ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ
ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ ИМ. Л.Н. ГУМИЛЕВА
GUMILYOV EURASIAN
NATIONAL UNIVERSITY

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2015» атты X Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ X Международной научной конференции студентов и молодых ученых «Наука и образование - 2015»

PROCEEDINGS of the X International Scientific Conference for students and young scholars «Science and education - 2015»

УДК 001:37.0
ББК72+74.04
Ғ 96

Ғ96
«Ғылым және білім – 2015» атты студенттер мен жас ғалымдардың X Халық. ғыл. конф. = X Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2015» = The X International Scientific Conference for students and young scholars «Science and education - 2015». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie-2015/, 2015. – 7419 стр. қазақша, орысша, ағылшынша.

ISBN 978-9965-31-695-1

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001:37.0
ББК 72+74.04

ISBN 978-9965-31-695-1

быть показана сразу на нескольких устройствах, ею можно будет обменяться с коллегами. Также программа привлекает возможностью создания анимации. Из недостатков лишь то, что программа может быть использован только для MAC (системы IOS). Также отсутствует библиотека файлов.

Slide Bureau - интересное программное обеспечение. Он в основном используется для IPADов, но он позволяет людям создавать презентации, которые консервативнее традиционных файлов PowerPoint. Интерфейс сосредоточен на готовых шаблонах, но они разделены на категории, что позволяет сделать профессиональную презентацию, несмотря на простоту в использовании. Как и SlideDog, программа может бытьиспользована только на Ipad. Из недостатков - затруднительное создание презентаций без шаблонов.

1. Для пользователей из творческой среды будут интересны программы Projeqt и PowToon.

Projeqt- это программное обеспечение способно объединять вместе рассказы и Flickr фотографии, RSS-каналы, твиты, YouTube или Vimeo видео, и любые средства массовой информации, хранящиеся на компьютере. Имеет возможность создавать профессиональные презентации без затруднений, но к сожалению, программе недостает вариаций компоновки.

PowToon, вероятно, один из лидеров в создании презентаций анимационного пространства. PowToon позволяет потребителям создавать презентации и видеозаписи, анимированные, интересные и привлекательные. Это программное обеспечение-глоток свежего воздуха для тех, кто хочет создавать яркие презентации. Имеет возможность создавать анимированные презентации без затруднений, так как программа легка в использовании.

На данный момент, создано очень много программного обеспечения для создания презентаций. В данной статье рассмотрена программа PowerPoint и её возможные аналоги: Emaze, CustomShow, HaikuDeck, Clearside, Kineticast, MotherShip, SlideDog,Prezi, Keynote, Slide Bureau, Projeqt и PowToon.Программы различны своим целевым направлениям, техническим возможностям и стоимости. HaikuDeck, Clearside и Kineticast будут интересны маркетологам; MotherShip, SlideDog и Prezi – студентам и преподавателям; Keynote и Slide Bureau – пользователем IOS, а Projeqt и PowToon – людям в творческой среде.

Список использованных источников

1. https://ru.wikipedia.org/wiki/Microsoft_PowerPoint
2. http://www.customshow.com/best-powerpoint-alternatives-presentation-programs/
3. http://www.powtoon.com/blog/10-best-powerpoint-alternatives/

УДК 003.09

КРИПТОГРАФИЯ И КОДИРОВАНИЕ ИНФОРМАЦИИ

Айкенова Алина

Студентка 1-го курса, специальности Связь с общественностью

ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Научный руководитель – Ж.Б.Ахаева, старший преподаватель

В XXI веке защита информации, недопущение попадания ее в чужие руки, сохранение конфиденциальности важны как никогда. Все чаще можно встретить закодированную передаваемую информацию. Цель кодирования – облегчить пересылку. Чтобы компьютер мог понять и обработать информацию, она должна быть переведена с языка, на котором написана, на так называемый двоичный язык. Он состоит из двух цифр: 0 и 1. Поэтому текст нужно перевести в двоичный код. После этого следует зашифровать его, чтобы он достался только законному получателю. Кодирование, расшифровка, шифрование, – это ведущие фигуры в обмене информации, которые повторяются ежедневно, ежечасно, ежеминутно

миллионы раз в секунду.

Криптография (тайнопись) - математическая наука о методах сохранения безопасности данных.

Для криптографов термин «кодирование» имеет несколько другой смысл, чем для нас. Для них кодирование – это изменение текста путем замены одних слов другими, а шифрование – это замена отдельных символов или букв.

Изобретение компьютера Colossus и расшифровка кода машины для защищенной связи «Энигма», которая была выбрана Германией для шифрования большей части своих военных донесений в годы Второй мировой войны, открыли путь к величайшей революции в сфере коммуникаций.

В результате работы по взлому кода «Энигмы» появился первый в мире компьютер, что можно считать самым значительным событием в долгой и яркой истории военного криптоанализа.

Гигантский шаг вперед произошел в значительной степени благодаря развитию систем шифрования, что обеспечило безопасную, эффективную и быструю связь по разветвленным сетям, представляющим собой компьютеры и их пользователей – то есть нас с вами.

Двоичная система – основа технологической революции. Этот суперпростой код, содержащий только два символа 0 и 1, используется в цифровых устройствах из-за его способности представлять состояние электронных смех: единица означает, что в контуре есть ток, ноль – нет.

Одна двоичная цифра 0 или 1 называется битом.

Особый набор символов, состоящий из восьми битов, является байтом, обозначающий символ, будь то букву или цифру. Они же и лежат в основе обычных коммуникаций, называющихся ASCII-кодами («американская стандартная кодировочная таблица»). В свою очередь ASCII-коды позволяют пользователям вводить текст в компьютер. Когда мы печатаем символ, компьютер превращает этот его в байт. К примеру, если мы напечатаем букву «А», компьютер превратит ее в 0100 0001.Двоичные ASCII-коды существуют для символов, которые включают в себя строчные буквы(26), заглавные буквы(26), цифры(10), символы пунктуации(7), а также некоторых специальных символов. Так, для каждого символа есть свое десятичное число.

Также в вычислениях используется еще один известный код. Шестнадцатеричная система - это система счисления, которая использует 16 особых символов, в отличие от системы с десятью цифрами (десятичной). Можно сказать, что шестнадцатеричная система является вторым языком компьютеров после двоичной системы. Байт – это комбинация двух шестнадцатеричных чисел. Шестнадцать цифр шестнадцатеричной системы – это традиционные цифры 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, и еще шесть символов, выбранных по соглашению: A, B, C, D, E, F. Числа в шестнадцатеричной системе записываются следующим образом:

- От 0 до 15: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.
- От 16 до 31: 10,11, 12, 13, 14, 15, 16, 17, 18, 19, 1A, 1B, 1C, 1D, 1E, 1F.
- От 32 и дальше: 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 2A, 2B, 2C…

При быстром развитии вычислительной техники криптография не игнорировалась. Процесс шифрования с помощью компьютера почти не отличается от шифрования без компьютера, но есть три основных отличия.

- Во-первых, компьютер можно запрограммировать для имитации работы обычной шифровальной машины, что избавляет от необходимости физически создавать такие устройства.
- Во-вторых, компьютер работает только с двоичными числами и, следовательно, все шифрование будет происходить на этом уровне (даже если числовая информация потом снова будет переведена в текст).
- В-третьих, компьютеры очень быстро работают с вычислениями и

расшифровывают сообщения.

Первый шифр, предназначенный для того, чтобы воспользоваться потенциалом компьютером, был разработан в 1970-х гг. Например, «Люцифер», шифр который разделял текст на блоки по 64 бита и зашифровывал некоторые из них с помощью сложной подстановки, а затем группировал их снова в новый блок зашифрованных битов и повторял процесс. Для работы такой системы было необходимо, чтобы отправитель и получатель имели компьютеры с одной и той же программой шифрования, а также общий цифровой ключ. DES, 56-битная версия шифра «Люцифер», была разработана в 1976 г.DES(DataEncryptionStandart – «стандарт шифрования данных») по-прежнему пользуется в наши дни, хотя и шифр был взломан в 1999 г. И заменен 128-битным AES (AdvancedEncryptionStandart) в 2002г.

Без сомнения, такие алгоритмы шифрования сполна использовали вычислительную мощь компьютеров, но, как и их предшественники тысячелетней давности, компьютерные шрифты по-прежнему были уязвимы, поскольку несанкционированный получатель мог перехватить ключ и, зная алгоритм шифрования, расшифровать сообщение. Этот основной недостаток каждой «классической» криптографической системы известен как проблема распределения ключей.

Список использованных источников

1. Кодирование информации: методические указания / сост.: В. Д. Горбоконенко, В. Е. Шикина. – Ульяновск: УлГТУ, 2006. – 56
2. Нечаев В.И. Элементы криптографии (Основы теории защиты информации): учебное пособие для университетов и педвузов. /Под.ред. В.А. Садовничего. - М.:Высш. шк., 1999. 256
3. Бекман И.Н. Компьютеры в информатике: курс лекций [Электронный ресурс] // Лекции. - URL: http://profbeckman.narod.ru/EVM.htm (дата обращения 15.03.2015)
4. Гомес Ж. - Математики, шпионы и хакеры. Кодирование и криптография (Мир математики) – 2014
5. http://nashol.com/2015010381355/mir-matematiki-matematiki-shpioni-i-hakeri-kodirovanie-i-kriptografiya-tom-2-gomes-j-2014.html
6. http://www.furfur.me/furfur/culture/culture/166567-kriptografiya
7. https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F
8. http://www.banner-agent.ru/materials/ascii-kod
9. http://www.banner-agent.ru/materials/kody_shifry_i_klyuchi
10. http://urss.ru/PDF/add_ru/193137-1.pdf

ӘОК: 372.167.1:002

МУЛЬТИМЕДИАЛЫҚ ОҚЫТУ ЖҮЙЕЛЕРІН ӘЗІРЛЕУ ЖӘНЕ МАТЕРИАЛДАРДЫ БЕРУ ҚАҒИДАЛАРЫ

Айлауова Жансая Сламханқызы
Калбаев Азизбек Махмудович
Jons_301193@inbox.ru
Ғылыми жетекшісі - Давлетова А.Х., п.ғ.к., академик ХАА,
Л.Н. Гумилев атындағы Еуразия ұлттық университеті

Стратегиялық проблемалар жөніндегі мамандар қашықтан оқыту формасын 21 ғасырдың білім беру жүйесі деп атап жүр. Бұл күні оған үлкен мән беріліп отыр. Бұрын технологияларға бағытталған қоғамдық прогрестің нәтижелерінің бүгінде ақпараттық аймақта орталықтандырылып жатқаны қашықтан оқытудың маңыздылығын арттырды.