Секция 1

ИНФОРМАТИКА И МАТЕМАТИКА

А.А. АБЛАЙ,
студент направления подготовки «Прикладная информатика»
Е.А. КИСЕЛЁВА,
доцент Алматинского филиала Санкт-Петербургского Гуманитарного университета профсоюзов, кандидат педагогических наук – руководитель

О ТЕХНОЛОГИИ QR-КОД И ПРАКТИКЕ ЕЕ ПРИМЕНЕНИЯ

В 2016 году такие приложения, как Whatsapp и Messenger Facebook, используют QR-коды как функцию для авторизации и добавления друзей. Бренд Coca-Cola использовали QR-код в качестве инструмента для маркетинговой компании. Крупные магазины используют QR-коды для приема платежей. Трудно представить, что такой простой инструмент, как QR-код, может все так упростить. QR-код стал частью нашей современной жизни, которой надо уметь пользоваться. Поэтому наша цель – провести систематизированный анализ данной перспективной технологии.

QR-код (quick response с англ. – «быстрый отклик») – это двухмерный штрих-код (матричный код), который был разработан «Denso Wave» (японской дочерней компанией Toyota) в 1994 году. Он позволяет в одном небольшом квадрате поместить 2953 байта информации, то есть 7089 цифр или 4296 букв, или 1817 иероглифов. Изначально QR-код использовался для замены штрих-кодов, для ускорения процесса производства деталей для автомобилей [Что такое QR-code? – URL: https://ylianova.ru].

В отличие от старого штрих-кода, который сканируется тонким лучом, QR-код определяется датчиком или камерой как двумерное изображение. Три квадрата в углах изображения и меньшие синхронизирующие квадратики по всему коду позволяют нормализовать размер изображения и его ориентацию, а также угол, под которым датчик расположен к поверхности изображения. Точки переводятся в двоичные числа с проверкой по контрольной сумме.

Кодировать информацию в QR-код можно несколькими способами. Выбор конкретного способа зависит от того, какие символы используются. Можно применить побайтовое кодирование

– это универсальный способ кодирования, им можно закодировать любые символы: 1) цифровое кодирование, если используются только цифры от 0 до 9; 2) алфавитно-цифровое кодирование, если кроме цифр необходимо зашифровать буквы латинского алфавита, пробел и символы ±*/$.%:*. Для шифрования китайских и японских иероглифов существует кодирование кандзи.

Перед каждым способом кодирования создаётся пустая последовательность бит, которая затем заполняется.

На QR-коде присутствуют обязательные поля, они не несут никакой закодированной информации, но содержат информацию для декодирования. Это:

– поисковые узоры;
– выравнивающие узоры;
– полосы синхронизации;
– код маски и уровня коррекции;
– код версии (с 7–й версии);
– обязательный отступ вокруг кода. Отступ – это рамка из белых модулей, её ширина – 4 модуля [Технические характеристики QR-кодов. – URL: https://creambee.ru].

Общий вид обязательных полей представлен на рисунке 1, данном ниже.

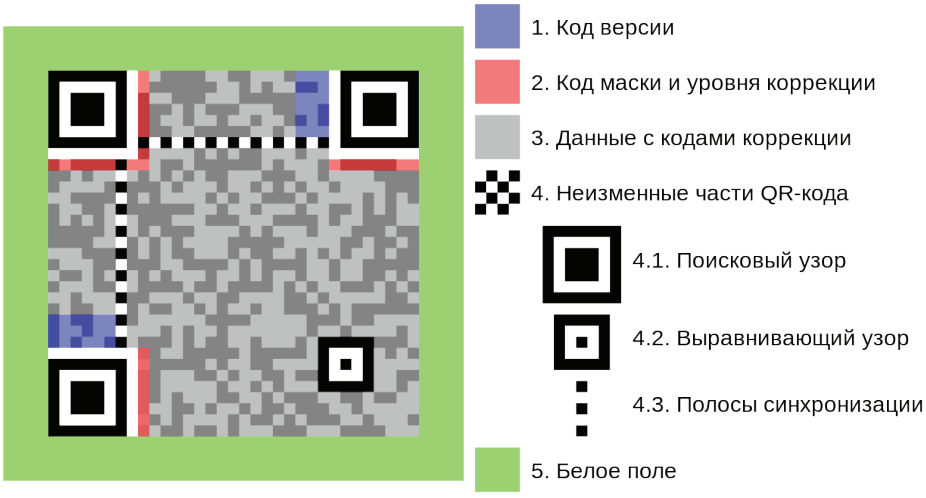


Рисунок 1 – Описание полей QR-кода

Основное использование QR-кодов:

1. Чеки и билеты. В 2019 году QR-код законодательно обязали наносить на чек кассового аппарата, на котором будет содержаться полная электронная копия чека. Использование QR-кода на билетах

облегчает проверку на подлинность, тем самым практически минимизировав использование подделок. В современной тенденции чеки можно сканировать для получения кэшбека.

2. Музеи и достопримечательности. В музеях можно подойти к экспонатам и, отсканировав код, получить всю информацию сразу на смартфоне. Иногда практикуется использование стороннего программного обеспечения, которое предоставляет более обширную информацию с диктором или дополненной реальностью.

3. Клиники для животных интегрируют QR в бирки и ошейники. В коде зашифрованы не только данные о самом питомце, но и контакты его хозяина. Технология помогает опознать домашнее животное, если оно потерялось, и вернуть его владельцу.

4. Безналичные платежи. Современные банки имеющие мобильные приложения для ускорения проведения платежей могут использовать QR-код за счет того, что не нужно вводить реквизиты, в следствии чего пользователь не совершит ошибочный перевод.

5. Предоставление информации. Оставлять визитку со своими данные уже не нужно, намного легче оставить изображение QR-кода, с помощью которого с вами смогут мгновенно связаться, у пользователя сразу откроется диалог с вами в мессенджере.

6. Библиотеки. По программе «Рухани жаңғыру» в библиотеках предоставляют электронные копии книг, сканировав код, можно полностью скачать книгу, выбрав любой язык.

7. Авторизация на сайтах используя QR-код. Такой способ аутентификации гораздо безопаснее, так как не указывается логин и пароль, по каналам связи передается только хэш, сгенерированный на основе пароля пользователя (master key) и уникального одноразового кода, зашифрованного в QR-коде (одноразовый код добавляется в URL). Мобильное приложение SQRL генерирует хэш и отправляет его на сервер для аутентификации (рис. 2).

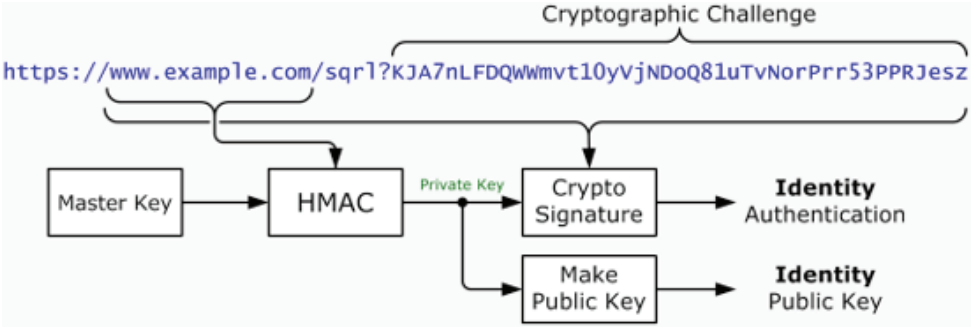


Рисунок 2 – Алгоритм SQRL

Таким образом, QR-кодирование обладает рядом преимуществ, которые в совокупности с использованием кодированных данных обеспечивают надежную защиту и быстрый доступ к информации со стороны потребителя.

А.Ю. ГАЙНУЛЛИНА,
студентка направления подготовки «Экономика»
Л.Х. ЖУНУСОВА,
доцент Алматинского филиала Санкт-Петербурского Гуманитарного университета профсоюзов, кандидат технических наук – руководитель

ПРИМЕНЕНИЕ МАТРИЧНОЙ АЛГЕБРЫ В ЭКОНОМИКЕ

Матрица позволяет оперировать с массивами чисел, функций или математических символов. Она имеет широкое распространение и используется в различных отраслях знаний, таких, например, как: математика, физика, информатика, экономика и многие другие. Именно матрицы позволяют решать различные сложные задачи и уравнения.

Бесспорна роль математики и математического моделирования в изучении различных закономерностей в экономике. Исходя из этого, является актуальной задача анализа математических методов с целью выявления тенденций развития экономической системы и применения их для прогнозирования.

Математика и экономика – это самостоятельные отрасли знаний, каждая из которых обладает своим объектом и предметом исследования. Математика – наука о структурах, порядке и отношениях, которая исторически сложилась на основе операций подсчёта, измерения и описания форм реальных объектов. Экономика – хозяйственная деятельность общества, а также совокупность отношений, складывающихся в системе производства, распределения, обмена и потребления.

Экономическая наука, как и любая другая, имеет свою специфику. Специфика ее определяется общей спецификой наук о человеке. Все общественные науки изучают самую сложную и высокоорганизованную форму движения – социальную. На данном уровне организации материи приходится учитывать обратную связь между субъектом и внешней средой. При этом связь эта представляет противоречивое единство интересов и целей отдельных организмов, участвующих в том или ином процессе. Экономическая наука изучает большой пласт процессов, как прямо имеющих место между субъектами при обмене различными продуктами, так и имеющих к

этому какое-либо отношение. До того, как люди стали обмениваться продуктами своего труда, отношения между ними никак нельзя было назвать экономическими. Возникновение экономических отношений положило начало специализации труда и соответственно, всему социально-экономическому прогрессу.

Цель нашего исследования – обоснование роли линейной алгебры для анализа деятельности экономической системы и изучения проблемы в экономике.

Сама матрица – это математический объект, который записывается в виде прямоугольной таблицы, которая в свою очередь представляет собой совокупность строк и столбцов, на пересечении которых находятся её элементы. Количество строк и столбцов матрицы задают размер матрицы. Хотя исторически рассматривались, например, треугольные матрицы, но в настоящее время говорят исключительно о матрицах прямоугольной формы, так как они являются наиболее удобными и общими.

В современной экономике используется множество математических методов, разработанных в XX веке. Эти математические методы применяются для решения различных задач как на малых предприятиях, так и на крупных. Современная экономика пользуется разработанными методами Л.В. Канторовича, В.В. Леонтьева, Е.Е. Слуцкого [Логвенков С.А., Самовол В.С. Линейная алгебра //Основы теории, примеры и задачи. М., 2017].

Среди основных методов решения различных экономических задач наиболее популярно использование элементов алгебры матриц. Это особенно актуально и важно при разработке, форматировании и использовании баз данных, где почти вся информация хранится и обрабатывается в матричной форме. Решение многих экономических задач приводит к составлению и решению систем линейных алгебраических уравнений. Ярким примером может являться составление прогноза выпуска продукции по известным запасам сырья.

Понятие матрицы и основанный на нем раздел математики – матричная алгебра – имеют большое значение для всех экономистов. Основная часть математических моделей экономических объектов и процессов записывается в простой и компактной матричной форме. С помощью матриц удобно описывать различные экономические закономерности, что намного упрощает долгие вычислительные операции [Малугин В.А. Линейная алгебра для экономистов: Учебник, практикум и сборник задач. Люберцы, 2016, с.64-68].

Например, удобно записывать распределения ресурсов по отдельным отраслям экономики. К примеру, имеется 3 разных вида

ресурсов и 3 определенных отрасли экономики (промышленность, сельское хозяйство и строительство). Все показатели можно записать в виде матрицы, которая будет размером 3*3.

Еще одним примером, который подходит для описания пользы матриц в экономике, является решение задач. К примеру, предприятие выпускает три вида продукции и на производство данной продукции использует два вида сырья. План выпуска продукции задан одной матрицей-строкой, а стоимость каждого сырья задана матрицей-столбом. И нужно найти общую себестоимость сырья. При помощи составления общей матрицы каждый элемент будет показывать, сколько сырья определенного типа может быть израсходовано на производство какого-то типа. А также при помощи нахождения затрат на сырье каждого вида можно найти общую стоимость сырья.

Таким образом, после всего вышесказанного, можно сделать вывод, что в экономической сфере активно используется матричный метод. Такой метод применяется с целью анализа сложных и многомерных экономических явлений. Чаще всего этот метод используется при необходимости сравнительной, сопоставительной оценки функционирования организаций и их структурных подразделений. Следовательно, матричный метод в экономике – это метод научного исследования свойств объектов на основе использования правил теории матриц, благодаря которым определяется значение элементов той модели, которая отражает все взаимосвязи экономических объектов. Используется матричный метод именно в тех случаях, когда главным объектом исследования являются балансовые соотношения затрат и результатов производительно-хозяйственной деятельности.

В заключение отметим, что легкость и простота использования этих элементов линейной алгебры как в теории, так и на практике играет важнейшую роль в решении экономических задач. Данный метод уменьшает, облегчает и улучшает работу человека. Применяя матрицы, экономист получает готовый и обоснованный ответ в виде некоего рейтинга, таблицы, показывающей все возможные альтернативы по всем критериям, а также ему предлагается проанализировать результаты и выявить всю происходящую ситуацию в производстве. Именно такое быстрое, скоростное решение довольно сложных задач и дальнейший анализ проведенной работы может привести к максимально оптимальным вариантам и, впоследствии, к улучшению всего экономического фактора производства.

Р.Т. ГАРЫНИН,
студент направления подготовки «Прикладная информатика»
Т.Г. ПЛОТНИКОВА,
доцент Алматинского филиала Санкт-Петербургского Гуманитарного университета профсоюзов – руководитель

ИСПОЛЬЗОВАНИЕ АВТОНОМНЫХ ЭМУЛЯТОРОВ КОМПЬЮТЕРОВ ДЛЯ ЗАЩИТЫ ОТ КИБЕРУГРОЗ

Виртуальная машина – это искусственно созданный при помощи специального программного обеспечения виртуальный компьютер. Процесс изоляции объектов в виртуальной машине называется виртуальной изоляцией. Виртуальная изоляция является хорошим инструментом защиты, но далеко не безупречным. В данной работе будет рассмотрено, как можно преодолеть барьер в виде виртуальной среды и как защититься от этой угрозы.

Организацию виртуальной машины можно осуществить с помощью VirtualBox [URL: https://ru.wikipedia.org]. У пользователей периодически появляется необходимость загружать в виртуальную машину файлы с основной машины (или, наоборот, в основную с виртуальной). Пользователь для осуществления такой необходимости использует такие инструменты, как общая папка, общий буфер обмена и функция прямого перемещения файлов Drag'n'Drop [URL: http://ru.wikipedia.org], которые идут в дополнении VirtualBox Guest Additions [URL: http://ru.wikipedia.org].

Согласно мнению исследователей, 85% инструментов для выхода за пределы виртуальной среды VirtualBox требуют наличие VirtualBox Guest Additions и сопутствующего функционала [URL: http://book.cyberyozh. com/ru].

Как альтернатива использованию данного функционала существует несколько вариантов.

Один из вариантов – организация взаимодействия хостовой и гостевой машины через облачное хранилище, предоставив виртуальной машине доступ к одной из папок в Google Диск, Яндекс.Диск или Dropbox, или завести отдельный аккаунт облачного хранилища исключительно для этих целей. Все, что может злоумышленник, получив доступ к вашей виртуальной машине, – загрузить или удалить в облачном хранилище какие-либо файлы. Разумеется, остается вероятность, что он как-то вынудит пользователя запустить скомпрометированный файл из облака на основной машине.

Второй вариант – взаимодействие через мессенджер. Для этого метода необходимо установить мессенджер на гостевую и основную систему и передавать файлы или ссылки путем отправки сообщений.

К сожалению, роутеры, как правило, оказываются уязвимыми для атак, а, получив доступ к роутеру, можно провести полноценную атаку на подключающиеся к нему устройства. Для этого метода злоумышленник, имея доступ к виртуальной машине, производит атаку на роутер. Далее происходит атака на подключенные к роутеру устройства, в том числе и хост-систему.

Можно выйти за пределы виртуализации и через USB-флешку, если она будет в этот момент подключена к виртуальной машине, а затем подсоединена к основной системе. В некоторых случаях можно провести атаку через средство беспроводной связи Bluetooth [URL: https://ru.wikipedia.org] на находящиеся поблизости устройства.

Для защиты от этого метода выхода из виртуальной машины рекомендуется позаботиться о безопасности своего Wi-Fi-роутера. В дополнение рекомендуется использовать виртуальную частную сеть (VPN) [URL: http://ru.wikipedia.org], которая поможет предотвратить последующую атаку. Также можно отключить возможность взаимодействия гостевой системы с USB-контроллерами и Bluetooth-модулями.

Одним из методов выхода из гостевой системы является нахождение уязвимостей. К сожалению, в продуктах виртуализации ежегодно обнаруживаются уязвимости, позволяющие злоумышленникам покинуть пределы виртуальной изоляции и атаковать основную машину. Необходимые для этого инструменты есть у спецслужб и связанных с ними хакерских группировок, такие инструменты ежегодно демонстрируются на хакерских конференциях.

Рекомендовано при возникновении подозрений в атаке высококвалифицированных хакеров использование аппаратной изоляции – использование полностью изолированного от основной машины компьютера. Виртуальная изоляция уязвима, и никогда нельзя исключать возможность наличия у недоброжелателей инструментов для выхода из используемой системы виртуализации.

При использовании программной изоляции необходимо своевременно обновлять эмулятор компьютеров и все компоненты, используемые на виртуальной машине.

Для выхода за пределы виртуальной среды иногда применяется метод, называемый «социальная инженерия». Многие современные вредоносные программы анализируют окружающую среду на предмет наличия виртуализации и, если обнаруживают, либо не запускаются

совсем, либо не активируют вредоносные функции. Это помогает скрываться от анализа экспертами и при различных автоматических и полуавтоматических проверках. Для среднестатистического пользователя необходимо помнить, что отсутствие вредоносной активности в виртуальной среде не означает, что ее не будет при запуске на основной системе.

Такой вид вредоносных программ известен под именем руткит [URL: http://habr.com/ru]. Для выявления руткитов существует ряд программных решений, среди них можно особо выделить Hypersight Rootkit Detector, так как это единственная программа, которая имеет функционал, определяющий руткит, работающий в режиме hypervisor [URL: https://habr.com/ru].

Известно немало случаев, когда люди тестировали программу на виртуальной машине и, не обнаруживая ничего подозрительного, запускали ее в основной системе и тем самым предоставляли доступ злоумышленникам к главной машине. Иногда вредоносная программа не маскируется, а сообщает пользователю о невозможности запуска в виртуальной среде, тем самым подталкивая его запустить файл в основной системе.

Анализируя вышеперечисленное, можно сформулировать следующие рекомендации по использовании автономных эмуляторов компьютеров:

– отказаться от использования таких функций, как: общая папка, общий буфер обмена и Drag’n’Drop (или их аналогов в других автономных эмуляторах компьютеров); а в качестве альтернативы рекомендуется использование облачного хранилища или мессенджера;

– позаботиться о безопасности Wi-Fi роутера;

– использовать VPN;

– отключить возможности использования гостевой машиной USB- устройств и Bluetooth-модулей;

– использовать программные решения, выявляющие руткиты.

Таким образом, были рассмотрены основные возможности проникновения злоумышленников из гостевой системы в основную, а также методы защиты от вышеперечисленных угроз. Было определено, что виртуальная изоляция не является полноценной заменой аппаратной изоляции, хотя и может быть использована при выполнении ряда вышеперечисленных рекомендаций.

Х.Х. ДАВЛЕТЬЯРОВ,
студент направления подготовки «Прикладная информатика»
Т.Г. ПЛОТНИКОВА,
доцент Алматинского филиала Санкт-Петербургского Гуманитарного университета профсоюзов – руководитель

УГРОЗЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ (IOT)

Повсеместное использование современных информационных технологий увеличивает опасность киберугроз как на бизнес-уровне, так и в частной жизни. В современном мире в глобальную сеть могут выходить не только компьютеры, смартфоны, планшеты, но также смарт-телевизоры, камеры видеонаблюдения, «умные» часы (smartwatch), холодильники, автомобили, фитнес-трекеры, видеорегистраторы. Количество таких устройств уже превышает несколько миллиардов, и с каждым годом их становится больше и больше. Проблемы безопасности использования подобных устройств очень актуальны.

Целью данной работы является изучение угрозы безопасности Интернета вещей (IoT).

Согласно определению Gartner, «IoT — сеть физических объектов, содержащих встроенные технологии связи и взаимодействия с внутренними состояниями или внешней средой» [URL: http://www.itweek.ru]. Сегодня многие устройства управляются встроенными операционными системами и соединены с Интернетом, что создает новые возможности для потребителей. Аналитики полагают, что в ближайшее время количество подобных устройств превысит 100 миллиардов.

Большинство устройств IoT имеет плохую или не имеет совсем защиты от кибератак. Для их подключения часто используются простые пары «логин – пароль», которые автоматически устанавливаются на различные модели. Следует отметить, что владельцы устройств часто не задумываются об изменении настроек, иногда это нельзя сделать из-за ограничений самих производителей. Злоумышленники относительно легко получают доступ к таким устройствам, используя подбор комбинаций по словарю, а также используя уязвимости установленных на них операционных систем.

Существует большое множество приложений для систем IoT. Это системы сигнализации дома и объектов охраны, передающие информацию на смартфон и другие устройства; смарт-часы, которые собирают медицинские данные, совместно используемые с врачами;

гаджеты, вычисляющие оптимальный маршрут; холодильники, напоминающие хозяевам купить необходимые товары, и пр. На макроуровне это «умные» городские приложения, такие как «умная» парковка и «умное» освещение. IoT обеспечивает бесконечные возможности, многие из которых мы пока не можем себе вообразить.

Рынок IoT активно развивается, его развитие предполагает открытие новых рынков, обеспечивая огромным количеством данных о покупательских привычках покупателей для дальнейших возможностей управления продажами.

Нельзя не учитывать, что могут возникнуть угрозы и со стороны Интернета вещей, которые связаны с безопасностью и конфиденциальностью. Типичный тому пример произошел не так давно, когда исследователи на примере взлома бортовой коммуникационной системы Jeep показали, как можно взять под свой контроль автомобиль. То, что это не единичный пример, было отмечено в исследовании компании PT&CLWG. Судебные специалисты указали, что изделия многих автомобилестроительных компаний могут быть взломаны [URL: http://www.itweek.ru].

Инциденты IoT могут использоваться не только для хищения информации (как кибератаки), но и для нанесения физического вреда и непосредственного ущерба. Расширение Интернета вещей может привести к появлению большого количества угроз для корпоративной и частной безопасности. Согласно Роберту Бигмену, бывшему CISO ЦРУ США, «устройства IoT, управляющие персональными медицинскими системами, станут следующим золотым дном для шантажа и получения выкупа» [URL: http://www.itweek.ru]. В связи с этим компании должны адаптировать свои методы управления рисками и расширять свои оценки рисков. Например, если гаджеты сотрудников могут быть использованы для перехватов информации корпоративного сети, то такие устройства попадают под оценку риска корпоративной информационной безопасности.

Следует отметить, что на данный момент нет абсолютного способа защититься от угроз Интернета вещей, но есть методы улучшения защиты узлов системы IoT.

Для обеспечения защиты конечных узлов системы IoT необходимо проводить анализ прошивки с последующей сертификацией на отсутствие недокументированных возможностей, усиление защиты (харденинг) операционной системы. Важно выявлять уязвимости в режиме реального времени, проводить корректную настройку встроенного межсетевого экрана, предотвращая вторжения как на прикладном уровне, так и на уровне протоколов передачи данных.

Необходимо внедрение контроля целостности прошивки, а также создание единого центра сертификации или децентрализованной доверенной системы аутентификации для общения между различными устройствами.

Важно осуществлять защиту облачной инфраструктуры, которая осуществляет управление и мониторинг, агрегирует и анализирует информацию, получаемую от IoT-устройств. Следует организовать работу таким образом, чтобы сеть и серверы были недоступны для атак. Результаты исследования фирмы HP показали, что «70% устройств, подключенных к IoT, имеют уязвимости, в числе которых можно назвать проблемы с безопасностью паролей, шифрованием трафика, а также полное отсутствие строгого контроля над доступом к информации пользователя» [URL: http://go.saas.hpe.com].

Разрабатывая направления защиты IoT-систем в целом, «необходимо тщательно прорабатывать требования информационной безопасности, детально анализировать риски, появляющиеся с внедрением тех или иных технологий IoT, и выстраивать систему с учетом минимизации этих рисков. На сегодняшний день лучшим решение было бы использовать IoT только для тех бизнес-процессов, нарушение функционирования которых не приводит к драматическим последствиям для бизнеса и здоровья людей» [URL: https://www.securitylab.ru].

Тысячи высокотехнологичных устройств, которые пользователи всё чаще применяют в повседневной жизни, фактически являются маленькими компьютерами с присущими им недостатками. Они подвержены аналогичным атакам и уязвимостям, при этом из-за особенностей и ограничений конструкции защитить их может быть значительно сложнее или же вовсе невозможно. Кроме того, многие пользователи не до конца осознают потенциальные риски и всё еще воспринимают «умные» устройства как безопасные и удобные «игрушки».

Таким образом, рассмотрев понятие Интернета вещей, а также угрозы, которые представляют для пользователей эти устройства, можно сделать вывод, что на данный момент технологии, которые используют IoT, имеют много недостатков и слабые места в защите, но в настоящее время эти технологии развиваются, и возможно в ближайшем будущем производители смогут решить данную проблему.

А.А. ДЕРИПАСКИНА,
студентка направления подготовки «Прикладная информатика»
С.Ж. КАРАТАБАНОВА,
доцент Алматинского филиала Санкт-Петербургского Гуманитарного университета профсоюзов, кандидат физико-математических наук – руководитель

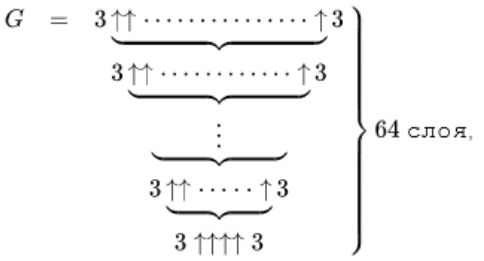
СВЕРХБОЛЬШИЕ ЧИСЛА И СПЕЦИФИКА ИХ ПРИМЕНЕНИЯ

Современная математика нуждается в использовании натуральных чисел, характеризующих понятие «сложность объекта». В первую очередь объектом, для которого измеряется сложность, является алгоритм. Вторым оцениваемым по сложности объектом является процесс вычисления, производимый с помощью некоторого алгоритма. И, наконец, третий объект с числовой оценкой его сложности – это физически реализуемый объект, требующий определенных энергетических затрат на своё создание.

Для всех трёх аспектов понятия «сложность» применяются числа, которым присвоены разные математические категории. На сегодняшний день категорий выделено только четыре: малые, средние, большие и сверхбольшие числа. Деление на категории производится по законам комбинаторики и теории нумераций. Описание четырех категорий может учитывать применение ЭВМ, но в данной статье мы имеем ввиду только вычислительные возможности человека [Расёва Е., Сикорский Р. Математика метаматематики. М., 1972, с.101].

Рассмотрим некоторые примеры чисел из категорий большие и сверхбольшие и проследим, при решении каких математических задач эти числа возникли.

В 1977 году появилось популярное описание, опубликованное Мартином Гарднером для большого числа G, использованного в доказательстве одной теоремы в комбинаторной теории Рамсея. В честь автора этого доказательства Рональда Грэма число было названо числом Грэма. Интересно, что Рональд Грэм был просто математиком-любителем, а работал он жонглером в цирке. В 1980 году это число попало в Книгу рекордов Гиннеса и стало необыкновенно популярным. Чтобы оценить его величину, попробуем сравнить его с числом гуголплекс. В первую очередь дадим определение на языке стрелочной нотации Дональда Кнута:



$G=g_{64}=3\uparrow g_{63}3=3\uparrow\ldots\uparrow 3$, и количество стрелок равно g_{63} [Кнут Д. Искусство программирования. Том 1. Основные алгоритмы. М., 2006, с.99].

Расшифруем эти вычисления:

$g_1=3\uparrow\uparrow\uparrow\uparrow 3$,

$3\uparrow 3=3^3$, $3\uparrow\uparrow 3=3\uparrow 3\uparrow 3=3^{3^3}=3^{27}>7\cdot 10^{12}$, т.е. 7 триллионов.

$3\uparrow\uparrow\uparrow 3=3\uparrow\uparrow 3\uparrow\uparrow 3$,

$3\uparrow\uparrow\uparrow\uparrow 3=3\uparrow\uparrow\uparrow 3\uparrow\uparrow\uparrow 3$,

переходим к $g_2=3\uparrow_{g_1}3$.

Итак, g_1 – это количество стрелок в числе g_2, g_2 – количество стрелок в g_3и т.д. Наконец, $G=g_{64}$.

$g_1>3^{7\cdot 10^{12}}$.

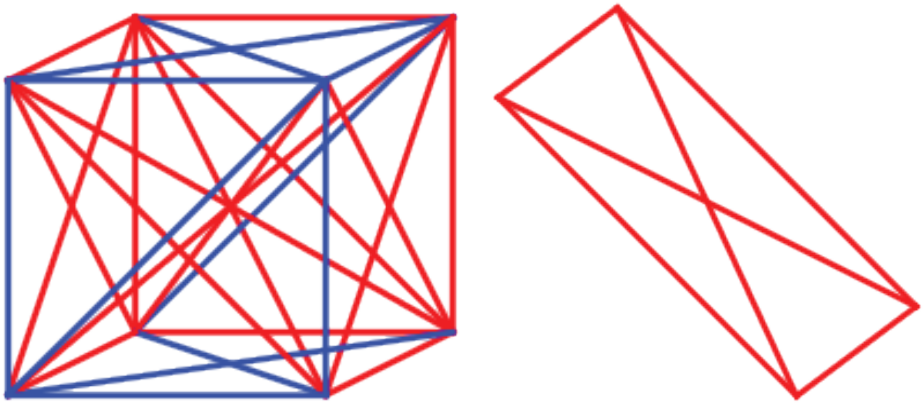
Попробуем оценить размеры Вселенной по данным космологов. Диаметр Вселенной в метрах имеет порядок 10^{26}, что даёт возможность поместить в неё 10^{80} атомов. По сравнению с гуголплекс, который равен $10^{10^{100}}$, это немного. Перейдем к другому масштабу.

Есть так называемый наименьший планковский объём, это порядка 10^{-35} в кубе, т.е. 10^{-105} метра кубического. Считая приблизительно, что наименьший объём есть 0,0…01 (105 знаков после запятой), получим, что Вселенная вмещает 10^{183}планковских объемов. Это больше, чем googol, но много меньше, чем гуголплекс, равный 10^{googol}. Число $googol=10^{100}$придумал американский математик Эдвард Казнер, чтобы оценивать объём Вселенной, который, как уже говорилось, равен $10^{26\cdot 3}$ метров кубических. Нельзя забывать, что под Вселенной мы понимаем только наблюдаемую Вселенную как шар диаметром 93 миллиарда световых лет, а размеры нашей галактики 167 млрд световых лет.

Итак, видимая Вселенная не позволяет явно выписать все знаки числа гуголплекс. Что касается числа Грэма G, то уже число $3\uparrow^3 3$ намного превосходит гуголплекс, не говоря уже о числах g_1, g_2 и т.д. Последовательностью Грэма называют $\{g_i\}$.

Число G можно использовать в математике. Дело в том, что существует задача Грэма, решением которой должно быть число, заключенное в интервале между 13 и G [Кнут Д. Искусство программирования. Том 2. Основные алгоритмы. М., 2006, с.225].

Приведём формулировку проблемы Грэма для размерности $n=3$. Дан куб, являющийся полным графом с 8 вершинами. Его изображение приводится на левом рисунке. Всего 28 ребер [URL: http://ru.wikipedia.org].



Полные подграфы, содержащие некоторые 4 вершины, изображены на правом рисунке. Требуется, чтобы среди 6 ребёр, соединяющих вершины такого прямоугольника или квадрата, не было монохромного набора, т.е. только красного или только синего цвета.

Для размерностей 3,4,5,6,…,13 задача разрешима, естественно, при замене плоскости на гиперплоскость. Доказательство существования правильной раскраски гиперкуба проводится методами комбинаторики. В 1971 году Грэм показал, что при некотором n_0, $6<n_0\leq G$, правильная раскраска невозможна для ребер n_0 – мерного гиперкуба. Т.е. найдутся четыре точки, лежащие в одной гиперплоскости и соединённые обязательно 6 ребрами одного цвета.

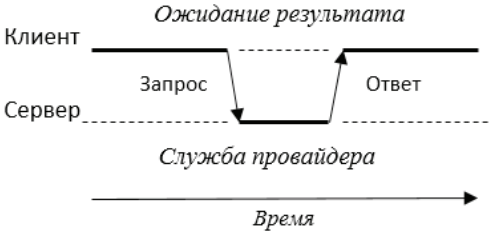
В 2008 году математики улучшили границы для n_0 до $13<n_0\leq G$. Это лучший результат на сегодняшний день в теории Рамсея о цветных графах. Кстати, сегодня известны 500 последних цифр числа G.

В заключение можно упомянуть числа, полезные в математике и при этом по величине ещё большие, чем число Грэма. Это числа Райо, построенные в 2007 году. В любом случае такие числа служат как образцы для описания быстрорастущих вычислимых функций. Ещё есть число Стасплекс, равное g_{100}, которое тоже используется математиками.

Д.С. ДУЙСЕБАЕВ,
студент направления подготовки «Прикладная информатика»
Г.А. АБДУЛКАРИМОВА,
доцент Алматинского филиала Санкт-Петербургского Гуманитарного университета профсоюзов, кандидат педагогических наук – руководитель

КЛИЕНТ-СЕРВЕРНЫЕ ТЕХНОЛОГИИ ДЛЯ ПРОЕКТИРОВАНИЯ WEB-ПРИЛОЖЕНИЙ

Признанным фактором в деловой и общественной жизни стал Интернет. В настоящее время многие бизнес-задачи решаются при использовании Интернет-технологий, объединяющих различные платформы и источники данных. Проблема связи разнородных данных и поиск способа получения информации в удобной для дальнейшей обработки форме становится все более актуальной. Решить эту задачу призвана концепция создания Web-приложений, основными положениями которой должны стать открытые стандарты объединения, интеграции разнородных систем и технологий для проектирования и разработки Web-приложений [Гайнанова Р.Ш., Широкова О.А. Создание клиент-серверных приложений. – URL: https://cyberleninka.ru]. Web-приложения в общем случае рассматриваются как приложения с архитектурой клиент-сервер. В базовом примере модели клиент-серверной архитектуры все процессы разделены на две перекрывающиеся группы. Серверы – это процессы, которые реализуют определенный сервис, например, файловую систему или базу данных. Клиенты – это процессы, которые запрашивают услуги у серверов, отправляя запрос и ожидая ответа от сервера. Их взаимодействие, широко известное как способ действия запрос-ответ, показано на рисунке, данном ниже.



При условии надежности базовой сети клиент и сервер могут взаимодействовать без установления соединения (посредством простого протокола) так же, как и при работе в локальной сети. Клиент при таком взаимодействии посылает свой запрос в виде сообщения и необхо-

димые исходные данные в запрашиваемую им службу. Находящийся в постоянном ожидании сервер получает и обрабатывает запрос, упаковывает результат обработки – сообщение – и отправляет его клиенту.

В процессе реализации этой связи между приложениями необходимо определиться с сетевыми протоколами. Остановимся подробнее на использовании стека сетевых протоколов TCP/IP, на котором основано всё взаимодействие пользователя и сервера в IP-сетях. Это набор сетевых протоколов, организованный иерархически для обеспечения взаимодействия в сети. Работа протоколов организуется так, чтобы не возникло незавершенных операций или конфликтов. Каждый из уровней стека протоколов выполняет конкретную задачу – подготовку, передачу и прием, последующие действия с данными. Протоколы верхних уровней реализуются программными средствами, протоколы нижних уровней – комбинацией аппаратных и программных средств. Уровни стека TCP/IP в общем случае можно разделить на категории: прикладной (протоколы HTTP, RTSP, FTP, служба DNS); транспортный (протоколы TCP, UDP, SCTP, DCCP); сетевой (стек TCP/IP) и канальный (технологии Ethernet, IEEE, Token Ring и др.) [Тузовский А.Ф. Проектирование и разработка Web-приложений. М., 2018].

Рассмотрим достоинства системы «клиент – сервер». Модульные компоненты системы компактны и автономны. Поэтому, во-первых, сбой сервера не влияет на остальные компоненты, в связи с тем, что каждый компонент работает в отдельном защищенном пользовательском режиме; во-вторых, автономные компоненты могут быть запущены на нескольких компьютерах сети (распределенные вычисления) или на нескольких процессорах на одном компьютере (многопроцессорная обработка данных).

Сторона «клиент» предоставляет средства для приема, отображения и редактирования данных, введенных пользователем, которые служат основой запроса к серверу. Для снижения нагрузки на ресурсы сервера «клиент» может быть настроен на обработку только части данных.

Преимуществами клиент-серверного подхода к проектированию Web-приложений также являются: сокращение сетевого трафика за счет передачи только результатов запросов; освобождение значительного объема дискового пространства на компьютерах-клиентов и уменьшение потребности клиентских приложений в оперативной памяти; повышение уровня непротиворечивости данных и уровня безопасности базы данных, поскольку правила целостности данных определяются в системе управления базами данных сервера и являются едиными для всех приложений, использующих эту базу данных; возможность хранить бизнес-правила на сервере, чтобы избежать дублирования кода в различных клиентских приложениях, использующих одну и ту же базу данных.

Для проектирования клиент-серверного приложения, на основе которого клиент взаимодействует с Web-сервером при помощи браузера, существуют четыре стадии: концептуальная, логическая, физическая и перспективная [Советов Б.Я. Базы данных. М., 2018, с.59]. Эти стадии позволяют реализовать базу данных, предназначенную для конкретной задачи. На концептуальном этапе основное внимание уделяется пользовательским сценариям использования приложения. Они должны отражать требования пользователей к решению конкретных бизнес-задач. На втором логическом этапе разрабатываются бизнес-объекты и необходимые сервисы на основе сценариев использования. Основой формальной модели и оценки различных вариантов физического решения является логическая структура приложения. На стадии физического решения разрабатываются компоненты для объектов и сервисов. Структура и дизайн компонентов должны отражать исходные бизнес-объекты и, конечно же, варианты использования. Дополнительные задачи на данном этапе включают в себя учет существующей инфраструктуры и технологий для минимизации рисков и сокращения цикла разработки. Сценарии перспективного использования приложения являются основой для дальнейшего расширения его возможностей. Мнения пользователей о будущем бизнес-решении также находят отражение в сценариях перспективного использования.

Таким образом, клиент-серверная архитектура позволяет дифференцировать функции сервера и клиента, что делает ее одной из самых популярных моделей систем управления данными. Клиент-серверное проектирование приложений является универсальным подходом для большинства разработчиков Web-сайтов, Web-сервисов и мобильных приложений.

О.А. КИМ,
студент направления подготовки «Прикладная информатика»
А.К. САРБАСОВА,
профессор Алматинского филиала Санкт-Петербургского Гуманитарного университета профсоюзов, кандидат физико-математических наук – руководитель

СПОСОБЫ ПРИМЕНЕНИЯ АЛГОРИТМОВ В БИЗНЕСЕ

Цель исследования – продемонстрировать совместимость математических алгоритмов и работы человека.

Математика – это предмет, который развивает в человеке критическое мышление, его интеллект. Предмет нельзя просто выучить от А до Я, нельзя его просто запомнить, как стихотворение по литературе, его нужно полюбить и стать с ним одним целым.

В школьное время мы знакомимся с первым интересным, сложным и многим непонятным предметом – «математика».

Первое знакомство с алгоритмами происходит в школьный период времени, когда на уроке математики мы встречаемся с уравнениями. Например, ax2+bx+c=0 – обычная формула квадратного уравнения, которая в зависимости от данных может быть решена двумя способами (теорема Виета или же через дискриминант). Поначалу мы начинаем использовать теорему Виета, когда это необходимо. Со временем мы начинаем решать уравнения с помощью дискриминанта, что является адаптивным способом решения для большинства уравнений.

Закончив среднее полное или среднее неполное образование, постепенно переходим к высшей математике, где принцип алгоритмов остается без изменений, используя формулы общего вида в правильном направлении.

Даже поступив в университет и после его окончания, мы продолжаем сталкиваться с алгоритмами. На сегодняшний день для решения уравнения из высшей математики требуется использовать от двух до трех формул для их решения.

Например:

log5(4+x)=2

log5(4+x)=2

Задача выполняется следующим образом: воспользуемся правилом умножения на единицу для числа 2.

2=2·log55=log552=log525

2=2·log55=log552=log525

Тогда исходное уравнение станет вот таким:

log5(4+x)=log525.

log5(4+x)=log525.

Зачеркиваем логарифмы:

4+x=25,

4+x=25,

x=21.

x=21.

Делаем проверку:

log5(4+21)=2

log5(4+21)=2

log525=2

log525=2

Решение верно.

К сожалению, алгоритм относится к тому типу слов, которые не имеют точного определения.

Рассмотрим влияние алгоритмов на человеческую жизнь на известном фильме «Форест Гамп». На курсах по повышению квалификации в сфере продаж демонстрируют именно этот фильм как действительный пример использования алгоритмов.

Форрест стал успешным благодаря одному простому алгоритму, который ему внушила его мама. Она стала для него программистом, а сам Форрест стал программой. В дальнейшем Форрест начинает сталкиваться с новыми трудностями, которые он преодолевал благодаря тому алгоритму, который был у него изначально.

Данный фильм отлично показывает влияние алгоритмов на человека, но не все так просто и легко. Вы можете посетить несколько курсов по повышению квалификации, получить 2-4 диплома. В итоге это вам ничего не даст кроме потраченного времени.

Используя опыт прошлых ученых, которые уже открыли для нас все, что могли, в свое время мы можем это использовать.

Используя теоремы, формулы и таблицы математики можно заметить, что они значительно облегчили процесс изучения различных процессов и обучения людей. Такие же формулы и таблицы существуют и в нашей обычной бытовой жизни.

Например, обучение в университете. Студенты посещают занятия, во время которых они отвечают на вопросы преподавателя (если проходит практическое занятие).

Алгоритм в бизнесе – это последовательность действий, которые приведут к ответу. Положительный он будет или отрицательный зависит от череды экономических факторов, и все же их можно и даже нужно просчитать.

На сегодняшний день каждый из нас сталкивался с алгоритмами информационного бизнеса. А именно продажа информации и все с ней связанное. При открытии своего предприятия или трудоустройстве можно столкнуться с определенным алгоритмом действий. Рассмотрим оба варианта.

Открытие предприятия. Для открытия предприятия необходим минимальный пакет знаний и инвестиция. Под пакетом знаний имеется в виду:

1. Знание налогового кодекса (на минимальном уровне).
2. Точное понимание своей сферы деятельности.
3. Экономические знания.
4. Анализ своей сферы деятельности или же аналитики выбранной ниши.

Интересно то, что это только минимальный пакет знаний для открытия своего дела. На следующем этапе (после открытия предпри-

ятия) необходимо правильно его преподнести клиентам; в этом вам могут помочь как специальные коучеры (люди, которые уже открыли свое дело и оно является успешным), так и наставники (ими могут выступать ваши инвесторы).

Данный алгоритм происходит с каждым человеком, который готов связать свою жизнь с бизнесом. Как и в математических формулах, есть еще один вариант открытия своего бизнеса. Это приобретение франшизы. Самым ярким примером по приобретению франшизы в Алматы является «Мята loungebar», которая впервые была открыта в Российской Федерации и уже после открыла свои двери в Казахстане.

Собеседование. Это то, что ждет каждого выпускника вуза, который является действительно специалистом в своей профессии. Однако здесь уже работает другой алгоритм. Алгоритм будет тесно связан с вашими профессиональными навыками и практическими знаниями: «Теория без практики невозможна». Под данный критерий невозможно подобрать универсальный алгоритм, ведь в каждой компании свои правила и свои тесты для принятия сотрудников на работу. Но возможно подвести это все под единый алгоритм.

1. Резюме (то, что увидит ваш работодатель), или его отдел кадров в первую очередь. Оттого, как вы его напишите, будет показана ваша готовность к работе.

2. Собеседование, возможно несколько вариантов тестирования:

– онлайн-тестирование в здании компании;

– устный экзамен;

– психологическое тестирование (в сфере продаж этот тест сыграет важнейшую роль).

3. Испытательный период. В срок до 3-х рабочих месяцев ваша задача – проявить свои навыки.

4. Ответ от компании. На данном этапе отдел кадров (ваш работодатель) будет суммировать ваши показатели с предыдущими этапами. Результат будет зависеть от каждого фактора.

Данные алгоритмы очень схожи с математическими (в общем виде): подставив любые значения в данные алгоритмы, можно подвести общий итог, показывающий успешность вашей деятельности или же его отсутствие.

Итак, результат данной работы – показ связи между математическими алгоритмами и жизнью человека – был выполнен.

И.А. КОБЗЕВ,
студент направления подготовки «Прикладная информатика»
Г.А. АБДУЛКАРИМОВА,
доцент Алматинского филиала Санкт-Петербургского Гуманитарного университета профсоюзов, кандидат педагогических наук – руководитель

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ РАЗРАБОТКИ СЕРВЕРНОЙ ЧАСТИ WEB-ПРИЛОЖЕНИЙ

Интернет давно является неотъемлемой частью жизни современного человека. Для большинства людей – это средство для получения различной информации, либо средство коммуникации. Одним из способов использования Интернета для бизнеса является продажа услуг. Одной из реализаций такого способа является Web-портал, который позволяет автоматизировать бизнес-процессы, например, обработку заказов клиентов. Подобная система может быть продолжением традиционного бизнеса или независимой структурой.

Web-браузеры обмениваются данными с Web-серверами, используя гипертекстовый транспортный протокол (HTTP). Web-серверы ожидают сообщения с клиентскими запросами, обрабатывают их и отвечают Web-браузеру, используя ответное сообщение HTTP. Серверная часть разработанного Web-приложения включает динамическую генерацию контента в ответ на запрос пользователя. При таком подходе страницы HTML обычно создаются путем вставки данных из базы данных в элементы шаблона HTML. Запросы данных отправляются серверу. Сервер интерпретирует запрос, считывает необходимую информацию из базы данных, объединяет извлеченные данные с шаблонами HTML и возвращает ответ, содержащий сгенерированный HTML. Большая часть кода для поддержки такого приложения должна выполняться на сервере.

К серверному программированию относится разработка подпрограмм-скриптов, исполняемых на удаленном сервере. На их работу не влияет ни комплектация компьютера пользователя, ни установленное программное обеспечение. «Программированием серверной части» или «программирование бэкенда» принято называть создание таких подпрограмм. В настоящее время для программирования серверной части используются платформы, которые упрощают создание и поддержку технических проектов. К ним относятся CMS (системы управления контентом) и фреймворки, основанные на конкретном языке программирования. Фреймворки представляют собой комплексную среду разработки программного обеспечения. Они включают в себя множество

компонентов, задача которых – упростить работу разработчика при создании приложений. Однако, несмотря на положительные аспекты использования большого количества готовых решений, у них есть и недостатки: они могут затруднять долгосрочную разработку, потому что существует зависимость от сторонних ресурсов. Также, когда речь идет о задачах, требующих нестандартного подхода, использование фреймворков становится неэффективным. Тогда используются стандартные конструкции языков программирования – основы Web-разработки.

Для хранения небольших объемов данных на сервере используют текстовые файлы, однако с увеличением объема обрабатываемой информации такой метод не пригоден, так как данные должны быть систематизированы. Для решения этой проблемы создается база данных. Языки взаимодействия с базой данных также являются языками серверного программирования. Наиболее распространенным является SQL.

В данной работе наша цель – рассмотреть некоторые стандартные методы серверного программирования. Основой таких систем являются SQL-ориентированные системы управления базами данных, выполняемые на SQL-серверах. Примерами таких систем управления базами данных являются Oracle, Firebird/Interbase, MS SQL Server, MySQL. Реализовать SQL-запросы к базам можно в виде Web-приложений, написанных с использованием различных языков Web-программирования, таких как PHP, Perl, Си#, Python.

PHP – скриптовый язык общего назначения, применяемый для разработки Web-приложений. В настоящее время поддерживается большинством хостинг-провайдеров и является одним из лидеров среди языков, применяющихся для создания динамических Web-сайтов. В проектах сейчас чаще используется наиболее распространенный набор серверных языков программирования: PHP5 и MySQL [Суэринг С., Конверс Т., Парк Д. PHP и MySQL. М., 2010].

Система управления базами данных типа «клиент-сервер» MySQL – компактный многопоточный сервер реляционных баз данных, характеризующийся большой скоростью, устойчивостью и легкостью в использовании. По сравнению с рядом других серверных MySQL имеет такие преимущества, как быстродействие и поддержка нескольких одновременных запросов; простая инсталляция и администрирование; гибкая система привилегий и паролей; возможность одновременного подключения неограниченного количества пользователей [Справочное руководство по MySQL. – URL: http:// www.mysql.ru].

От несанкционированного доступа система управления базами данных MySQL оснащена развитой системой защиты. Для доступа к

серверу MySQL клиентской программе необходимо сообщить параметры соединения. Следует указать хост, имя пользователя и пароль. Осуществляется доступ к базе данных в два этапа: проверка соединения и проверка запроса.

На первом этапе, если сервер находит запись в таблице пользователей, в которой совпадают имя хоста и имя пользователя с введенными данными, а также указан правильный пароль, то сервер устанавливает соединение.

Ко второму этапу сервер переходит после установления соединения. Для выполнения каждого входящего запроса сервер проверяет полномочия, и осуществляет допуск в зависимости от типа операции, которую нужно выполнить.

К недостаткам и ограничениям MySQL относят отсутствие поддержки транзакций, проблемы с надежностью – из-за некоторых способов обработки данных MySQL (связи, аудиты) иногда уступает другим системам управления базами данных по надежности [Зеленков Ю.А. Введение в базы данных: Архитектура клиент-сервер. – URL: http://www.mstu.edu.ru].

Поэтому, работая с MySQL, пользователь реально работает с двумя программами: 1) программой сервера базы данных (сервер MySQL), которая принимает запросы клиентов, поступающие по сети, и осуществляет доступ к содержимому базы данных для предоставления информации, которую запрашивают клиенты; 2) клиентской программой, которая осуществляет подключение к серверу, передает запросы на сервер баз данных и отображает полученные с сервера результаты. MySQL используется в качестве сервера, к которому обращаются локальные или удалённые клиенты, однако в дистрибутив входит библиотека внутреннего сервера, позволяющая включать MySQL и в автономные программы.

Таким образом, на основе проведенного анализа можно сделать следующие выводы: система управления базами данных MySQL является оптимальным решением для разработки малых и средних Web-приложений. MySQL можно эффективно использовать в совокупности с другим программным продуктом – гипертекстовым процессором PHP, реализовав клиент-серверную технологию обмена данными: создать базы данных на сервере MySQL, а приложения, в которых будут работать пользователи с базами, могут быть реализованы в виде PHP-сценариев, содержащих SQL-команды работы с базами данных.

К.К. КОЗУБЕЦ,
студентка направления подготовки «Экономика»
Л.М. ТУКЕНОВА,
доцент Алматинского филиала Санкт-Петербургского Гуманитарного университета профсоюзов, кандидат физико-математических наук – руководитель

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ РАСПРОСТРАНЕНИЯ ЭКОНОМИЧЕСКОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

В данной статье рассматривается использование Интернет-технологий в маркетинге, что может принести реальную экономию и прибыль. Это связано с большими выгодами и удобствами, которые получают как потребители, так и фирмы. В надвигающейся глобальной компьютеризации, наступление которой планируется на ближайшее будущее, роль маркетинга в Интернете заметно вырастет. Для того чтобы исследовать и понять процессы распространения информации в Интернете, была построена модель SIRS, которая демонстрирует процесс распространения информации о продвижении продукта и услуг в социальной сети. Для получения реальных статистических данных из социальной сети, было построено Web-приложение.

Анализ распространения информации можно представить моделью эпидемии. Детерминированная модель эпидемии SIRS (susceptible – infected- removed) описывает способ передачи информации (эпидемии) от одного индивида (агента) к другому со следующими основными переменными (динамическими):

S – количество уязвимых агентов от рекламы (информации);

I – количество агентов, которые распространяют рекламу;

R – количество невосприимчивых агентов к рекламе.

Количество агентов в сети можно выразить как $N = S(t)+I(t)+R(t)$.

Для более детального и приближенного к реальности описания модели необходимо представить набор параметров:

σ – коэффициент контакта между агентами;

∂ – вероятность контакта между восприимчивым и зараженным агентом, что приводит к передаче информации;

β – средняя частота заражения информацией;

γ – постоянная средняя скорость забывания информации в единицу времени;

μ – средняя частота присоединения к сети в единицу времени;

δ – средняя частота выхода агента из сети в единицу времени;

α – вероятность перехода из невосприимчивого состояния в уязвимое.

Количество передач информации среди восприимчивых экономических агентов в период времени зависит от контакта между агентами σ в данный период и вероятности передачи данной информации (∂). Следовательно, константа β (средняя частота заражения информацией) получена произведением σ и ∂ , где $\beta = \sigma\partial$. Доля зараженных (информированных рекламной информацией) в общей численности агентов выражена как $\beta\frac{S(t)I(t)}{N}$.

Социальная сеть обладает изменчивостью во времени – это означает, что агенты могут присоединиться к сети или покинуть сеть (параметры μ и δ).

Система дифференциальных уравнений, которая демонстрирует динамику агентов в сети:

$$\begin{cases} \frac{dS(t)}{dt} = -\beta\frac{S(t)I(t)}{N} + \mu\big(N - S(t)\big) + \alpha R(t) \\ \frac{dI(t)}{dt} = \beta\frac{S(t)I(t)}{N} - \gamma I(t) - \delta I(t) \\ \frac{dR(t)}{dt} = \gamma I(t) - \delta R(t) - \alpha R(t) \end{cases} \quad (1)$$

Продемонстрируем действие модели SIRS в реальной ситуации. Выберем канал в социальной сети, а именно сообщество, в котором находится необходимая целевая группа потенциальных покупателей, а также входные параметры для данного канала, полученные в предыдущих главах, которые помогут описать процесс распространения информации среди агентов.

Количество зараженных информацией *I(0)* = 668 агентов, количество уязвимых влиянием информации S(0)=79 426 агентов, количество пользователей невосприимчивых к информации *R(0)* = 282 217 агентов. Таким образом, в момент времени *t* = 0 общее количество агентов в системе будет: *N(0)= S(0) +I(0)+ R(0)* = 362 311 агентов.

Коэффициент контакта между агентами σ = 0.37 , вероятность контакта между восприимчивым и зараженным агентом ∂ = 0.83. Следовательно, средняя частота заражения информацией β = 0.31, средняя скорость забывания информации γ = 0.051, средняя частота присоединения к сети μ = 0.00081, средняя частота выхода из системы =0.00036 (динамика социальной группы), вероятность перехода из невосприимчивого состояния в уязвимое α = 0.032, время *t* = 60 дней.

Система дифференциальных уравнений будет выглядеть следующим образом:

$$\begin{cases} \frac{dS(t)}{dt} = -0.31\frac{S(t)I(t)}{N} + 0.00081\big(N - S(t)\big) + 0.032R(t) \\ \frac{dI(t)}{dt} = 0.31\frac{S(t)I(t)}{N} - 0.051I(t) - 0.00036I(t) \\ \frac{dR(t)}{dt} = 0.051I(t) - 0.00036R(t) - 0.032R(t) \end{cases} \quad (2)$$

Продемонстрируем решение данной задачи с помощью инструмента *SIMULINK* программного продукта *MatLab*.

Система дифференциальных уравнений в данной среде будет выглядеть следующим образом (рисунок 1):

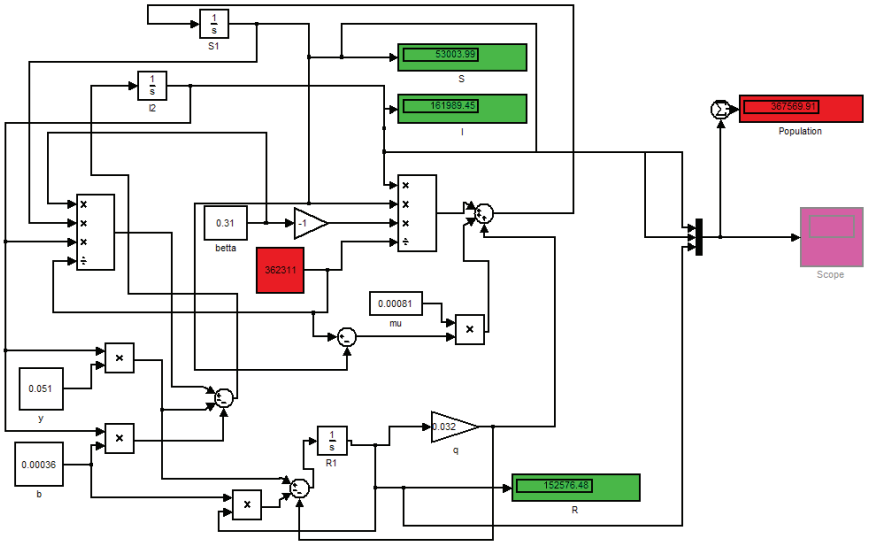


Рисунок -1 Модель SIRS

Получены следующие результаты за период времени t = 60 дней:

I = 161 989 агентов зараженных информацией;

S = 53 003 агентов уязвимых влиянию информации;

R = 152 576 агентов невосприимчивых к информации;

N = 367 568 всего агентов в системе.

Группа увеличилась за 60 дней на 5 257 агентов.

Динамика изменения состояния агентов изображена на следующем графике (рисунок 2):

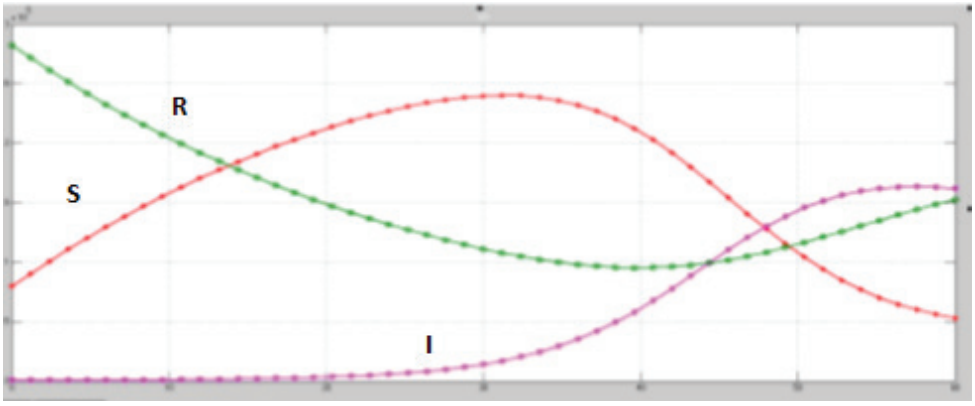


Рисунок 2 – Модель SIRS

На графике находятся S – уязвимые агенты (красная линия), I – зараженные агенты (фиолетовая линия), R – невосприимчивые агенты (зеленая линия).

На основании вышесказанного, можно сделать следующий вывод: в поддержании рекламы в сообществе стоит вкладывать инвестиции до момента времени t = 31-32 день, где достигается точка экстремума уязвимых агентов (желтая линия). На следующем изображении (рисунок 3) показана точка экстремума функции уязвимых агентов:

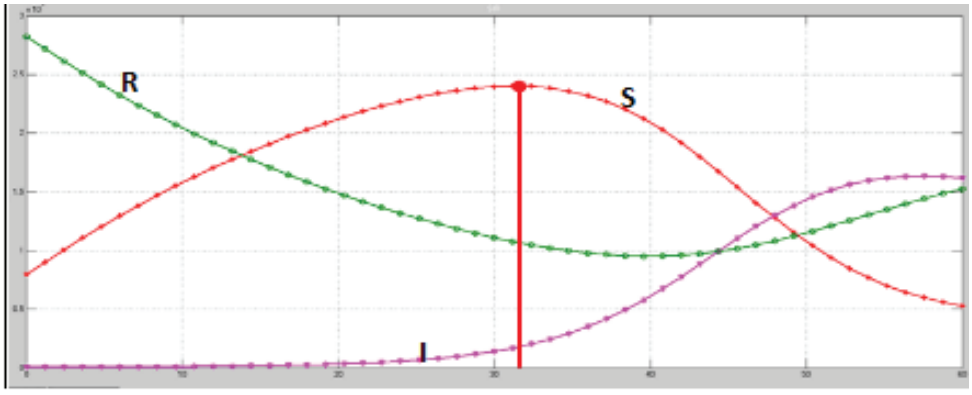


Рисунок 3 – Модель SIRS

На основании полученных данных, при моделировании распространения информации мы можем спрогнозировать количество потенциальных покупателей C на основании экспертной оценки вероятности перехода из зараженного состояния в состояние потенциального покупателя. Число потенциальных покупателей будет напрямую зависеть от количества зараженных агентов (агенты, которые увидели рекламу и

распространяют её) и вероятности перехода зараженных агентов в потенциальных покупателей *k*.

На основании прогноза потенциальных покупателей при помощи экспертных оценок можно добавить следующее:

1. Достоинством экспертных методов является их относительная простота и применяемость для прогнозирования практически любых ситуаций, в том числе в условиях неполной информации. Важной особенностью этих методов является возможность прогнозировать качественные характеристики рынка, например, изменение социально-политического положения на рынке или влияние экологии на производство и потребление тех или иных товаров.

2. К недостаткам экспертных методов относятся субъективизм мнений экспертов, ограниченность их суждений.

А.А. СВИРИДОВ,
студент направления подготовки «Прикладная информатика»
И.Г. ПОЛЕГЕНЬКО,
доцент Алматинского филиала Санкт-Петербургского Гуманитарного университета профсоюзов, кандидат технических наук – руководитель

РАЗВИТИЕ КРИПТОГРАФИИ В ПЕРВОЙ ПОЛОВИНЕ XX ВЕКА В СССР

История мировой криптографии насчитывает несколько тысячелетий. Шифрование информации активно применялось с III тысячелетия до н.э. В это время использовались простые механизмы шифрования, принцип которых основывался на замене букв алфавита исходного текста на буквы и символы другого алфавита.

Следующим периодом в истории криптографии является период использования нескольких алфавитов для шифрования текста. На Ближнем Востоке изобретателем такой технологии шифрования является Аль-Кинди, который в 850 году написал книгу «Трактат о дешифровке криптографических сообщений», в котором описал основные принципы шифровки и дешифровки сообщений, используя несколько алфавитов. В европейских странах открывателем в XV веке является Леон Баттиста Альберти.

Криптография XX века характеризуется появлением электромеханических устройств для осуществления шифрования. К началу XX века ведущими странами в области криптографии были Россия, Франция, США и Германия. Эти страны имели большой опыт

использования различных шифров для передачи сообщений, умели перехватывать и расшифровывать сообщения других стран.

В начале XX века в России, как и в других странах, использовались полиалфавитные принципы шифрования, использующие замену. В 1916 году подпоручик И.А. Попазов создал устройство для шифрования «Прибор Вави». Этот прибор использовал 20 колец, на крайнем одном или двух наносились числа от единицы до тридцати, а на внутренних – буквы в случайном порядке. Используя основной ключ и «ключ шага», можно было зашифровать сообщение любой длины.

После Октябрьской революции в 1921 году В.И. Ленин был ознакомлен с результатами и материалами работы разведки и шифровального дела в целом за годы Первой мировой войны и Гражданской войны. После ВЧК и Реввоенсовету было поручено заняться организацией специальной радиоразведки. 12 апреля 1921 года на заседании Малого Совнаркома был представлен проект создания Специального отдела при ВЧК. С докладом выступил один из руководителей ВЧК Глеб Иванович Бокий, который впоследствии также стал и руководителем Специального отдела.

Специальный отдел, непосредственно занимающийся шифровальной и криптоаналитической деятельностью, обеспечивал органы государственного управления, спецслужбы, военные организации Советского Союза стойкими шифрами на протяжении долгих лет.

Основным методом шифрования в 30-е годы XX века являлся метод перестановки символов исходного текста. Различные вариации шифра перестановки использовались как в обмене информацией внутри государства, так и для передачи сообщений другим странам. Особенно шифр перестановки закрепился в отделе разведчиков, это было связано с простотой использования алгоритмов шифрования и с достаточным уровнем криптостойкости получаемого шифра для быстрой отправки сообщения.

Первые попытки создания шифровальной машины привели к появлению аппарата В-4, который разрабатывался с 1934 по 1937 годы конструктором И.П. Волоском. Данное устройство было вскоре модернизировано В.М. Шарыгиным и названо М-100 «Спектр». Вес полного комплекта устройства, состоявшего из трёх основных частей, равнялся 140 килограммам, но, несмотря на столь высокий показатель, эта машина пошла в серийное производство и показала результат шифрования в 300 знаков в минуту, что было быстрее ручного шифрования в 3-5 раз. В 1938 году В.М. Шарыгиным, И.П. Волоском и М.С. Козловым была разработана новая шифр-машина, получившая

название М-101 «Изумруд». Данная модель имела значительно меньшие габариты по сравнению с М-100 «Спектр» и имела всего две составных части, что позволило ей пойти в массовое производство уже к началу 40-х годов XX века.

В годы Великой Отечественной войны на отделы шифр-связи легла большая нагрузка по передачи большого числа секретных телеграмм. В период с 1941 по 1945 год было передано свыше 1,6 миллионов зашифрованных телеграмм и сообщений. В определённые моменты количество передаваемых телеграмм могло достигать 1500 телеграмм в сутки.

Помимо телеграфной связи существовала правительственная стационарная «ВЧ-связь», предназначенная для переговоров и обмена сообщениями между высшими органами правительства Советского Союза. Для обеспечения безопасности передаваемых данных ВЧ-связь обладала новейшими на то время сложными системами засекречивания, такими как «Нева», «Сова», «Волга-С». Для описания эффективности работы ВЧ-связи больше всего подойдут слова маршала СССР Александра Михайловича Василевского: «Ни одно донесение о готовящихся военно-стратегических операциях нашей армии не стало достоянием фашистских разведок. Будучи начальником Генерального штаба, я ни одной минуты не мог обойтись без ВЧ-связи, которая благодаря высокой сознательности и мастерству воинов-связистов наилучшим образом обеспечивала оперативное руководство действующими фронтами и армиями» [URL: https://cyberleninka.ru].

Стоит отметить вклад советских учёных-конструкторов, математиков, создавших стойкие, надёжные шифры и воплотившие их в механические устройства. Такие ученые, как И.П. Волосок, П.А. Судаков и В.Н. Рытов получили государственные премии за разработку машины М-101 «Изумруд». Орденами были награждены В.М. Шарыгин, М.С. Козлов, П.И. Строителев и Н.И. Гусев. А лично И.П. Волоску была присвоена учёная степень «кандидат технических наук».

С течением времени криптография становилась всё более актуальной наукой, а её технологии постепенно переходили в массовое использование. Изменяясь и приобретая новые черты и сферы использования, до нас она дошла не только как наука, возможности которой используются в государственном или военном управлении, а как инструмент, необходимый каждому.

Современная криптография получила своё развитие совместно с информационными технологиями. Технологии криптографии активно используются в банковском деле для обеспечения защищённости

конфиденциальной информации, в алгоритмах электронных цифровых подписей для проверки документов и в криптовалюте. В последние годы криптовалюта стала популярным направлением в экономических отношениях. Одним из главных преимуществ использования криптовалюты является абсолютная анонимность, прозрачность системы и удобство при переводе из одной страны в другую. Но сложности, связанные с получением криптовалюты и ее обработкой, пока не позволяют использовать все её возможности в широких массах.

Итак, технологии криптографии как раньше, так и сейчас применяются в основном для осуществления безопасности важных данных при передаче или хранении. Криптография всегда занимала одно из важнейших мест среди наук и объектов для исследования.

А.Д. ШКАВРОНСКИЙ,
студент направления подготовки «Прикладная информатика»
С.О. ЧУГАЙ,
старший преподаватель Алматинского филиала Санкт-Петербургского Гуманитарного университета профсоюзов – руководитель

АНТИПЛАГИАТ КАК ИНФОРМАЦИОННАЯ СИСТЕМА

С популяризацией глобальной сети Интернет плагиат студенческих работ стал серьезной проблемой. Большинство работ попадают на файлообменник как по желанию студентов, так и без их участия. Эта проблема касается не только сферы образования, но еще затрагивает промышленность и научное общество.

В начале 2000-х годов стали появляться так называемые системы «Антиплагиат». Но большую популярность получила система антиплагиата от компании Forecsys. В 2006 году эта программа стала победителем конкурса русских инноваций и получила премии от Министерства информационных технологий и связи Российской Федерации. Уже в 2007 году система была рекомендована российским вузам Роспотребнадзором. Позже в 2013 году была проведена пресс-конференция, на которой было представлено исследование, в ходе которого анонимно для улучшения алгоритмов были проверены все диссертации исторического направления. В том же году Министерство науки и образования Российской Федерации выпустило проект приказа, согласно которому вузы обязаны проверять дипломные работы на наличие плагиата. Тем не менее, «Антиплагиат» не имеет никакого отношения ни к Минобрнауки России, ни к Высшей аттестационной комиссии и является коммерческим продуктом. Но и сейчас эта система является одной из популярных не только в вузах России, но и в СНГ.

Несмотря на наличие очевидных плюсов системы, она регулярно подвергается критике как со стороны студентов и выпускников вузов, так и со стороны преподавателей, руководства и деятелей культуры и образования [URL: http://vedomosti.ru]. Главной причиной для критики является безальтернативный алгоритм работ большинства данных систем, который подразумевает поиск заимствований из общедоступных, индексируемых поисковыми системами интернет-источников, реже из баз данных работ вузов и электронных библиотек [URL: http://habr.com/ru]. Несмотря на совершенствование систем проверки работ на наличие заимствований, принцип их работы остается тем же.

Итак, основными тезисами для критики являются:

1. Система является платной. Хотя система и имеет бесплатный функционал, она не дает возможность получить корректный процент и источники плагиата учащимся с бесплатной версией, что провоцирует коррупцию, манипуляцию и бюрократизацию в образовательной системе.

2. Темы, которые выдают вузы, повторяются каждый год. Современная система образования является недостаточно гибкой, в связи с чем программы обучения, как и темы работ, предлагаемых студентам, ежегодно повторяются. Кроме того, разные вузы на близких специальностях выдают для разработки похожие темы, в итоге готовые работы по многим направлениям со временем попадают в единое мировое пространство и написать оригинальную работу на стандартную тему становится все труднее. В следствии этого написание работы по теме без попадания в процент плагиата с каждым годом становятся менее осуществимой задачей.

3. Обязательная проверка с помощью системы «Антиплагиат» работ реферативного характера, а также работ по дисциплинам, в которых обновление материала невозможно или происходит редко (например, история юриспруденции, теория точных наук).

4. Подход к проверке работ является формальным, потому как под термином «оригинальность» понимается не содержание работы, а отсутствие похожих материалов в Интернете.

5. Большое количество мошеннических сервисов, обещающих повышение уникальности работ различными способами.

6. Нарушение прав студентов. В связи с повсеместным, не имеющим законных оснований применением программы, не имеющей официального статуса и государственного регулирования, по умолчанию признается виновность студента в списывании и игнорируется «презумпция виновности», то есть учебное заведение, работники кафедр и преподаватели проводят тестирование всех работ на антиплагиат без

оснований к проверке или подозрений на плагиат в конкретных работах учащихся. При этом поверка результатов тестирования системами антиплагиата на ссылки, не имеющие отношения к материалу, не проводится, а цифра, выданная программой, становится одним из критериев оценивания работ.

7. Антиплагиат снижает качество работ и культуру речи. Исходя из повсеместного использования системы, основной целью работы является не выражение законченной мысли, а обход алгоритмов системы с помощью переписывания, перевода, нестандартного построения предложений.

Основным алгоритмом работы данных систем является сверка и поиск совпадений в тексте на индексируемых страницах в Интернете, а также в различных локальных и подключаемых базах с помощью различных методов. Основными методами поиска являются: сравнение строк, метод нечетких дубликатов, метод межязыкового определения, множество слов, обнаружение на основе цитат, стилометрии.

Процесс происходит так: ввод текста – оценка локального сходства – оценка сходства в целом – дактилоскопия – анализ встречаемости терминов – анализ на основе цитирования – стилометрия – подсчет процента совпадения – вывод результата. Объем заимствованного текста вычисляется подсчетом количества заимствованных строк, слов или символов. Далее более подробно запускается алгоритм поиска соответствия подстроки, затем срабатывает механизм анализа множества слов, а также выполняется анализ шаблона цитат [URL: http://dvachaya.ru].

На основе приведенной критики можно сделать вывод, что данная система имеет слишком большое количество недостатков и не соответствует современным требованиям и не только не повышает качество работ, но и снижает уровень образования в целом. Полное исключение системы проверки на плагиат в образовании невозможно, но требуется полное переосмысление, регулирование данных систем.

Возможными предложениями для улучшения положения могут стать:

1. Создание общедоступной, централизованной государственной системы Антиплагиат, предполагающей реестр дипломных работ, прошедших защиту во всех вузах страны. Устранение монополии частной компании на предоставление услуг ненадлежащего качества.

2. Запрет использования системы для проверки реферативных работ или работ с высоким уровнем цитирования (история, юриспруденция, политология и прочее).

3. Невозможность использования системы без подозрения учащегося в плагиате, исключением могут служить дипломные работы.

4. Невозможность использования процента уникальности как допуска к защите или критерия оценки.

5. Общий функционал для студента и преподавателя.

И.В. ЦОЙ,
студент направления подготовки «Прикладная информатика»
О.С. АХМЕТОВА,
доцент Алматинского филиала Санкт-Петербургского Гуманитарного университета профсоюзов, кандидат педагогических наук – руководитель

ТЕОРЕМА О ЧЕТЫРЕХ КРАСКАХ И ПОПЫТКИ ЕЕ ФОРМАЛИЗАЦИИ

Еще в 1852 году, создавая карту Великобритании и её колоний, студент Френсис Гутри обратил внимание на то, что ему для разделения территорий на графства хватило четырёх красок. Он поделился наблюдением с известным математиком Огастесом де Морганом. Морган в своём письме сообщил об этом наблюдении математической общественности. В 1878 году более общую формулировку интересной гипотезы опубликовал А. Кэли, поставив задачу найти доказательство или опровергнуть теорему о раскраске карт. Большинство заинтересовавшихся учёных при решении данной проблемы сталкивались с большими трудностями. Многократные попытки опубликовать доказательство гипотезы неизменно приводили к обнаружению содержащейся ошибки. Но прогресс всё-таки наметился, и в 1890 году Джон Хивуд доказал, что для правильной раскраски карт достаточно пяти красок. Теорема Хивуда формулировалась на языке плоских графов с цветными вершинами.

В 1975 году в США Мартин Граднер опубликовал проблему четырёх красок как популярную журнальную задачу, и вскоре появилось необычное по методике её решение.

Говоря о правильности раскраски, имеют ввиду, что две одноцветные области не должны иметь общей границы. Точка, в которой состыковываются несколько областей, в счёт не идут.

Итак, в 1976 году в Иллинойском университете теорема о четырёх красках была доказана Кеннетом Аппелем (1932-2013) и Вольфгангом Хакеном (1928-наст. вр.). В книге, содержащей это доказательство, приводится набор неких вариантов карт в количестве 1936, которые претендовали на роль наименьшего контрпримера к теореме. После

проверки списка методом доказательства от противного авторы делают вывод, что наименьшего контрпримера не существует.

Необычность доказательства, выполненного Аппелем Хакеном, состоит в том, что к тексту прилагалась программа для суперкомпьютера, проверяющего наличие некоторого характерного свойства во всех «неустранимых» 1936 графах. Повторить вычисление компьютера или проверить правильность программы на сегодняшний день очень сложно, т.к. 2000 часов машинного времени на суперкомпьютере очень дорого. Формально считается, что доказательство выполнено и гипотеза четырёх красок верна [Пруцков А.В., Волкова Л.Л. Математическая логика и теория алгоритмов. М., 2017, с.111].

Наша цель – рассмотреть некоторые формализации, используемые в математической теории хроматических графов. Чтобы построить граф, идентичный карте, надо заменить столицы на вершины, а границы на рёбра. Затем можно вычислить хроматическое число графа.

Например, если граф является непустым деревом, то его можно окрашивать по этажам, так что получается $\chi(T)=2$. На рисунке 1 приводится минимальная раскраска трех классических планарных графов, цвета указаны числами:

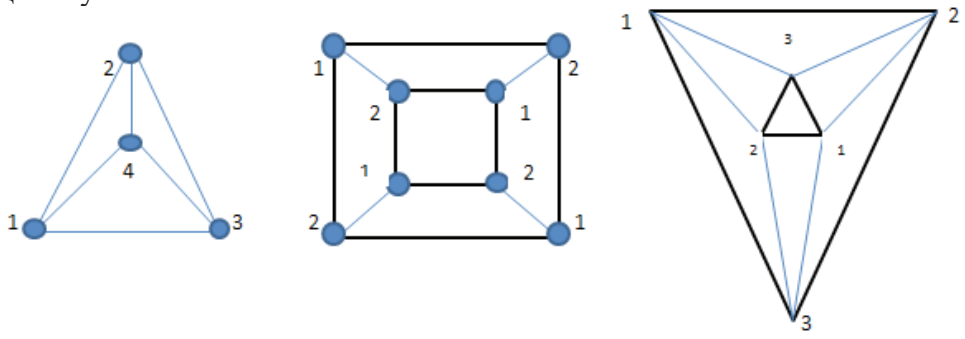


Рисунок 1 - Минимальная раскраска классических планарных графов

Соответственно, их хроматические числа равны $\chi(K4)=4$, $\chi(Q3)=2$, $\chi(G)=3$.

Надо отметить, что поиск алгоритма для вычисления хроматического числа пока остаётся актуальной задачей. В подобной ситуации большим достижением считается любая найденная оценка для $\chi(\Gamma)$. Например, его можно оценить сверху через наибольшую степень у вершин графа $\chi(\Gamma)\chi P(\Gamma)+1$. Для связных графов с n вершинами и m ребрами есть оценка сверху

$$c(\Gamma) \leq \left[\frac{3+\sqrt{9+8(m-n)}}{2}\right].$$

Если использовать число, называемое неплотностью графа, то можно также задать границы хроматического числа. Например, у следующего двудольного графа на рисунке 2 очевидная плотность $\alpha_0(\Gamma)=5$.

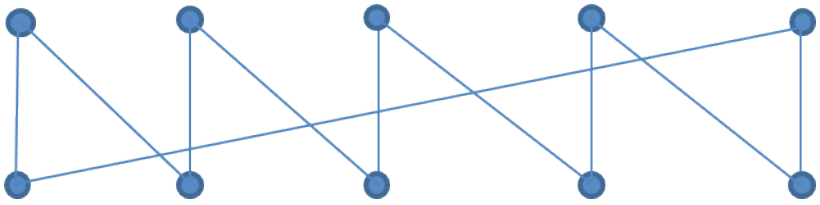


Рисунок 2 - Двудольный граф

Если порождать графы множеством только нижних или только верхних вершин, то они будут пустыми. Имеется оценка хроматического числа

$\chi(\Gamma)\chi n-\alpha 0(\Gamma)+1$.

Граф Г называется критическим, если удаление любой из его вершин уменьшает значение $\chi(\Gamma)$. При $n>1$ все полные графы являются критическими, а простые циклы только при нечетных *n*. Действительно, при *n*=6 имеется изоморфизм цикла C_6 и двудольного графа $\chi(C_6)=2$ (рисунок 3):

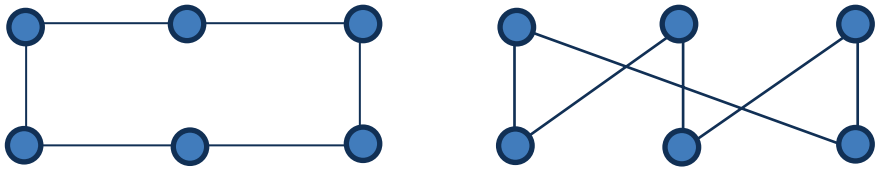


Рисунок 3 - Критические графы

Удаление любой вершины превращает цикл в дерево Т, а ранее говорилось, что $\chi(T)=2$. В результате C_6 оказался некритическим.

Для нечетного цикла C_7 очевидно $\chi(C_7)=3$. На рисунке 4 приведен пример минимальной раскраски.

Рисунок 4 - Минимальная раскраска нечетного цикла C_7

Удаление любой вершины уменьшит $\chi(C_7)$ до $\chi(T)=2$. Это говорит о критичности нечетного цикла [Шапорев С.Д. Дискретная математика. М., 2006, с.167].

Известные сегодня алгоритмы последовательной раскраски графа обычно не приводят к минимальной раскраске, поэтому на сегодня схема доказательства гипотезы четырёх красок методом от противного является единственной. Конечно, участие компьютера в этой схеме несколько подрывает доверие к её безошибочности.

Новое доказательство было опубликовано в 2005 году, но оно тоже проводилось с использованием компьютера.

Отметим, что более чем столетняя история теории хроматических графов привела к решению многих практических задач, например, при составлении расписаний, при распределении оборудования, при проектировании технических изделий и т.п. С другой стороны, первое доказательство с помощью компьютера даёт шанс ускорить процесс доказательства и сделать его доступным в период одной жизни математика. Впоследствии Аппель и Хакен уменьшили число проверяемых конфигураций до 1482. Эта цифра постепенно снижается и, по последним данным, их уже 633.

На сегодняшний день ускорение процесса доказательства математических теорем возможно пойдёт за счёт: 1) использования ЭВМ; 2) проверки правильности рассуждений интернет-сообществом; 3) прогресса в науке о защите информации от шумов; 4) изобретении способов проверки правильности программ; 5) усовершенствовании операционных систем.

Пока ведутся философские споры о новой природе понятия «доказательство», по пути разделения работы на «человеческую» и «компьютерную» части идут всё новые и новые математики. Робин Уилсон условно проводит психологический водораздел на тех, кому за 40, и тех, кому меньше сорока. Первые не желают верить в безупречность компьютерных доказательств, а вторые склонны считать, что ошибки чаще совершает именно человек.

Что касается непосредственно теоремы о четырёх красках, то к её доказательству подключаются геометры, предлагающие использовать функцию кривизны пространства, зависящую от времени [Стюарт И. Величайшие математические задачи. М., 2019, с.155]. Физики предлагают использовать блуждания в пространстве электрического заряда. У теоремы возможно в будущем появятся принципиально новые варианты доказательства с модернизированными алгоритмами раскраски карты.

Таким образом, несмотря на все разногласия среди математиков, решение проблемы четырёх красок есть первая математическая теорема, при доказательстве которой впервые был использован компьютер, и является примером неклассического доказательства в современной математике, сферы использования которой будут еще расширяться.