document Format) – межплатформенный открытый формат электронных документов, предназначенный для представления полиграфической продукции в электронном виде. Ниже представлена структура PDF-файла.

Из приведенной схемы видно, что у PDF-файла есть оригинальная часть, которая и отображает нам текст файла при его открытии, а также одна или несколько частей обновлений для хранения различных версий документа, т. е. небольшие части документа, которые содержат изменения по сравнению с предыдущей версией. Эти части называются инкрементными обновлениями.

Заголовок
Оригинальное тело
Оригинальный раздел перекрестных ссылок
Оригинальный трейлер
Обновление тела № 1
Раздел перекрестных ссылок № 1
Обновление трейлера № 1
.....
Обновление тела № n
Раздел перекрестных ссылок № n
Обновление трейлера № n

Рисунок 1 – Структура PDF-файла

В этих обновлениях мы и реализуем наш первый метод. С использованием данного метода были разработаны три способа сокрытия информации [3, 4].

Первый способ встраивает данные, изменяя текст видимым образом, затем записывает инкрементное обновление, содержащее исходные данные PDF, поэтому измененный текст не отображается. Второй метод встраивает данные, записывая инкрементные обновления для объектов, которые не существуют в исходных данных, поэтому обновление не имеет никакого эффекта. Данные встроенные в значение объектов потока, используются в обновлении. Третий метод включает данные, записывая инкрементные обновления с помощью заданной длины для нескольких объектов. Следовательно, данные можно получить, прочитав раздел перекрестных ссылок обновления, который включает начальный адрес каждого обновленного объекта.

Следующий метод применяется уже не к метаданным файла, а непосредственно к тексту файла. PDF-документ состоит из множества объектов, которые определяют внешний вид документа. Способ отображения объектов контролируется определенными командами внутри объекта, называемыми операторами. Например, оператор *Tc* и оператор *Tw* определяют характер и расстояние между словами. Оператор *Tj* используется для отображения текстовой строки.

Улучшенный оператор *TJ* также используется для отображения текстовой строки, но в отличие от простого оператора *Tj* он может управлять позиционированием отдельных символов в текстовой строке. Он содержит массив строк и чисел, состоящих из символов и значений пространства, используемых между этими символами.

Каждое значение пространства между символами вычитается из текущей текстовой позиции, которая сдвигает соответствующую строку влево на это значение (или вправо, в случае отрицательного значения).

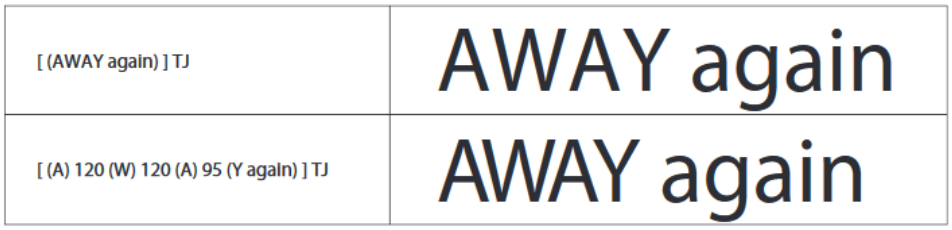


Рисунок 2 – Пример оператора TJ

Оператор TJ используется практически в каждом PDF-файле, содержащем параграфы текста. Каждая строка текста представлена одним оператором TJ. Если текст выровнен по краям, то оператор TJ используется чаще, чтобы ввести переменное расстояние между словами и символами для соответствия правилам выравнивая текста.

Для выравнивания текста используется PDF-writer, который генерирует случайные значения для *TJ* операторов. В таком случае можно скрыть данные в наименее значимых битах TJ оператора. Однако это можно применить только тогда, когда значения *TJ* оператора являются случайными и не содержат шаблон, для этого в алгоритме предусмотрена псевдохаотичность.

Последние два метода используют неразрывные пробелы, соответствующие коду A0 в кодировке ASCII. Первый метод заключается в замене обычных пробельных символов на неразрывные пробелы A0 для кодирования единицы и неизменности обычных пробельных символов – для кодирования ноля. Изменение в ширины символа A0 до нуля позволяет вставлять любое количество таких символов в документ без опасения, что данные изменения будут визуально видны в результирующем документе. Во втором методе между двумя любыми символами в документе встраивается несколько символов A0, количество которых кодирует необходимый ASCII символ.

Можно сделать вывод, что PDF-документ очень структурирован и скрытые в нем с помощью предложенных методов данные не могут быть легко обнаружены. Идея информационного сокрытия в электронных документах, несомненно, будет востребована, однако для этого необходимо выполнить больше исследований.

ЛИТЕРАТУРА

1. Блинова, Е. А. Сравнительные особенности использования стеганографических методов в электронных картах / Е. А. Блинова, П. П. Урбанович // X Международная научно-техническая конференция «Информационные технологии в промышленности, логистике и социальной сфере» (ITI*2019): тезисы докладов, Минск, 23-24 мая 2019 г. – Минск: ОИПИ НАН Беларуси, 2019. – С. 22-25.

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

3. Hongmei, Liu. Three novel algorithms for hiding data in pdf files based on incremental updates / Liu Hongmei, Lei Li, Jian Li, Jiwu Huang // Technical report –Sun Yat-sen University, Guangzhou, China. –2007. – P. 167–179.

4. Zhong, Shangping. Data hiding in a kind of pdf texts for secret communication / Shangping Zhong, Xueqi Cheng, Tierui Chen // International Journal of Network Security. – 2007. – № 4(1). – P. 17–26.

УДК 004.056

Студ. Е. С. Щепина
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ ПРИ РЕАЛИЗАЦИИ АЛГОРИТМА RSA ДЛЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Секретность информации всегда играла важную роль в жизни людей. Появление мощной современной вычислительной техники позволило получать доступ к ней быстрыми способами. Сегодня без использования криптографии немыслимо решение задач по обеспечению безопасности информации [1, 2].

Объект данного исследования – ключевая информация в алгоритме RSA для электронной цифровой подписи (ЭЦП). Цель работы – показать, как влияет выбор ключевых значений на криптостойкость и скорость работы алгоритма.

RSA – это асимметричный алгоритм (с открытым ключом). Основная идея заключается в том, чтобы использовать ключи парами: ключа зашифрования и ключа расшифрования, которые невозможно вычислить один из другого. Но существуют нюансы, без учёта которых реализацию RSA можно будет взломать за считанные секунды.

Что же касается подписи: рукописные подписи используются с давних времен, для того чтобы доказать принадлежность авторства документа лицу или согласия с ним. Подписанный документ нельзя изменить, невозможно отречься от подписи. Эти же функции выполняет ЭЦП.

Перейдем к ядру исследования – к особенностям ключевой информации. Любой алгоритм шифрования должен иметь высокую скорость работы, чтобы избежать задержек, так как в противном случае он будет подвержен взлому. Шифрование по алгоритму RSA выполняется намного быстрее, если правильно выбрать значение e. Тремя наиболее частыми вариантами являются: 3, 7 и 65537 (2^{16}+1). Двоичное представление 65537 содержит только 2 единицы, поэтому для возведения в степень нужно выполнить только 17 операций умножения. Стандарту X.509 соответствует число 65537, PEM рекомендует 3, а PKCS #1 – 3 или 65537.

К тому же криптостойкость RSA зависит от трудоемкости решения проблемы разложение на множители больших чисел, в частности числа $n=p*q$ (проблема факторизации больших чисел). Взлом заключается в нахождении числа d (секретного ключа), обратного e по модулю $\varphi(n)$. Это проще сделать, если знать числа p и q. Математически не доказано, что для восстановления сообщения по шифртексту и по значению открытого ключа нужно разложить число n на множители. В настоящее время значение n рекомендовано использовать порядка 1024 или 2048 бит. А также p и q не должны быть близки по значению, в противном случае криптостойкость падает.

Существует также проблема генерации простого числа. Как мы знаем, для алгоритмов с открытыми ключами нужны простые числа. Их нужно множество для любой достаточно большой сети. Существует примерно 10151 простых чисел длиной от 1 до 512 бит включительно [1]. Для чисел, близких к n, вероятность того, что случайно выбранное число окажется простым, равна $1/\ln(n)$. Поэтому полное число простых чисел, меньших n, равно $n/\ln(n)$.

Для анализа ключевых значений было разработано программное средство, реализующее алгоритм RSA для ЭЦП файла. Цифровая подпись реализуется следующим способом: над содержимым файла вычисляется хеш-функция, затем значение хеша шифруется алгоритмом RSA, и эта зашифрованная последовательность передается далее адресату. Адресат, в свою очередь, получив файл ЭЦП, вычисляет над содержимым файла значение хеш-функции, расшифровывает алгоритмом RSA полученную ЭЦП, получая тем самым значение переданного хеша. Далее он сравнивает значение вычисленного им самим хеша с полученным значением. Если значения совпадают, значит, файл подлинный и подпись верна, в противном случае – файл не подлинный и отличается от того, который передавал отправитель.

В программном средстве были использованы как рекомендованные значения ключевой информации, так и значения с низкой крипто-

стойкостью. Также был осуществлен замер времени работы алгоритма в обоих случаях.

Пользователь изначально выбирает файл с исходными данными, а также файл для ЭЦП. Далее вводит простые числа p и q и нажимает кнопку «*Подписать*», тем самым в программе вычисляется значение n, секретный ключ d, а также хеш, который шифруется и заносится в файл. В качестве исходных данных использовался текст «Katya». Для верификации подписи следует нажать кнопку «*Проверитьподпись*». Одно из окон приложения показано на рис. 1.

В первом случае были выбраны значения p=1009, q=619 и e=65537=(2^{16}+1), которые являются криптоустойчивыми за счет операций с большими числами. Также существует проверка, если исходный файл или файл с подписью был изменен. Пользовать сразу узнает об этом при проверке подлинности подписи (рис. 2). Что касается время работы подписи файла, то оно составило 69,81 миллисекунд.А проверка подлинности подписи составила 872,92миллисекунды.

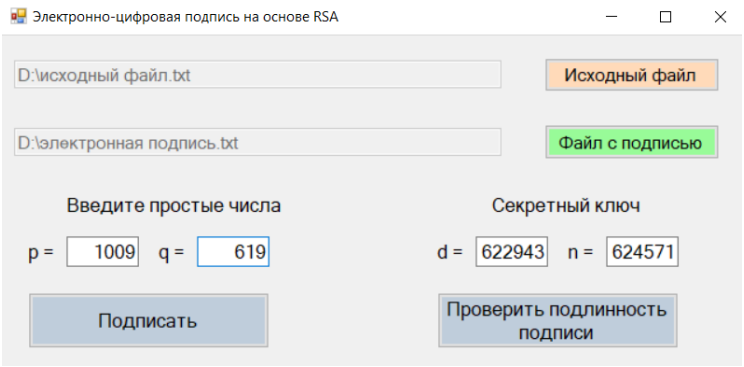


Рисунок 1 – Визуализация программного средства

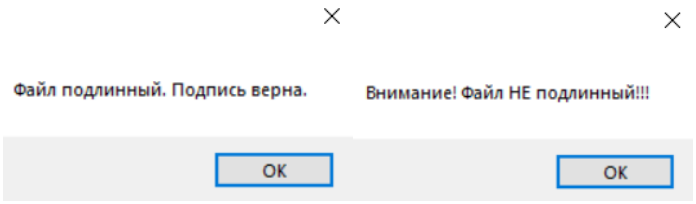


Рисунок 2 – Результаты верификации ЭЦП

Во втором случае было решено проделать те же шаги, но со значениямиp=113, q=151 и e=5. Такие значения делают шифр менее криптоустойчивым. Нужно отметить, что при меньших значениях p и q время, затраченное на подпись файла, составляет 1,93 миллисекунды. Это в 36 раз быстрее по сравнению с первым случаем. А время, затраченное на проверку подписи, составляет 2,79 миллисекунды, что в312,8 раз быстрее, чем работа в первом эксперименте.

Таким образом, особенности ключевой информации играют большую роль в обеспечении криптоустойчивости и скорости работы алгоритмаRSA для электронной цифровой подписи.При больших значениях ключевой информации криптоустойчивость возрастает, однако скорость работы падает за счет операций с большими числами, которые могут иметь размерность вплоть до 2048 бит.

ЛИТЕРАТУРА

1. Шнайер, Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си/ Б. Шнайер. М.: Триумф, 2003. – 610 с.

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

УДК 37.045:378.662(476)

Магистрант Е. Н. Бондарчик
Науч. рук. ст. преп. Е. А. Блинова
(кафедра информационных систем и технологий, БГТУ)

АНАЛИЗ МЕТОДОВ РАСПРЕДЕЛЕНИЯ НАГРУЗКИ ПРЕПОДАВАТЕЛЕЙ КАФЕДРЫ УНИВЕРСИТЕТА

В рамках управления учебным процессом учреждения высшего образования решается одна из наиболее важных задач – задача распределения нагрузки кафедры между профессорско-преподавательским составом оптимальным образом. Для оптимального распределения учебной нагрузки кафедры необходимо иметь возможность моделировать различные ее варианты, изменяя исходные данные. Варьируя распределением планируемой нагрузки кафедры между профессорско-преподавательским составом кафедры по семестрам, необходимо спланировать оптимальным образом учебный процесс с тем расчетом, чтобы наибольший объем учебной нагрузки по приоритетным типам работ назначался наиболее компетентному преподавателям с учетом равномерной их загрузки в учебном году [1].

Исходными данными для задачи распределения учебной нагрузки между преподавателями кафедры, являются: учебная нагрузка кафедры по читаемым дисциплинам; плановое штатное расписание кафедры; фактический штат преподавателей кафедры; критерии и ограничения (рис.1).

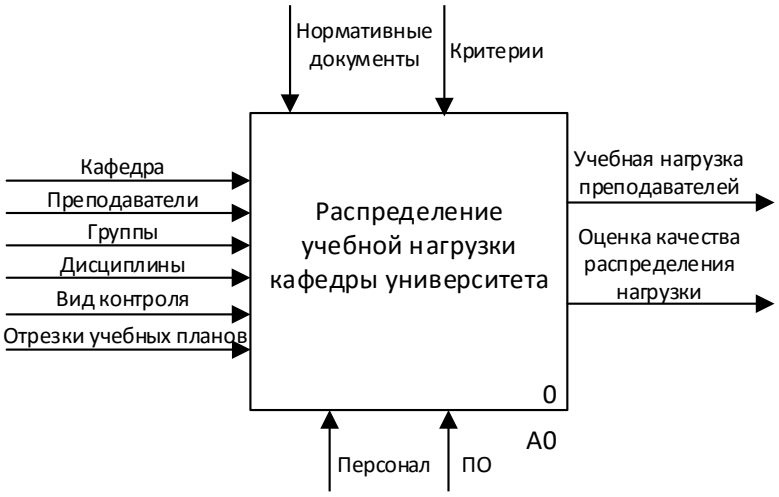


Рисунок 1 – Контекстная диаграмма А0

Требуется найти такое распределение, при котором разность между плановой и фактической учебной нагрузкой преподавателей была бы минимальной при заданных критериях и ограничениях.

Существует несколько методов решения задач данной тематики:

- распределению научной работы преподавателей по критерию ее эффективности с точки зрения эффективности с целью максимизации общего научного результата. При этом эффективность выполнения учебной работы для всех преподавателей принимается одинаковой и ее объем назначается как разность между общей нагрузкой преподавателя и нагрузкой, выполняемой по другим видам работ;
- распределению научной работы преподавателей по выбору одного из двух критериев: равная средняя учебная нагрузка или максимально-допустимая нагрузка для преподавателя. Ни тот ни другой критерий не обеспечивает относительно равномерную нагрузки преподавателей по разным видам работ;

В дальнейшем был выбран алгоритм решения задачи распределения нагрузки профессорско-преподавательского состава кафедры, который сводится к минимизации целевой функции с учетом ограничений на управляемые переменные.

Приведем основные положения математической модели распределения учебной нагрузки между преподавателями кафедры [2]. Пусть за кафедрой закреплено s дисциплин: A_1, A_2, …, A_i,…, A_s– нагрузка по каждой дисциплине и n преподавателей: B_1, B_2, …, B_k,…, B_n– нагрузка по каждому преподавателю, $\sum_{i=1}^{s} A_i = \sum_{k=1}^{n} B_k$ Каждая дисциплина в свою очередь состоит из t видов учебных работ: C_1, C_2, …, C_k,…, C_t, нагрузка по каждому виду учебной работы, C_j A_i. Для каждого t-го преподавателя задаются: преемственность – f_{tij} (т. е. выполнял t-й преподаватель

j-й вид учебной работы *i*-й дисциплины или нет); диапазон плановой нагрузки *v* по *j*-му виду учебной работы для преподавателей всех должностей и по учебной нагрузке преподавателя для каждой должности.

Для того чтобы задать диапазон плановой нагрузки по *j*-му виду учебной работы для преподавателей всех должностей и по учебной нагрузке преподавателя для каждой должности необходимо определить средние показатели: среднюю нагрузку по кафедре, среднюю нагрузку по должностям преподавателей, среднюю нагрузку преподавателей по конкретному виду учебной работы, необходимых для распределения нагрузки.

В качестве критерия распределения предложено использовать заданную равномерность загрузки преподавателей различными видами учебной работы с учетом должностных коэффициентов по видам работ и по учебной нагрузке в целом.

Формализованная задача распределения учебной нагрузки между преподавателями кафедры будет иметь следующий вид:

$$F = \left| B_{t,j}^{fact} - B_{t,j}^{plan} \right| \to \min \ , \qquad (1)$$

где

$$B_{t,j}^{fact} = \sum_{i=1}^{s} \sum_{j=1}^{k} x_{jit} C_{ji} f_{ji} , B_{t,j}^{plan} = \sum_{i=1}^{s} \sum_{j=1}^{k} x_{jit} C_{ji} f_{ji} v_t ,$$

$$t = \overline{1,n} , \ f_{tji} \in \{0;1\},$$

где s – количество дисциплин; n – количество преподавателей; A_i – нагрузка по *i*-й дисциплине $i = \overline{1,s}$; x_{jit} – назначение *j*-го вида учебной работы *i*-й дисциплины *t*-му преподавателю; $x_{tji} \in \{0;1\}$; C_{ji} – нагрузка по *j*-му виду учебной работы *i*-й дисциплины.

Приведенная в работе математическая модель, при возможности ее реализации в систему распределения учебной нагрузки кафедры университета [3], позволит получать по заданным критериям и ограничениям множество допустимых вариантов распределения учебной нагрузки, из которых лицо, принимающее решение, выбирает наилучший вариант распределения. Такой подход позволит не только обеспечить оптимальность при распределении учебной нагрузки, но и предоставить руководству кафедрой возможность эффективно использовать педагогический и научный потенциал кафедры в интересах ее развития, повышения эффективности учебной, методической и научной работы

за счет перераспределения указанных видов работ между профессорско-преподавательским составом кафедры.

ЛИТЕРАТУРА

1 Гусев В.В. Система моделей и методов рационального планирования и организации учебного плана в вузе / В.В. Гусев, Н.Я. Краснер. – Воронеж: ВГУ, 1984. – 152 с.

2 Тархов, С.В. Математическая модель распределения учебной нагрузки между преподавателями кафедры / С.В.Тархов, С.Н.Султанова Информационные технологии моделирования и управления. №5. Воронеж: Научная книга,2005. С.676–681.

3 Исходный код системы распределения учебной нагрузки кафедры университета [Электронный ресурс]. Режим доступа: https://github.com/ZhenyaBond/LoadDistributionManagementSystem. – Дата доступа: 23.04.2020.

УДК 004.056+003.26

Студ. Ю. А. Карленок
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

ШИФРОВАЛЬНАЯ МАШИНА «ЭНИГМА»: УСТРОЙСТВО, ФУНКЦИОНАЛ, СИМУЛЯТОР

Энигма – переносная электромеханическая роторная шифровальная машина, использовавшаяся для шифрования и дешифрования секретных сообщений примерно до середины 20 века. Машина основана на использовании многоалфавитных шифров подстановки [1]. Конструктивно машина состояла из четырех отсеков: три служили (либо четыре) для роторов и один – для расположения в нем рефлектора. По своему строению ротор имел 26 сечений, по одному в соответствии каждой букве латинского алфавита; кроме этого в нем было 26 контактов, которые служат в качестве элементов соединения с другими роторами. В то время как оператор нажимает на кнопку, цепь в шифровальной машине замыкается, после чего появляется зашифрованная буква. Цепь замыкалась также при помощи рефлектора.

После отражения сигнала на рефлекторе производятся обратные операции тем, что были проделаны выше. В результате на выходе будет получена зашифрованная буква. Более наглядное представление алгоритма иллюстрировано ниже (рис. 1) [2].

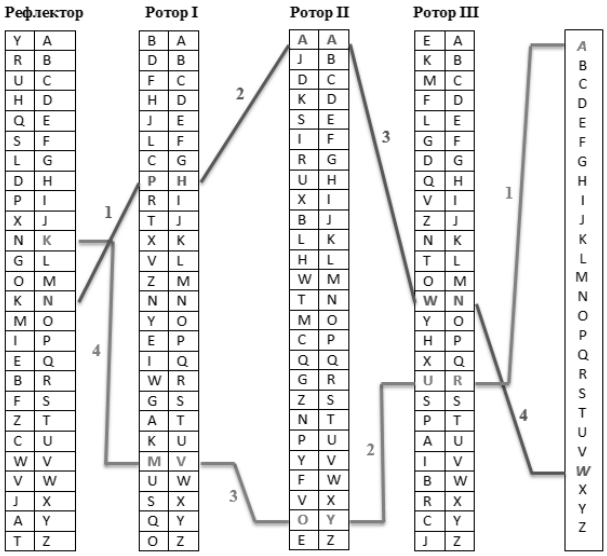


Рисунок 1 – Схема работы шифровальной машины «Энигма»

Реализация шифровальной машины имеет ряд уникальных свойств, к основным из которых относятся следующие:

- если установить одни и те же роторы в одном и том же порядке, то повторно закодированные сообщения будут одинаковы;
- при кодировании одинаковых и идущих друг за другом символов на выходе образуются абсолютно разные буквы.

Основная цель нашей работы: создание пользовательского приложения, которое бы симулировало работу Энигмы.

Созданный симулятор «располагает» 10 роторами, из которых в процессе шифрования участвуют только 3; панелью задания стартовых позиция для роторов, а также шага смещения каждого ротора; коммутационной панелью, которая позволяет соединить 26 символов алфавита 13 каналами, согласно которым происходит попарная замена букв; устройством ввода/вывода.

Для успешной шифрации/дешифрации симулятору нужно:

- установить роторы в нужной последовательности;
- установить начальные позиции роторов;
- установить шаг (если шифруется несколько символов);
- установить пары коммутаторов.

Была также проведена оценка криптостойкости симулятора. Мы получили 100 046 363 423 806 800 000 или примерно 10^{20} всевозможных подстановок [3]. Версия Энигмы (три ротора с выбором из 5 роторов, отражатель и 10 штекерных кабелей для коммутационной панели) может быть настроена на 1,07 • 1023 различных состояний, что сопоставимо с 77-битным криптографическим ключом.

Также рассмотрены некоторые аспекты использования подстановочных шифров в сетевых приложениях [4].

ЛИТЕРАТУРА

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

2. Исследование алгоритма работы шифровальной машины Энигма [Электронный ресурс]: http://human.snauka.ru/2016/06/15717, Дата доступа: 15.04.2020.

3. Криптоанализ «Энигмы» [Электронный ресурс]: https://ru.wikipedia.org/wiki/Криптоанализ_«Энигмы», Дата доступа: 15.04.2020.

4. Урбанович, П. П. Компьютерные сети: учебное пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. – Минск: БГТУ, 2011. – 399 с.

УДК 519.168

Студ. Р. Ю. Злобин
Науч. рук. доц. И. К. Асмыкович
(кафедра высшей математики, БГТУ)

СРАВНЕНИЕ СКОРОСТИ РАБОТЫ АЛГОРИТМОВ РЕШЕНИЯ ЗАДАЧИ КОММИВОЯЖЁРА

На сегодняшний день конкуренция на рынке курьерских служб очень велика. Одной из самых важных задач для работы службы является определение оптимального пути доставки заказов, то есть решить задачу коммивояжёра.

Цель работы – провести поиск алгоритмов решения задачи коммивояжера, выяснить какие из них являются наиболее эффективными и практически применимыми.

Задача коммивояжёра – одна из самых известных задач комбинаторной оптимизации, заключающаяся в поиске самого выгодного маршрута, проходящего через указанные города хотя бы по одному разу с последующим возвратом в исходный город. В условиях теории графов [1] задача заключается в поиске кратчайшего гамильтонова цикла. Данная задача в своём классическом описании является NP-трудной, если же необходимо найти пути длинной не превышающий X, то задача будет NP-полной [2].

Было рассмотрено 5 алгоритмов: полный перебор, метод динамического программирования, метод ветвей и границ, метод имитации отжига и метод муравьиной колонии.

Решение методом полного перебора подразумевает под собой, разбор всех возможных перестановок городов в цикле и поиск среди них оптимального решения. Данный метод имеет асимптотическую сложность $O(nP_n)$ по времени.

Основная идея метода динамического программирования заключается в вычислении путей от исходного города до каждого из остальных городов, затем суммирования этой величины с путем из каждого из остальных городов до оставшихся городов и т. д. Преимущество данного метода D перед методом полного перебора F заключается в существенном сокращении полного объема вычислений.

$$P_D = (6n-1) - n2^{n-1} + 4n(n-1)2^{n-2},\ \ P_F = n! \approx n^n e^{-n}\sqrt{2\pi n}, P_D \ll P_F$$

за счет заметного увеличения объема памяти $Q_D \sim 2^n\sqrt{\frac{2n}{\pi}}, Q_F = 2, Q_D \gg Q_F$. Затраты по памяти настолько велики, что при $n = 30$ составляют около 120 Гб.

Метод ветвей и границ, а именно его частный случай алгоритм Литтла, является оптимальным выбором для нахождения точного решения задачи коммивояжёра. Общая идея тривиальна: нужно разделить огромное число перебираемых вариантов на классы и получить оценки для этих классов, чтобы иметь возможность отбрасывать варианты не по одному, а целыми классами. Данный метод в худшем случае имеет асимптотическую сложность полного перебора, в лучшем – $O(n^2)$. [2].

Скорость работы алгоритмов оценим случайно сгенерированными тестами различных размеров. Тестирование проведено на персональном компьютере на базе процессора IntelCorei5 – 6200U. Результат представлен в единицах процессорного времени, такт, что равно одной тысячной секунды.

Таблица 1 – Результат работы алгоритмов

Количество городов	ДП	МВиГ	Полный перебор
5	1	1	0
7	0	0	1
9	4	1	9
11	22	1	677
13	109	1	83711

По результатам работы алгоритмов видно, что оптимальным выбором при точном решении задачи коммивояжёра является метод ветвей и границ.

Метод имитации отжига и муравьиной колонии – вероятностные методы. Они позволяют найти решение близкое к наилучшему за полиномиальное время.

Основная цель метод имитации отжига – привести систему в состояние с меньшей энергией. На каждой итерации алгоритма происходит переход текущего состояния системы в новое случайное состояние, при этом переход в лучшее состояние совершается всегда, а в худшее с некоторой вероятностью, зависящей от разницы энергии состояний и температуры итерации [3].

В основе метода муравьиной колонии лежит поведение муравьев некоторых видов, которые изначально перемещаются в поисках пищи случайным образом, но, найдя ее, возвращаются в свою колонию, помечая путь феромонами, которые со временем испаряются. Это избавляет других муравьев от необходимости случайного поиска пищи и делает его более целенаправленным: найдя путь, помеченный феромонами, муравьи движутся по нему, усиливая плотность феромонов [4].

Для сравнения скорости и точности работы данных алгоритмов воспользовались готовым тестовым примером eil101 пакета TSPLIB95 с оптимальным ответом 629.

Таблица 2 – Результат работы вероятностный алгоритмов

Алгоритм	Время	Ответ	Точность
Имитация отжига	**92**	808	77,8%
Муравьиная колония	4028	**690**	**91,1%**

Видно, что имитационный отжиг заметно выигрывает во времени работы, но проигрывает в точности решения.

ЛИТЕРАТУРА

1. Злобин Р. Ю. Некоторые применения теории графов Актуальные проблемы информатики и информационных технологий в образовании: материалы Всероссийской конф. с межд. участием. Красноярск, 23 апреля 2019 г. [Эл.Рес.] / отв. ред. П.С. Ломаско; / Краснояр.гос. пед. ун-т им. В.П. Астафьева. – Красноярск, 2019. – С. 119 – 126.

2. Мудров В.И.. Задача о коммивояжёре. – М.: «Знание», 1969. – С. 62.

3. Каллан Роберт. Основные концепции нейронных сетей. – М.: Издательский дом Вильямс, 2003. – 288 с. – С. 146 – 148.

4. Штовба С.Д. Муравьиные алгоритмы // ExponentaPro. Математика в приложениях. – 2003. – №4. – С. 70–75.

UDK 004.72

PhD student Ghassan Jaber
Supervise N. V. Patsei
(Department of software engineering, BSTU)

MODELING OF DATA CONTENT OBJECT OPERATIONS IN SEMANTIC INFORMATION-CENTRIC NETWORKS

This work addresses the problem of naming and routing in the Information-Centric Networking (ICN) where a new semantic-based scheme entitled «Semantic Information Centric Networking» (SICN) is proposed. This proposal takes into consideration the problem of data communication types. For instance, the legacy proposals in ICN have weaknesses in dealing with host-to-host communication type. In order to deal with this problem, a three-dimension addressing scheme and a routing mechanism were presented [1-2]. It use the geographical, semantic, and publisher ID address for the addressing scheme. In model we utilize the IPv6 extension header to define a new routing scheme that can deal with the three-dimension address. As a result, the proposed scheme will evolve the interests of subscribers to a higher abstract level, reduce the name resolution brokers, reduce the delays and evolve towards the new generation semantic web [1].

In order to compare between different schemers, we build a model composed of public network with not fully connected routers. All the tables hold by routers learnt the addresses before. Each router reconnected to many interfaces and only some of them are connected to cache.

There are four scenarios classified according to data types. Scenario (Type A): deals with data from type A [1]. WhatsApp call is an example on scenario of Type A (Fig. 1). The communication components are the publisher and two subscribers who contact each other. WhatsApp is the publisher and suppose it has these two addresses: Pub ID and Geo IP. The first subscriber is the calling phone and the second subscriber is the called phone. Subscriber sends IRM (Interest Request Message) having the 3D-address as show in Table 1.

Table 1 -3D-address in IRM

Pub ID:	WhatsApp
Geo IP:	none
Semantic:	none

IRM propagates(broadcasts) to the routers and search in each Geo-ID table till reach the publisher (where matching will occur between IRM and the Pub ID). IRM will be updated by the new IP at each router. The publisher router (WhatsApp router) will send ARM (Address Request Message)with the 3D-address in Table 2.

ARM will propagate on the same path of IRM but in inverse a direction till reaching the source of IRM. The Geo-ID table of each router passed by ARM will be added by a new record. The calling subscriber router will send CRM (Content Request Message) to the called subscriber router passing through the publisher WhatsApp router. CRM will have the 3D- address as shown in Table 3.

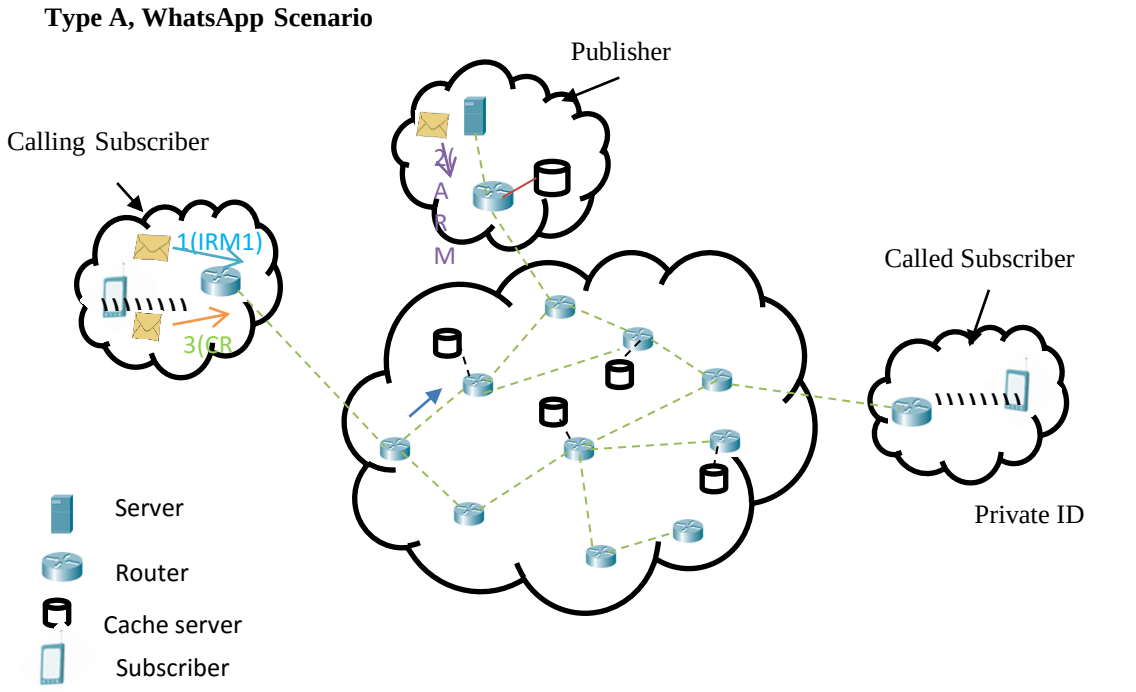


Figure 1 – SICN model architecture with one-to-one data searching scenario

Table 2 -3D-address in ARM

Pub ID:	**WhatsApp**
Geo IP:	2B:: 012C
Semantic:	none

Table 3 -3D-address in CRM

Pub ID:	**WhatsApp: Private ID: +375**
Geo IP:	2B:: 012C
Semantic:	none

For new algorithms have been developed for add new records, update TTL (Time To Leave) for the record, add records to cache when TTL reaches threshold another update algorithm will update the TTL in the cache. In addition, matching algorithm is presented. Moreover, garbage collector algorithm for records in tables (addresses) and caches (data) were presented. Garbage collector algorithm role is to remove the records based on TTL thresholds to manage the volume helping in scalability issue.

To compare between the different schemas, we build a model under some assumptions and used Python program to obtain the results. Model

constituted of following components: *Publisher* - the main content source; *Subscriber* - the user of the data content; *Search engine* - it is needed for some of the schemas to translate the data from informal to formal form; *DNS* - is needed for some of the schemas to find data source IP; *Cache*.

We held the following assumptions: u - number of users (u=10); n - publisher depth; e - search engine depth(e=n); d - DNS depth(d=n/2); c - cache depth (c=n/2); s - sharing coefficient (s=0.25); r - sharing factor (r = 1+s(u- 1); L - total number of extended branches for each subscriber to data source $L= 2^{(n+1)}- 2$. It is supposed that each node has two branches.

During modeling, we considered parameter *TD* (Time Delay).

Figure 2 illustrates *TD* versus number of links to the data source in the six schema. As shown in the figure 2, in case the content, schemas using name resolution routing (SICN, CBCB and KBN) outperforms schemas using name-based routing (IP, DONA, PUSUIT).

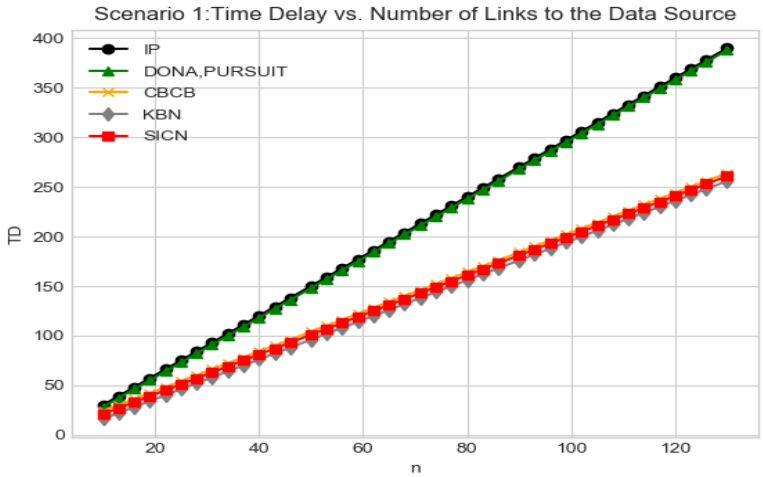


Figure 21 - Time delay vs number of links to the data source

Results were tested over other scenarios that differs according to content abstract level. The levels are data, information, and knowledge. Three different metrics. These metrics are: Time Delay, Flooding or traffic, and Efficiency Reuse factor for data. In terms of *TD* SICN outperforms the other schemes.In terms of Efficiency SICN shows a good results compared with many schemes, but KBN outperforms it.

REFERENCES

1. *Patsei N., Jaber G.* Routing Schem for Information-Centric Networking//11th International Conference NEET. Lublin University of Technology, Lublin, Poland, June 25 – 28.- 2019 – P.29.

2. *Jaber G., Patsei N. Rahal F.* Routing Challenges in Information-Centric Networking // «Applied Issues of Exact Siences» III International Sientific Practical Conference of graduate and postgraduate students, lectures, 1-2 November 2019, Armavir.- 2019. – P.252-255.

УДК 004.932.2

Магистрант А. Д. Самаль
Науч. рук. доц. Н. В. Пацей
(кафедра программной инженерии, БГТУ)

АНАЛИЗ АЛГОРИТМОВ КЛАССИФИКАЦИИ ОБЪЕКТОВ ИЗОБРАЖЕНИЙ

Распознавание образов на снимках применяется в различных сферах, таких как сельское хозяйство, лесное хозяйство, анализ рельефа, мониторинг разливов нефти и распознавание техники [1-3].

Целью работы является анализ алгоритмов классификации для дальнейшего их использования в работе.

Для исследования был выбран алгоритм k ближайших соседей. Он относится к метрическим алгоритмам классификации с обучающей выборкой Ω_O [1]. Такие алгоритмы относят объект u к тому классу $y \in Y$, для которого суммарный вес ближайших объектов из обучающей выборки максимален:

$$a(u,\Omega_O)=arg\ \max_{y\in Y} \Gamma_y(u,\Omega_O),\ \text{и}\ \Gamma_y(u,\Omega_O)=\sum_{i=1}^{k}[y_u^{(i)}=y]\omega(i,u).$$

Где весовая функция $\omega(i,u)$ оценивает степень важности -го соседа для классификации объекта u. Функция $\Gamma_y(u,\Omega_O)$ является оценкой близости объекта u к классу y. Функция степени важности выбирается неотрицательной и не возрастающей по i. Критерии выбора обусловлены тем, что чем меньше расстояние между исследуемыми объектами выборки u и $xu^{(i)}$, тем больше вероятности верной классификации. В алгоритме k ближайших соседей, объект u относят к такому классу, которому принадлежит больше элементов, среди k ближайших соседей $xu^{(i)}$, i=1,k:

$$\omega(i,u)=[i\le k]\omega_i,\ a(u,\Omega_O,k)=arg\ \max_{y\in Y}\sum_{i=1}^{k}[yu^{(i)}=y]\omega_i.$$

В качестве метрики чаще всего выбирается евклидова метрика из-за ее простоты и понятности [2].

Евклидово расстояние между двумя точками x,y определяется в евклидовом n-мерном пространстве как:

$$r(x,y)=\sqrt{(x1-y1)^2+(x2-y2)^2+\cdots+(xn-yn)2}=\sqrt{\sum_{i=1}^{n}(xi-yi)^2}.$$

Под деревом решений понимается структура иерархического типа, в ветках которой определяют разбиение пространства признаков, а листами являются элементарные функции классификации [3]. Существует различные методы построения деревьев. Случайный лес – алгоритм машинного обучения, заключающийся в использовании ансамбля решающих деревьев.

В результате работы выполнен сравнительный анализ существующих методов классификаций изображений. Выделен вектор классификационных признаков, используемых для распознавания объектов на изображениях. Разработано программное средство на языке Python для многоуровневой классификации изображений. Выполнено исследование эффективности классификации на основе алгоритмов LDA, KNN, RF и SVM [4-5].

Для сравнительного анализа использовался набор данных с изображениями ландшафта, таким как море, береговая линия и суша. А в качестве признаков использовались момент изображения, а так же признак Харалика. График, демонстрирующий точность сравниваемых алгоритмов изображен на рисунке 1.

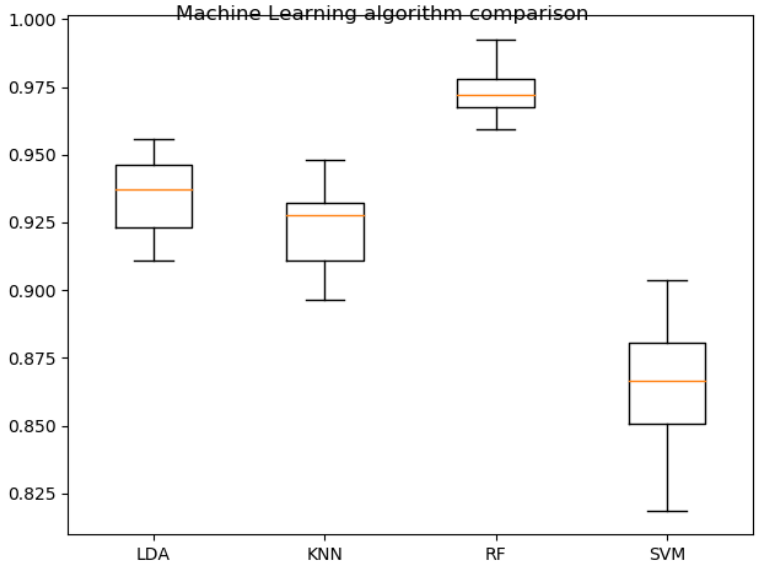


Рисунок 1 – График сравнения работы алгоритмов

Согласно полученным данным можно сделать вывод о том, что метод случайный лес превосходит остальные по точности классификации. Для него характерна высокая точность и маленький разброс значений. Одним из преимуществ данного алгоритма является то, что он одинаково хорошо обрабатывает как непрерывные, так и дискретные признаки. Существуют методы построения деревьев по данным с пропущенными значениями признаков.

ЛИТЕРАТУРА

1. D. Michie, D.J. Spiegelhalter, C.C. Taylor. Machine Learning, Neural and Statistical Classification/ D. Michie, D.J. Spiegelhalter, C.C. Taylor, 1994. – 265c.

2. Машинное обучение: виды, алгоритмы, примеры [Электрон. ресурс] // Генеральный директор. – Персональный журнал руководителя. дан. -Режимдоступа: https://www.gd.ru.

3. Ian Goodfellow, Yoshua Bengio, Aaron Courville. Deep Learning/ Ian Goodfellow, Yoshua Bengio, Aaron Courville / Deep Learning. – 2016. – 775 с.

4. Пацей Н.В., Самаль А.Д. Анализ работы модели классификации объектов изображений // Молодежь и научно-технический прогресс: Сборник докладов XIII международной научно-практической конференции студентов, аспирантов и молодых ученых. В 2 т. Т. 1. / Сост.: Е. Н. Иванцова, В. М. Уваров [и др.]. – Губкин; Старый Оскол: ООО «Ассистент плюс», 2020. – с.182-183.

5. Пацей Н. В., Самаль А.Д., Годун А. В. Алгоритм многоуровневой классификации объектов изображений на основе ErrorCorrectingOutputCodes // Информационные технологии : материалы 84-й науч.-техн. конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 3-15 февраля 2020 года [Электронный ресурс] / отв. за издание И.В. Войтов; УО БГТУ. – Минск: БГТУ, 2020. – с. 76-78.

УДК 628.39

Студ. А. В. Байдук
Науч. рук. зав. кафедрой Г. И. Касперов
(кафедра инженерной графики, БГТУ)

ОЦЕНКА ТЕХНИЧЕСКОГО СОСТОЯНИЯ ОЧИСТНЫХ СООРУЖЕНИЙ

Очистные сооружения представляют собой специализированное оборудование, проходя через которое загрязненные стоки (бытовые, промышленные, сельскохозяйственные) очищаются от вредных примесей, способных неблагоприятно повлиять на водоемы-водоприемники, куда их сбрасывают, и на экологическую обстановку в целом. Поэтому аварии на очистных сооружениях являются опасными и могут повлечь за собой различные негативные последствия, ведь продуктом производственного процесса нередко становятся агрессивные стоки, содержащие примеси тяжелых металлов и других токсичных веществ [1, 2].

Аварии на очистных сооружениях могут происходить по нескольким причинам: отключение электричества, износ оборудования, погода и стихийные бедствия, человеческий фактор и нештатная работа очистных сооружений. Аварии на очистных сооружениях могут

быть локального характера, а могут очень быстро перерасти в настоящую экологическую трансграничную катастрофу, так как моря и реки способны распространять ядовитые стоки на очень большие расстояния, становясь причиной гибели живых организмов и нанося окружающей среде непоправимый вред. Именно поэтому в рамках выполнения задания 3.1.04 «Исследование масштабов и разработка прогнозных моделей развития деформаций гидротехнических сооружений водоемов технического назначения (охладительных, очистных, технологических) для профилактики и оценки последствий чрезвычайных ситуаций» ГПНИ «Информатика, космос и безопасность» активно ведется разработка организационно-технических мероприятий, нацеленных на предотвращение аварий на очистных сооружениях любого типа.

В 2016–2018 гг. были проведены натурные обследования 44 объектов, расположенных на территории Гродненской, Минской и Могилевской областей (табл.).

Таблица – Количество обследованных и сроки эксплуатации очистных сооружений (ОС)

Область	Кол-во объектов		Процент находящихся в эксплуатации ОС, лет			
	по списку	обследованных	10–19	20–29	30–39	40 и более
Гродненская	17	16	18	18	41	23
Могилевская	22	14	29	14	19	38
Минская	21	14	5	30	43	22

В процессе выполнения натурных обследовании, а также по данным районных отделов по чрезвычайным ситуациям [3] устанавливали сроки ввода в эксплуатацию (реконструкции) очистных сооружений (табл. 1).

Сравнительный анализ находящихся в эксплуатации очистных сооружений по АТЕ показывает, что 57–65% из них работают 30 и более лет.

Результаты проведенных натурных обследований по оценке технического состояния пятидесяти водоемов технического назначения (очистных) показали, что [3]:

– доминирующую роль в развитии деформаций откосов водоемов технического назначения (очистных) играет режим колебания уровней и развитие фильтрационных явлений, проявляющихся в виде суффозионных выносов в нижнем бъефе земляных сооружений, контактной фильтрации вдоль бетонных конструкций, а также просадок гребня дамб и локального развития абразионных процессов;

– ряд объектов очистных сооружений находятся в неудовлетворительном состоянии (9,5%) и требуют ремонта или их реконструкции.

– на вероятность возникновения чрезвычайных ситуаций на очистных сооружениях важную роль оказывает человеческий фактор – качество изысканий, проектирования, строительства и эксплуатации объекта повышенной опасности, каковыми являются все без исключения ГТС;

– наибольшее количество аварий происходит на очистных сооружениях предприятий, срок эксплуатации которых превышает 35–40 лет и более.

ЛИТЕРАТУРА

1. Об обращении с отходами: Закон Республики Беларусь, 20 июля 2007 г. № 271-З.

2. Водный кодекс Республики Беларусь от 30 апреля 2014 г. № 143-З.

3. Разработать научно-методические основы ведения мониторинга состояния сооружений на водоемах технического назначения для оценки последствий и ущербов от чрезвычайных ситуаций: отчет о НИР (окончат.) /БГТУ; рук. темы Г.И. Касперов. – Минск, 2018. –254 с. – № ГР 20160782.

УДК 004.925

Студ. Я. А. Игнаткова, А. А. Жукова
Науч. рук. ст. преп. Н. И. Потапенко
(кафедра информатики и веб-дизайна, БГТУ)

СТИЛИ ДИЗАЙНА И ОПЫТ ПОЛЬЗОВАТЕЛЯ

На этапе проектирования любого веб-продукта дизайнер сталкивается со сложностями выбора стиля и размещения элементов. Многие дизайнеры следуют модным тенденциям и своим предпочтениям, забывая при этом об особенностях восприятия информации обыкновенными пользователями и их опыте работы с другими похожими веб-сайтам и приложениями.

Дизайн – первое, на что пользователь обращает свое внимание, когда открывает веб-страничку или приложение. Опыт пользователя, в основном, зависит от дизайна, а также того, как он способствует узнаваемости бренда.

Сегодня можно сделать визуально красивый сайт, однако не учесть нужды простого пользователя. Опыт пользователя – это важ-

ный определяющий фактор, потому без него любые ухищрения не смогут принести необходимую конверсию [1].

При создании веб-продукта необходимо правильно согласовать тематику с контентном. Информации на сайте не должно быть много, иначе она утомит пользователя, при этом её не должно быть мало, потому что тогда пользователь не получит необходимые ему данные. Информация должна выдаваться постепенно, порционно и последовательно. Для удобной и упорядоченной подачи информации необходимо грамотно использовать дизайнерские приемы и закономерности.

На данным момент можно выделить четыре типа сайтов, в зависимости от соответствия их тематики, дизайна и контента:

– сайты, дизайн которых не соответствует тематике представляемой фирмы или компании. Такие сайты пользователи покидают быстро, находя их неприятными и странными;

– сайты, дизайн которых устарел, но соответствует услугам представляемой фирмы или компании. Данный вид сайтов приемлем для своей постоянной аудитории, но не привлекает новых пользователей, поскольку не может заинтересовать их своим внешнем видом;

– сайты, соответствующие последним трендам дизайна, но не дающие полной и понятной информации о представляемой фирме или компании. На таких сайтах обычно приятно находиться, но не понятно, что делать;

– сайты, соответствующие последним трендам дизайна и отражающие тематику фирмы. Самый лучший вариант, к которому надо стремиться. Но поскольку все люди разные и особенности восприятия информации у них разняться, то нельзя создать «идеальный» сайт, который воспринимался бы всеми одинаково и точно. Любой сайт создаётся ориентированным на контурную группу людей, зная их примерный опыт работы и требования к сайту.

Для того, чтобы выяснить насколько велика разница между данными типами сайтов и от чего зависит восприятие общей направленности сайта, было проведено исследование в виде опроса.

В опросе приняли участие 20 человек в возрасте от 17 до 23 лет, 75% опрашиваемых женского пола и 25% – мужского. Каждому респонденту представлялись 10 отобранных заранее сайтов и задавались четыре вопроса о каждом из сайтов.

Первый вопрос – как быстро вы поняли тематику данного сайта? На данный вопрос был предложено четыре варианта ответа: быстро, долго, я не понял тематику, другое. В пункте другое пользователь мог написать свой вариант.

Далее у пользователя спрашивалась тематика сайта. Данный вопрос был открытого типа. Ответы принимались в свободной форме.

Третий вопрос – на ваш взгляд, дизайн данного сайта сайт соответствует его тематике? На этот вопрос имелось так же четыре варианта ответа: да, нет, не совсем, другое.

В четвертом вопросе предлагалось выбрать из списка элементы сайта, которые помогли пользователю понять тематику: меню, логотип, контент, дизайн, интуиция (в данном случае этот ответ подразумевал тот багаж знаний и навыков, которые имел пользовать ранее), нет таких элементов (это вариант ответа подразумевал, что на сайте нет информации, которая помогла бы пользователю для распознания тематики сайта), другое.

Из десяти рассмотренных сайтов одна половина представляла сайты с устаревшим или странным дизайном, а другая – с современным оформлением и качественным контентом. Выбранные сайты представляли разные стили, сферы деятельности, содержали контент на различных языках.

При анализе полученных данных в целом были выявлены некоторые закономерности:

– для сайтов с устаревшим и странным оформлением основополагающими элементами при распознавании тематики являлись контент и меню. Это говорит о том, что пользователям приходится вчитываться и детально изучать сайт, для того, чтобы понять его тематику. В данном случае таким компонентам, как дизайн и интуиция, пользователи не придают особого значения;

– сайты с устаревшим дизайном, но богатым контентом были быстро поняты пользователями, но не заинтересовали их в должной мере. Почти все опрашиваемые быстро и правильно понимали тематику сайта, но отмечали, что дизайн неинтересен и не подходит для данного сайта;

– тематика сайтов с современным оформлением воспринимается пользователями больше через дизайн и интуицию. Это говорит о том, что пользователь на интуитивном уровне понимает специфику сайта ещё до восприятия контента. Так же привлекательный дизайн создаёт благоприятный имидж компании, что весьма важно для хорошего и правильного сайта;

– ряд сайтов с современным дизайном не был понят респондентами. Обилие графики и малое количество контента запутали пользователей. Это доказывает, что на главной странице сайта должна быть чётко сформулирована его идея, назначение.

Ярким примером грамотного сочетания дизайна и информативности служит один из анализируемых сайтов – сайт продажи музы-

кального оборудования «Libraton». Сочетание большой фотографии товара, двух строк описания к нему, «говорящего» логотипа с птицей и минималистичного дизайна создают приятное впечатление о сайте и побуждают остаться на нём.

На основании выявленных особенностей были сформулированы следующие выводы:

– опыт пользователя оказывает существенное влияние на восприятие сайта в целом;

– дизайн важен, но обилие графики должно быть подкреплено минимальным текстовым сопровождением. Это поможет пользователю подтвердить свои первые догадки о теме сайта и продолжить работу с ним;

– сайты без стилистического оформления понятны пользователю по навигации, логотипу и контенту, но не вызывают у него приятного впечатления и желания продолжать работу.

ЛИТЕРАТУРА

1. Важность пользовательского опыта в веб-дизайне [Электронный ресурс]. – 2016. – Режим доступа: http://www.blog.jazov.com/uiux-design/vazhnost-polzovatelskogo-opyta-v-veb-dizajne.html – Дата доступа: 20.03.2020.