#20
09 – 11. 2013

Информационная безопасность

Интервью с заведующим новой кафедры Игорем Анатольевичем Соколовым

стр. 4

В ногу с жизнью

Актуальный взгляд на мир за пределами кода

Криптография

Как Gmail использует технологию амбарного замка

стр. 8

Управление временем

Советы по выживанию

стр. 10

стр. 14

Победа России

Важное и интересное о финале одимпиады по программированию ACM/ICPC

стр. 12

Готовь сани... осенью

Как выбрать лыжи/сноуборд и где на них кататься

стр. 14

газета факультета ВМК МГУ

Лето, наполненное поездками и отдыхом, а у кого-то – работой и сдачей экзаменов, сменяется золотой осенью. Водоворот лекций и семинаров, интересные научные задачи, встречи с однокурсниками и преподавателями снова становятся привычной частью жизни. Наше обучение – это не только обязательные домашки, монотонные пары и общение с друзьями, но и во многом та специализация, которую мы выбираем. Вычисления, программы, новые алгоритмы и теоремы – всё это может быть безумно интересно, если выбрать именно ту область, которая нравится. Ведь что может быть лучше личного вклада в огромную науку, что может быть интереснее, чем найти пробел в мировых знаниях и наполнить его своим результатом?

Мы решили приоткрыть научную жизнь ВМК на примере направления защиты информации. Что общего у сертификата открытого ключа с амбарным замком? В чём тайны криптографии? Будет ли режим секретности у выпускников новой кафедры Защиты информации? Кто же заведующий этой кафедрой, и как он пришёл в науку? Эти актуальные вопросы раскрываются на страницах номера.

Хорошие исследования должны сменяться хорошим отдыхом. Поэтому если вы хотите получить свой заслуженный отдых после ближайшей сессии, то стоит начать думать об этом уже сегодня. Например, покупать горные лыжи или сноуборд :)

Но как всё успеть? Ведь кроме учёбы у нас ещё немало других интересных занятий, да и на личную жизнь нужно время...

Решение проблемы – тайм-менеджмент. Слышали это слово, но всё не доходили руки освоить его практические методы? Это пора сделать сейчас – в начале года, а не ругать себя после несданных экзаменов за то, что опять ничего не успели! Уникальные технологии организации времени на любой вкус – в этом номере ;)

Интересной вам научной работы, учёбы, и их эффективного совмещения со всем остальным!

Ксения Молоканова

СОДЕРЖАНИЕ

АНОНСЫ 3

ИНТЕРВЬЮ
Приветствуем – кафедра ИБ! 4

ПРОСТО О СЛОЖНОМ
Про криптографию, амбарные замки и почту ВМК 8

СОВЕТЫ
Научитесь управлять временем! 10

РЕПОРТАЖ
Россия снова покорила ACM/ICPC 12

СПОРТ
Ай-да на южный... покатаемся! 14

СЛОВО НЕ ВОРОБЕЙ
Цитаты преподавателей 16

КУХНЯ
Рецепты 16

Вконтакте: vk.com/vnogus
E-mail: vnogus@gmail.com
Все выпуски: issuu.com/dontsov
ЖЖ: vmk_journal.livejournal.com

Анонсы научных и образовательных мероприятий на портале Vnogus Media: vk.com/vnogus

Главный редактор:
Ксения Молоканова

Зам. главного редактора:
Романа Галицкая

Редакторы:
Татьяна Шишкова
Дарья Кафтан
Тима Орсини

Корректоры:
Матвей Андриенко
Елена Щербакова

Корреспонденты:
Ангелина Плечкайтите
Наталия Морозова
Сания Зарипова

Дизайн и вёрстка:
Романа Галицкая
Данила Сигалов

Над номером работали:
Валерия Шерварлы
Елена Платонова
Юлия Антохина
Иван Чижов

Фотографии:
Алексей Манухов
Надир Чанышев
Э. Р. Корепанов
Ангелина Плечкайтите
Максим Кашин
Евгений Донцов
С сайтов: genesyslab.com, compbez.ru, islam.ru, tipsworld.org, carolynbaana.com, sch556.narod.ru

Фото на обложке:
Евгений Донцов

Выражаем благодарность заместителю декана факультета ВМК Березину Б. И., Матвеевой А. Н., издательству «МАКС Пресс» и лично Гутенёвой И. Н. за моральную поддержку и помощь в публикации.

Печатается при поддержке Студенческой комиссии профкома ВМК.

Отпечатано в типографии МГУ.
Тираж 999 экз.
Гарнитура Open Sans.
Распространяется в учебных корпусах МГУ.

Мнение редакции может не совпадать с точкой зрения авторов. При перепечатке ссылка на «В ногу с жизнью» обязательна.

Газета «В ногу с жизнью» ждёт своих героев!

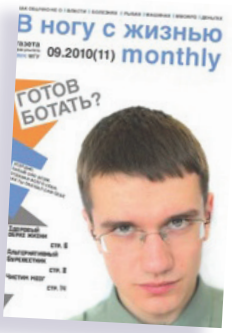
В первой половине ноября на ВМК состоится новый набор в редакцию газеты «В ногу с жизнью».

Вы хотите писать интересные статьи или красиво верстать текст? Корректировать или грамотно организовывать работу редакции? Учась на ВМК, вы тайно мечтаете о журналистике? Мечты сбываются!

Газета ВМК ищет:

- корреспондентов печатного издания и социальных медиа;
- корректоров;
- редакторов;
- дизайнеров;
- верстальщиков;
- менеджеров

и всех остальных, кто хочет создавать нашу газету!



На новом наборе будет организован семинар по журналистике. Вы узнаете, из каких частей состоит любая новость и как написать яркий анонс. Услышите секреты телевизионной рекламы и эффективного донесения любой информации. Мы расскажем, как сделать так, чтобы именно вашу статью прочитали!

Приходите на новый набор – сделаем газету лучшего факультета вместе!

Елена Платонова

Фестиваль Карьеры 2013: будущее зависит от меня!

С 7 по 11 октября в МГУ прошёл второй студенческий Фестиваль Карьеры! Всего за неделю все желающие смогли узнать из первых уст всё о самых популярных среди наших выпускников отраслях и компаниях. Почему лучше один раз прийти на Фестиваль, чем десять раз погуглить?

Каждый из нас при поступлении слышал: «Выпускникам ВМК все дороги открыты!» Но какой путь выбрать? Какие отрасли мне интересны? Обычно приходится провести много часов в интернете в поиске информации. Какие российские и мировые компании являются лучшими? Где лучше получить свой первый опыт и начать карьерный путь?

В течение недели Фестиваль помог студентам найти ответы на все вопросы – достаточно было только не полениться и прийти на мероприятия! Каждый день был отдельной ступенью: мотивирующие лекции от добившихся успеха бизнесменов и ТОП-менеджеров, лекции и мастер-классы от экспертов ведущих компаний, индивидуальные тестовые и практические занятия.

Завершающей ступенью Фестиваля Карьеры стали Техническая и Бизнес Ярмарки. В течение дня HR-специалисты более чем 40 компаний отвечали на вопросы студентов и с удовольствием назначали желающим даты собеседований в офисе компании.

Приходите на Фестиваль в следующем году и помните, что будущее зависит только от вас!

Сайт: msucareerfest.ru/
Группа ВКонтакте: vk.com/msucareerfest
Группа Фейсбук: facebook.com/msucareerfest

Ангелина Плечкайтите

Приветствуем – кафедра ИБ!

С этого года на ВМК начинает свою работу новая кафедра Информационной безопасности. Мы решили поближе познакомиться с её заведующим и разузнать все подробности.

Информационная безопасность – очень востребованная область в наши дни. Раньше на факультете она была представлена лишь на кафедре Математической кибернетики, направление информационной безопасности. Попасть туда было нелегко: много желающих, большой конкурс. Но с этого года появилась целая кафедра, готовящая специалистов в этой области. Для справки: сейчас на ней обучается 15 человек, чей средний балл в среднем составляет 3,89.

Заведующим кафедрой назначен *Игорь Анатольевич Соколов,* директор Института проблем информатики РАН. Наша газета взяла у него интервью и задала вопросы как о новой кафедре, так и личного характера.

Как проходил процесс отделения кафедры?

Никакого отделения, конечно, не было. Задача организовать подготовку специалистов в области информационной безопасности встала перед Университетом достаточно давно. Во-первых, в составе Университета был создан Институт проблем информационной безопасности (ИПИБ), на факультете ВМК его сотрудники организовывали спецкурсы, на мехмате было создано несколько специальных потоков, связанных с информационной безопасностью. Но тогда ряд формальностей не позволил в полной мере развернуть преподавание в Университете по этой специальности, хотя в России сейчас уже больше 130 (я думаю, уже подходит к полутора сотням) вузов, где преподается та или иная специальность из данного направления.

В последнее время всё чаще к Садовничему стали обращаться российские государственные структуры и зарубежные ученые с вопросом о преподавании информационной безопасности в Университете, что сподвигло его (я считаю, совершенно справедливо) всерьёз задуматься об организации этого процесса в МГУ. Он обратился ко мне с предложением возглавить межфакультетское образование или кафедру (тогда еще не было понятно, что именно) на мехмате, ВМК или где-то ещё, где профессионально бы занимались подготовкой студентов в этом направлении. Мы пришли к выводу, что на первых порах лучше всего это сделать на факультете ВМК.

Кафедра математической кибернетики (и другие кафедры ВМК) уже несколько лет ведёт преподавание по направлению, связанному с информационной безопасностью. Поэтому, когда этот вопрос перешёл в практическую плоскость, стали собирать специалистов с кафедр математической кибернетики и математической статистики. То есть нельзя говорить, что созданная кафедра исключительно порождение мат. кибернетики. Да, большая часть новой кафедры на сегодняшний день состоит из сотрудников этой кафедры, но есть и другие пригла-

шенные специалисты, в том числе и преподающие сейчас за рубежом, которые с большим удовольствием принимают приглашение вести занятия в Университете. Поэтому здесь нет никакого деления, скорее сбор специалистов в данной области с разных кафедр.

Придёт время более серьёзного преподавания этой специальности и на военной кафедре, потому что информационная безопасность требует рассмотрения вопросов, связанных с гостайной, например, криптография. Не только математические методы криптографии, но и реализация их. Принципиальная договорённость об этом уже есть.

Почему на ВМК? Во-первых, основной инструмент – это криптографические преобразования, т. е. математика. Во-вторых, современные системы защиты немыслимы без глубокого понимания работы компьютера. Уже сегодня вирусы проникают не только в систему, но и в чипы. Ну и в-третьих, также необходима теория программирования и понимание работы программных систем. Всё присутствует на ВМК.

А останется ли на кафедре математической кибернетики направление, связанное с информационной безопасностью?

Частично останется, частично уйдёт к нам на кафедру. Там останутся люди, которые будут преподавать свои спецкурсы. С Алексеевым, заведующим кафедры мат. кибернетики, мы, безусловно, договорились, работу будем вести согласованно, чтобы не было дублирования и противоречий.

Вы сейчас набрали третий курс. А четвертый и пятый, получается, будут пока пустыми?

Вообще говоря, да, но никто не запрещает (наоборот – это приветствуется) посещение спецкурсов студентами других кафедр.

«ТОГДА Я ПОНЯЛ, ЧТО МОИ ПРЕДСТАВЛЕНИЯ О «ЛЕГКО ДАЁТСЯ» БЫЛИ СОВСЕМ НЕПРАВИЛЬНЫЕ»

Каких студентов Вы хотели бы видеть на Вашей кафедре?

У меня есть кафедра в МИРЭА. Я спрашиваю студентов, приходящих на практику в ИПИ РАН, чем бы они хотели заниматься: математическими методами, инженерией и проектированием устройств или, может быть, аспектами эксплуатации и управления, что тоже очень важно. На ВМК на новой кафедре должны быть студенты с интересом к первому: они должны любить математику и хотеть ей заниматься.

Должны ли будут выпускники кафедры по её окончании соблюдать режим секретности?

Нет. Так будет, если реализуется идея преподавания этой специальности на военной кафедре. Тому, кто свяжет свою жизнь с работой на государство, стоит идти на военную кафедру. На факультете всё будет открыто.

Как Вы в целом видите развитие криптографии в России?

В конце 19-го – начале 20-го века в России была мощная математическая школа: Марков, Колмогоров, Прохоров – прямой продолжатель идей школы Колмогорова. Математики тогда определяли мощность криптографической школы. Сегодня, к сожалению, в России всё меньше развиваются именно математические методы криптографии. Этим, конечно, занимаются Математический институт им. Стеклова, ИПИ РАН, некоторые другие академические и отраслевые институты. Есть ещё академия ФСБ, но надо понимать, что из-за высокой секретности там имеют право готовить специалистов только для спецпотребителей. Мест мало, следовательно – меньше специалистов.

«ЛЮДИ, КОТОРЫЕ НАМ ПРЕПОДАВАЛИ, ЯВЛЯЛИСЬ И ЯВЛЯЮТСЯ КРУПНЕЙШИМИ УЧЁНЫМИ СТРАНЫ»

Сегодня в России явная нехватка специалистов и мест их подготовки. Любые начинания в этой области помогут повысить наш приоритет, который сейчас, к сожалению, в большой степени потерян. Можно сказать, что это актуальнейшая математическая сфера, имеющая совершенно очевидную прикладную направленность. Я надеюсь, что благодаря специалистам МГУ и РАН нам удастся сохранить имеющиеся достижения и мы начнём готовить в требуемом количестве специалистов. Если нет, то криптографии в России просто не будет. Это очень динамичная область с большим количеством специалистов за рубежом, и позволить себе отставать ни в коем случае нельзя.

Расскажите пару слов о Вашей научной карьере: чем Вы занимались, что относилось и относится к области Ваших научных интересов?

Я родился в Тамбове, учился в обычной средней школе, а последние два года (в школе № 29) – в классе с углубленным изучением математики. Интересовался математикой, я считал, что она мне легко даётся, но, когда поступил в университет, понял, что сильно заблуждался.

«ЭТО АКТУАЛЬНЕЙШАЯ МАТЕМАТИЧЕСКАЯ СФЕРА, ИМЕЮЩАЯ СОВЕРШЕННО ОЧЕВИДНУЮ ПРИКЛАДНУЮ НАПРАВЛЕННОСТЬ»

Когда мы оканчивали школу, я узнал, что в МГУ организован новый факультет Вычислительной математики и кибернетики. В это время я уже учился в заочной математической школе при мехмате: решал всякого рода дистанционные задания, которые мне присылали обычной почтой, отправ-

лял решения, получал письма от преподавателей с разбором моих решений – всё это мне было интересно. В разных олимпиадах занимал первые места. Сейчас это уже так не звучит, но в то время олимпиад было мало, и участие в них было событием.

Я узнал про ВМК и сразу загорелся: с одной стороны, математика, а с другой стороны, компьютеры. Что такое компьютер, я смутно представлял. Когда окончил школу, приехал сюда один, без какой-либо протекции. Это был второй набор (свой первый выпуск факультет формировал путём на-

«В РОССИИ ЯВНАЯ НЕХВАТКА СПЕЦИАЛИСТОВ И МЕСТ ИХ ПОДГОТОВКИ»

бора с мехмата). Из 250 мест на ВМК в тот год 125 было для иногородних, проводился раздельный конкурс. Это, конечно, связано с ограничением количества мест в общежитии. Я обычным образом сдал экзамены, думал, что могу и не поступить, поскольку конкурс большой: шесть-семь человек на место. Но поступил, начал учиться.

Первый же зачёт по математическому анализу, у Сухарева, легко написал, поскольку был уверен в своих силах в задачах взятия интегралов, нахождения пределов и т. д., первый сдал и получил двойку. И тогда я понял, что мои представления о «легко даётся» были совсем неправильные. После этого у меня долгое время не было ни троек, ни четвёрок. Что говорит о правильном преподавании в Университете.

Учились очень много. Мы жили в пятом корпусе общежития, по пять человек в комнате на четыре кровати (ставили ещё одну раскладушку). Но мы с девяти до трёх в Университете, затем самостоятельная подготовка: домашние задания и не только. Так что свободного времени совсем не было, круглые сутки учились. Читали, решали задачи, обсуждали в комнатах, в коридоре, в читальном зале.

«Я СЧИТАЮ ВМК ТЕМ МЕСТОМ, ГДЕ СФОРМИРОВАЛСЯ КАК ЧЕЛОВЕК»

В то время, как и во всём хозяйстве, был план на отсев студентов. Так как специальность «вычислительная математика и кибернетика» признавалась приоритетной, на нашем факультете имели право отсеять больше, чем на любом другом или в другом институте. И я общался с людьми, которые были отчислены тогда – они переводились на другие факультеты МГУ – и мне говорили так: «Как мы вас жалеем! У нас настоящая студенческая жизнь, а вы света белого не видите». Но это неправда, конечно. Свет мы видели.

С третьего курса учился на кафедре математической статистики, причём большое влияние на меня оказал Юрий Васильевич Прохоров. Было заметно, что кафедра выделяется своим подходом к организации учёбы, к студентам: скажем, было позволено пользоваться любой литературой на экзамене. Другие экзаменаторы шпаргалки отслеживали, а Юрий Васильевич, а за ним и все остальные преподаватели, говорил, что если хочешь – даже в библиотеку иди. Главное, мы с тобой поговорим и поймём, знаешь ты или нет, и если что не знаешь, не прогоним, а посоветуем, что почитать.

Юрий Васильевич, конечно, великий учёный и преподаватель. Если бы не он, факультет выглядел бы по-другому. Он привнёс дух правильного студенчества и правильного к нему отношения.

Матвеев Виктор Фёдорович, мой непосредственный научный руководитель, увлёк теорией массового обслуживания, случайными процессами.

После пяти лет учёбы предложили остаться в аспирантуре, я с удовольствием согласился, сдал экзамены и учился ещё три года. Это самое продуктивное и счастливое время в моей жизни, я считаю. Во-первых, занимался непосредственно тем, что выбрал. Во-вторых, материальное положение было даже лучше, чем когда я начал работать. Не только интересные задачи решаешь, но ещё и за деньги. Возможности неограниченные – библиотеки. Интернета, конечно, не было, но мне хватало, чтобы быть в курсе всех событий в своей области в России и за рубежом. В Ленинской библиотеке у меня был абонемент, который позволял получить любую статью, любую книгу из любой библиотеки. Нужно было подождать неделю-две, но мы же занимаемся наукой, что такое две недели.

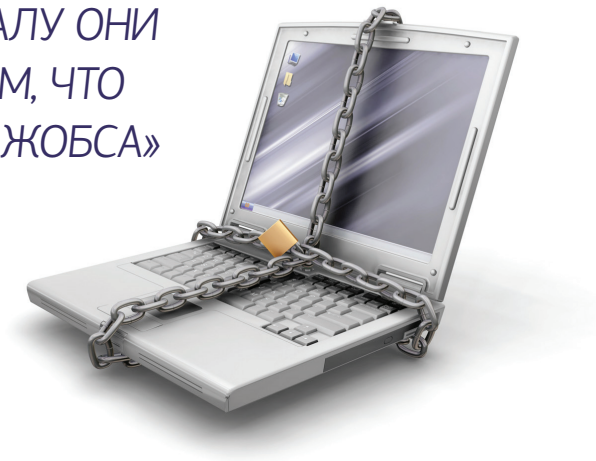
Молодые были, всё успевали. Я увлекался водным туризмом, достаточно серьёзно. Мы ходили в походы шестой категории сложности (самые сложные). Игровыми автоматами увлекались. На то время пришлось появление первых игровых автоматов в России, сначала в Сокольниках, потом в Парке культуры. Боулинг тоже. Одно то, что там выдавали кроссовки – это было что-то.

Я написал диссертацию «Дискретные приоритетные системы массового обслуживания», защитить не успел во время учёбы: очередь не подошла, заседания диссертационного совета были спланированы на много месяцев вперёд. Но в итоге дождался и удачно защитился.

Пришлось трудоустраиваться. Было много предложений, в том числе и остаться в Университете. Но в это время министерство промышленности средств связи, министр которого понимал необходимость привлечения в эту отрасль новых

математических идей и методов для инновационного развития, открыло отдел в Академии наук СССР. Туда были направлены выпускники МГУ и МФТИ, пошёл и я. Это был необычайно хороший отдел, творческая атмосфера. Занимались в первую очередь моделированием, проводили математические расчёты (характеристика, анализ, синтез систем связи, оптимальные характеристики аппаратуры, исследовали протоколы и т. д.). Причём всё это делалось одновременно с нашими коллегами за рубежом примерно с конца 70-х до конца 80-х годов.

«ПО ФУНКЦИОНАЛУ ОНИ РАВНЯЛИСЬ ТЕМ, ЧТО БЫЛИ У СТИВА ДЖОБСА»



Конечно, область применения наших разработок была в первую очередь военная, и публиковались мы в основном в закрытых изданиях. В дальнейшем наши товарищи, которые работали в открытых организациях имели больше возможностей по представлению своих презентаций за рубежом.

В 1990 году академик Мизин Игорь Александрович пригласил меня в Институт проблем информатики Академии наук СССР. Здесь я первое время был в моделирующем секторе, потом пошёл дальше, и я в конце концов директор, чему не могу быть очень рад, потому что Игорь Александрович скончался преждевременно в 64 года в 1999 году. Он мог бы ещё работать и работать. В 2003 году я стал членом-корреспондентом РАН, в 2008 академиком, а сейчас меня выбрали главным учёным секретарём президиума Российской Федерации.

Уже в 80-е годы у нас были персональные компьютеры, собственные операционные системы, собственные редакторы, собственные системы управления базами данных. В чём-то, конечно, технические средства были несовершенны, но по функционалу они были равными тем, что были у Стива Джобса – так сказать, IBM PC Compatible. Ещё в середине 80-х годов институт получил государственное задание по использованию современных средств вычислительной техники в школах. Мы проделали огромную работу, были выбраны ПК фирмы Yamaha (замечательные компьютеры, они до сих пор работают) и установлены более чем в 1000 школ Советского Союза.

«ОДНО ТО, ЧТО ТАМ ВЫДАВАЛИ КРОССОВКИ – ЭТО БЫЛО ЧТО-ТО»

Научно-практическая деятельность была вполне успешной. По профессорско-преподавательскому составу факультет ВМК МГУ был на голову выше многих и многих зарубежных университетов. Нас учили Прохоров, Ильин, Тихонов – он первую лекцию читал нам первого сентября, пришёл с распечаткой многометровой (метров 16–20) числа Пи с точностью до сотен знаков, рассказывал, как можно этого добиться. Люди, которые нам преподавали, являлись и являются крупнейшими учёными страны.

Последние годы Вы как-то взаимодействовали с ВМК?

Постоянно, всегда. У меня в институте очень много выпускников ВМК разных лет. В ИПИ РАН постоянно обучаются аспиранты ВМК, преподает Калиниченко Леонид Андреевич, специалист мирового уровня в области программирования. Его аспиранты, студенты часто потом работают в ИПИ РАН. У нас есть несколько научно-образовательных центров с ВМК. Этот симбиоз постоянный. На самом деле, считаю ВМК тем местом, где я сформировался как человек.

Вы такой занятой человек, а остается ли у Вас время на какое-либо хобби или на спорт?

Спортом я давно уже не занимаюсь, водным туризмом. Основная причина в том, что с распадом Советского Союза труднодоступны стали горы в СНГ. Ну а потом уже, видимо, возраст, дополнительные обязанности. А если говорить о каком-то хобби, очень увлекаюсь рыбалкой, но последние несколько лет все реже удаётся найти свободное время.

Есть ли у Вас настольная книга, которую Вы постоянно перечитываете?

Есть. Во-первых, Лев Николаевич Толстой. Это классика, к которой нужно относиться с интересом. У него исключительно строгие в логическом смысле произведения, там всё связано между собой, ничего лишнего, несмотря на большие объемы. Поэтому «Войну и мир» я постоянно держу под рукой.

Очень люблю Тургенева. После прочтения его произведений какое-то время даже не могу читать переводную литературу, он величайший русский писатель.

Зарубежных авторов люблю меньше, корявость перевода всегда чувствуется, а в оригинале читать не могу: не настолько владею языком, чтобы понимать все нюансы.

Что бы Вы хотели пожелать студентам?

Больше учиться, меньше работать, пока студенты. Затем сторицей воздастся. Каждую минуту уделять учёбе. Потом это сильно чувствуется и в человеке, и в его карьере, и в его отношении к жизни, и, как ни странно, в разнообразии интересов.

ИНФОРМАЦИЯ О КАФЕДРЕ:
cs.msu.ru/departments/ib

Иван Чижов

Про криптографию, амбарные замки и почту ВМК

У факультета ВМК есть корпоративная почта https://webmail.cmc.msu.ru. Если вы перейдёте по этому адресу в браузере, то случится страшное! Появится сообщение «Сертификат безопасности этого веб-узла не был выпущен доверенным центром сертификации» и рекомендация покинуть страницу. Что же произошло? Попробуем разобраться на примере почтового сервиса Gmail.

Таинства безопасности

Сервис Gmail позиционируется как очень безопасный. Когда вы заходите на gmail.com, вводите логин и пароль и нажимаете «Войти», происходит перенаправление на страницу, имеющую префикс https (такой же, как в адресе почты факультета) вместо привычного http. Это означает, что данные передаются по защищённому каналу, то есть логин и пароль шифруются перед отправкой на сервер, где они будут расшифрованы и проверены на корректность.

Чтобы что-то зашифровать, нужно иметь ключ. И чтобы сервер смог расшифровать логин и пароль, ему нужно знать, на каком ключе они зашифрованы! Как же передать этот ключ? Если перешлём обычным способом, злоумышленник может его узнать, значит, и сам ключ надо зашифровать. Но тогда нужно передавать и ключ шифрования ключа! Значит, его также нужно зашифровать! Эти нехитрые размышления заводят в тупик. Получается, шифрование логина и пароля абсолютно неосуществимо?

Как возможно шифрование?

Уитфилд Диффи и Мартин Хеллман в 1976 году опубликовали статью «New Directions in Cryptology», в которой предложили концепцию криптосистемы с открытым ключом.

ТРАДИЦИОННОЕ ШИФРОВАНИЕ ПРЕДПОЛАГАЕТ, ЧТО У ОТПРАВИТЕЛЯ И ПОЛУЧАТЕЛЯ ИМЕЕТСЯ ОБЩИЙ КЛЮЧ, ХРАНЯЩИЙСЯ В СЕКРЕТЕ.

Это похоже на обмен сообщениями через ящик с врезным замком. Если вы с товарищем хотите тайно обмениваться сообщениями, то покупаете такой ящик и берёте ключи от него. Ваш друг кладёт записку в ящик, закрывает его своим ключом и передаёт ящик вам. Получив ящик, вы открываете его собственным ключом.

Шифрование с помощью криптосистемы с открытым ключом можно сравнить с обменом сообщениями через ящик с амбарным замком. Представьте себе место, где каждый может (совершенно бесплатно!) хранить свой амбарный замок. Вы покупаете амбарный замок и оставляете себе ключ от него, который больше никому не передаёте. Открыв замок, вы сдаёте его в хранилище. Ваш друг, желающий отправить вам сообщение, берёт ящик, находит ваш замок в хранилище и запирает им ящик. Заметьте: ключ ему для этого совершенно не нужен. Получив ящик от друга, вы просто открываете замок своим ключом.

В криптографии ключ от амбарного замка, который хранится у вас, называется *закрытым* ключом, а сам амбарный замок – *открытым*. Защёлкивание замка – алгоритм шифрования, а открытие замка – алгоритм расшифрования. Иногда алгоритм расшифрования называют *дешифрованием*. Но это некорректно:

ОБЫЧНО ПОД ДЕШИФРОВАНИЕМ ПОНИМАЕТСЯ ВЗЛОМ КРИПТОГРАММЫ ЗЛОУМЫШЛЕННИКОМ.

В нашем примере это взлом амбарного замка с помощью отмычки или процедура изъятия у вас ключа с помощью паяльника :)

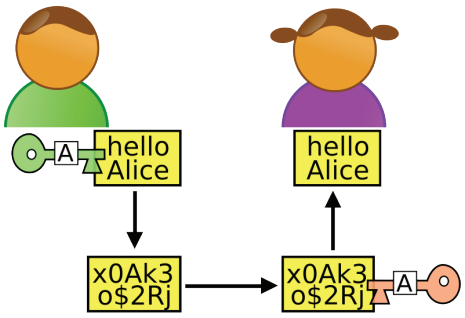
Протокол SSL/TLS на основе амбарных замков

Вернёмся к почте Gmail. Вооружившись замками и ключами, опишем процесс взаимодействия браузера и сервера.

СНАЧАЛА КОМПАНИЯ GOOGLE КУПИЛА АМБАРНЫЙ ЗАМОК, ОТКРЫЛА ЕГО И НАДЁЖНО СПРЯТАЛА КЛЮЧ.

По нажатию на кнопку «Войти» браузер запрашивает у сервера Gmail амбарный замок для шифрования. Сервер отсылает его браузеру по незащищённому каналу.

Источник фото: stockfreeimages.com



ТРУДНОСТИ ПЕРЕВОДА: АЛИСА И БОБ ДЕМОНСТРИРУЮТ МЕТОД ОТКРЫТОГО-ЗАКРЫТОГО КЛЮЧА

Получив амбарный замок, браузер генерирует собственный ящик с врезным замком. Дело в том, что в реальности пара логин и пароль шифруется именно криптосистемой с секретным ключом (ящиком с врезным замком), а не криптосистемой с открытым ключом (ящиком с амбарным замком), ведь врезной замок намного надёжнее амбарного! Секретный ключ при этом генерируется браузером случайным образом и кладётся в другой специальный ящик, который закрывается амбарным замком и отправляется почтовому серверу. Сервер, получив посылку, достает из надёжного места ключ от амбарного замка и вынимает из ящика ключ от ящика браузера.

Теперь у браузера есть свой ящик с врезным замком, а сервер имеет копию ключа от него. Всё готово для отправки логина и пароля.

БРАУЗЕР ПОМЕЩАЕТ ЛОГИН И ПАРОЛЬ В ЯЩИК С ВРЕЗНЫМ ЗАМКОМ, ЗАКРЫВАЕТ ЕГО СВОИМ КЛЮЧОМ И ОТПРАВЛЯЕТ СЕРВЕРУ.

Тот открывает ящик копией ключа и достаёт оттуда логин и пароль. Дальше всё просто: сервер проверяет корректность пары логин-пароль и либо открывает доступ к почте, либо сообщает, что данные неверны.

Описанная процедура обмена носит название протокол SSL/TLS. Конечно, вместо замков и ящиков в SSL/TLS используются их криптографические аналоги, для описания и построения которых используется сложнейший математический аппарат линейной алгебры, дискретной математики, теории групп, теории конечных полей, теории чисел, теории вероятностей...

А как же сертификаты?

Снова обратимся к почте ВМК и выясним, о каком сертификате идёт речь в сообщении браузера.

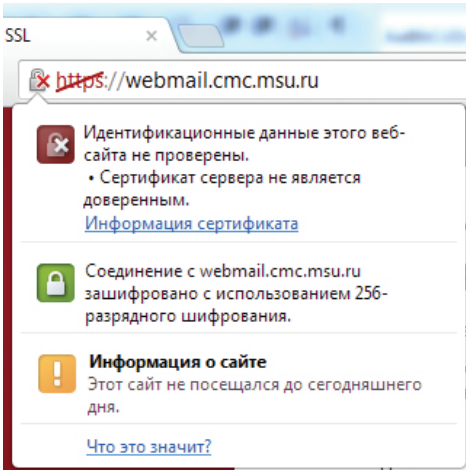
Как вы помните, в схеме шифрования с открытым ключом (ящик с амбарным замком) мы предположили наличие некоторого хранилища амбарных замков. Для шифрования сообщения ваш друг должен забрать замок из хранилища. Но если в этом хранилище поменяют ваш замок на замок Васи Пупкина, произойдёт путаница, Вася перехватит ваш ящик и сможет прочитать переданный секрет! Избавиться от таких неприятностей помогает сертификат открытого ключа: он гарантирует, что амбарный замок принадлежит вам, а не Васе.

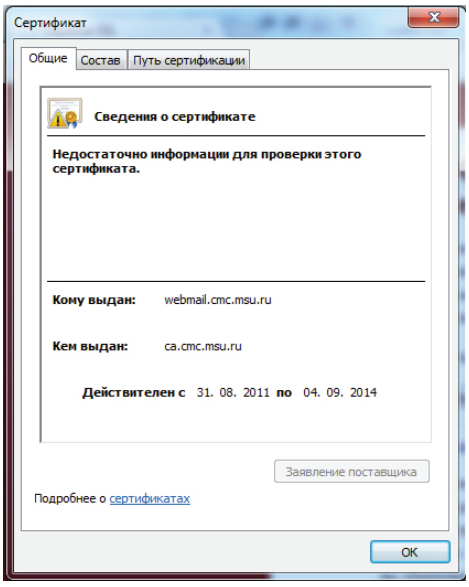
Если продолжать аналогию, сертификат работает так. Пусть доверенное хранилище имеет печать и бумажный конверт. Когда вы сдаёте замок, хранилище проверяет ваш паспорт, кладёт замок в бумажный конверт, подписывает его вашим именем и ставит печать. Теперь невозможно вскрыть конверт, не повредив штамп. Всё! Теперь никто не сможет подменить ваш замок. На языке криптографии хранилища называются удостоверяющими центрами, а конверты – сертификатами открытого ключа. Эти сертификаты гарантируют, что открытый ключ принадлежит именно вам.

Сообщение с предупреждением о доверии к сертификату открытого ключа появляется, в частности, если этот сертификат создан удостоверяющим центром, которому вы ещё не доверяете

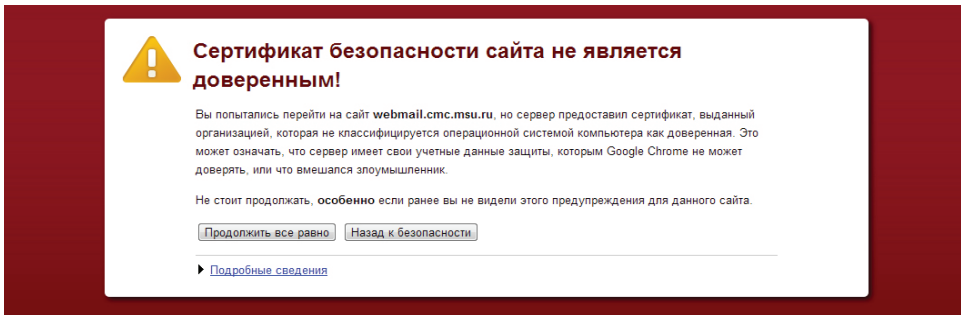
ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ СООБЩЕНИЕ БРАУЗЕРА: ЕСЛИ РЕЧЬ ИДЁТ ИМЕННО О НЕПРОВЕРЕННОМ ИЗДАТЕЛЕ, ПОСМОТРИТЕ, КЕМ БЫЛ ВЫПУЩЕН СЕРТИФИКАТ.

(в разных браузерах это делается по-разному, например, в Chrome нажмите на пиктограмму перечёркнутого замка слева в строке адреса и выберите пункт «Информация сертификата»). В случае почты ВМК, в поле «Кем выдан» стоит «ca.cms.msu.ru», а в поле «Кому выдан» – «webmail.cmc.msu.ru», так что можно смело открывать главную страницу почтового сервера. В других случаях так поступать не стоит.





А лучше всё-таки назначить удостоверяющий центр «ca.cmc.msu.ru» доверенным. Как – это уже совсем другая история...



Полную версию статьи смотрите в ЖЖ журнала.

Сания Зарипова

Научитесь управлять временем!

Фото с carolynbaana.com

В течение семестра многие сталкивались с катастрофической нехваткой времени, трудностями с учёбой и подготовкой к сессии. Основной источник таких проблем – неправильное распределение времени: зачастую вместо того, чтобы сделать всё заранее, а оставшееся время посвятить отдыху, мы откладываем дела до последнего и работаем в сжатые сроки. От этого страдает и качество проделанной работы. Мы расскажем вам о нескольких эффективных способах управления временем.

Тайм-менеджмент – это технология планирования и управления временем, помогающая избежать стрессов, утомляемости и апатии. Сэкономить до 25% времени поможет список дел, расположенных по убыванию приоритета. Помните: 10% времени, затраченного на планирование, сэкономит 90% времени при решении задач.

Основные правила планирования

• Обязательно фиксируйте свои планы на бумаге: «если цель не записана, то она не существует» *(П. Ф. Друкер «Эффективный управляющий»).*
• Список задач на следующий день готовьте с вечера. Так вы всегда будете знать, с чего начать.
• Добавляя в список новое дело, располагайте его в соответствии с приоритетом по отношению к остальным делам.
• Выполнив очередную задачу, вычеркивайте её из списка. Это даст вам чувство удовлетворенности от проделанной работы и прибавит энтузиазма.
• Сложную задачу делите на более мелкие, пока процесс её выполнения не станет простым и ясным.

Принципы Эйзенхауэра

«На все дела времени не хватит никогда, но его всегда достаточно для самого важного». Разделяйте дела на четыре группы по принципу американского президента *Дуайта Эйзенхауэра:*
1. Первостепенные задачи решайте немедленно, чтобы избежать неприятных последствий.
2. Важные, но не срочные дела можно отложить, но заранее просчитайте временной резерв, иначе они быстро превратятся в срочные и важные.
3. Срочные, но не важные задачи мало влияют на ваш успех и сильно снижают эффективность – уменьшайте их количество.
4. Несрочные и неважные дела можно смело вычеркивать из вашего списка.

Первым делом – «съесть лягушку»

В старой притче говорится: если утром вы должны съесть живую лягушку, по меньшей мере, это худшее, что может случиться за день. Бизнес-консультант *Брайан Трейси* сравнивает лягушку с самым важным и неприятным делом: вместо того, чтобы откладывать его, накапливая отрицательные эмоции и создавая ненужные последствия, расправьтесь с ним без раздумий и промедлений, это придаст вам заряд энергии на целый день.

Структурированная прокрастинация*

ЧИТАЙ ОБ ЭТОМ МЕТОДЕ В СТАТЬЕ: goo.gl/oP2Bs

При обычном методе планирования за дело с меньшим приоритетом нельзя браться, пока не выполнена задача с бóльшим. Однако есть и другой метод, предложенный *Джоном Перри,* профессором философии Стэнфорда. Так как вам не хочется выполнять самые важные (а значит, и самые трудные) дела, вы вместо этого занимаетесь делами, расположенными внизу списка. На мотивации не делать самое важное дело вы успеете сделать кучу полезного! Когда вы закончите эти дела, появятся новые задачи, еще более важные. Теперь важные дела превратились в неважные, и вы приступите к их выполнению с не меньшим энтузиазмом.

** Прокрастинация – склонность к постоянному «откладыванию на потом» неприятных мыслей и дел.*

Научитесь говорить «нет»

Лучший способ сэкономить время – отказаться от задач с самым низким приоритетом, на которые вы тратите много времени, но которые не приносят пользы и не приближают вас к цели. Не берите новых дел в периоды острой нехватки времени.

Порядок на рабочем месте – залог успеха

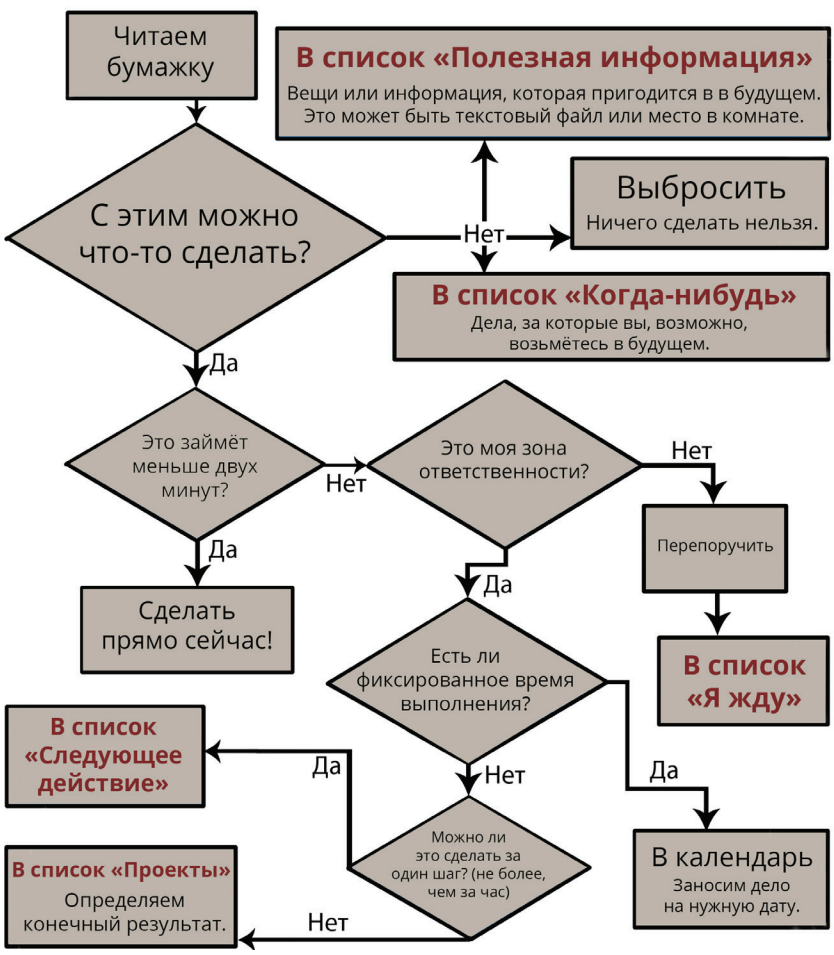
Беспорядок на столе свидетельствует о несобранности и непродуктивности. Периодически выбрасывайте ненужные бумаги, ведь на поиски в беспорядке тратится до 30% рабочего времени!

Прочь из моей головы

Интересную схему планирования предлагает *Дэвид Ален* («Как разобраться с делами»), она помогает максимально эффективно тратить свои силы и предотвращает появление дедлайнов.

Подготовьте много маленьких бумажек и корзину. Каждую мысль, которая появляется в вашей голове, необходимо записать на бумажку и положить в корзину. Мысли – от «как написать эту программу?!», «хочу в Европу», «люблю Васю» до «передо мной лежит карандаш», «жизнь не имеет смысла» – должны оказаться в корзине, отчего в мозгу появится необычайное состояние лёгкости и свободы.

Далее каждая бумажка перемещается из корзины в один из списков по следующей схеме (класть бумажку обратно в корзину нельзя):



Нужно организовать пять списков так, чтобы они были мобильны, в них легко было добавлять и убирать информацию. Можно завести тетради или, что более близко ВМК-шникам, всю систему документов хранить в Evernote, Dropbox и других программах. Приложения для телефона, компьютера или планшета сделают их доступными отовсюду.

Списки можно дробить. Так, «Следующее действие» можно разбить на «Дома», «На факультете», «В магазине», «В интернете».

ЕСЛИ УТРОМ ВЫ ДОЛЖНЫ СЪЕСТЬ ЖИВУЮ ЛЯГУШКУ, ЭТО ХУДШЕЕ, ЧТО МОЖЕТ СЛУЧИТЬСЯ ЗА ДЕНЬ

Приходя на место, сразу выполняйте «следующее действие». Держите файл для записи мыслей и идей, приходящих в течение дня: главное не дать важным мыслям пропасть. Вечером все идеи за день переносите в соответствующие списки. Например, во время очередного разбора мыслей вы поняли, что на факультете вам надо зайти в учебную часть, сдать распечатанную программу, забрать у друга флешку, спросить у одногруппника про алгоритм и скопировать программу с компьютера машзала. Образуется список мелких дел, которые можно сделать и за час. Начните выполнять их в интуитивном порядке, как хочется. Если обновлять списки каждый день, в каждом будет небольшое количество дел, и вы успеете выполнить все. При этом интуитивный, подсознательный выбор не доведёт до дедлайнов.

Раз в неделю просматривайте списки, чтобы вычёркивать лишние, переносить существующие дела, заносить новые мысли и идеи.

Так вы освобождаете свою голову от потока мыслей. Количество дел, которые вы держите в голове, обратно пропорционально эффективности: очистив голову от кучи дел, вы освобождаете место под новые идеи и творчество. В «пустой голове» возникают новые гениальные идеи, на которые раньше просто не было сил из-за рутины.

Отдых

Не забывайте о правильном отдыхе. Тайм-менеджмент не поможет, если вы не будете поддерживать себя в хорошей форме. Не доводите себя делами до изнеможения. Если ваша жизнь интересна и насыщенна, у вас больше сил для эффективной работы. Наконец, очень важна мотивация: написанный на бумаге идеальный план может и не осуществиться при отсутствии энергии. Всё в ваших руках!

Романа Галицкая

Россия снова покорила ACM/ICPC

3 июля 2013 года в Санкт-Петербурге состоялся финал чемпионата мира по программированию ICM/ICPC. Чемпионат впервые проходил в России, его принимал университет Информационных технологий, механики и оптики, команда которого четырежды становилась чемпионом и в этом году стала им в пятый раз! Наш корреспондент побывала на чемпионате и расспросила участников и их наставников обо всех подробностях.

Четвертьфинал олимпиады среди команд Москвы и Московской области проходил на ВМК в октябре 2012 (см. № 19). В рамках Школы Журналистики*, куда члены нашей редакции ездят не первый год, я посетила финал ACM/ICPC в спортивном комплексе Юбилейный.

Мы приехали к СК в девять утра. Была чудесная погода, и участники чемпионата группками в цветных футболочках прогуливались перед зданием. Я подошла к ребятам в ярко-фиолетовом, команде из Кубы.

Наставник команды – молодой человек с интересным именем Vladimir Antonio Charchabal Escalona (на фото второй справа). Ребята сказали, что хорошим результатом для них будут три-четыре решённые задачи, а самой сильной они считают команду ИТМО, в чём не ошиблись. Экскурсии по Питеру, организованные для всех приезжих участников, им очень понравились, как и Москва, где они уже побывали ранее.

ЗАДАЧИ СПЕЦИАЛЬНО СОСТАВЛЯЮТСЯ ТАК, ЧТОБЫ НЕВОЗМОЖНО БЫЛО РЕШИТЬ ВСЁ

На входе в спортивный комплекс всем гостям чемпионата выдавали красивые бейджи. Я встретила команду МГУ, они были одеты в чёрное и очень серьёзны, даже разговаривать со мной не стали – объяснили, что настраиваются. Это было не зря: решив шесть задач из одиннадцати, они получили бронзу.

До начала соревнования прошло больше часа. Мы успели хорошенько рассмотреть множество столов с ограждениями, на которых были написаны названия университетов, и послушать громкий голос невидимого организатора, который рассказывал на английском что-то весёлое и воодушевляющее (из-за эха слов было не разобрать) командам, которых мы тоже не видели. Наконец, участники стали заходить в зал. Пространство со столами быстро заполнялось потоком людей в разноцветных футболках. Ребята махали зрителям, многих встречали овациями. Все расселись, ставший видимым организатор сказал пару напутственных слов, обратный отсчёт на больших электронных часах дошёл до отметки 0:00:00 – и чемпионат начался!

НЕЛЬЗЯ ПРОСТО ТАК ВЗЯТЬ И ПЕРЕСТАТЬ УЧАСТВОВАТЬ

Огромная масса людей за столами всколыхнулась, и все принялись за работу. Любое действие команды – решение, отправка задачи и результаты её проверки судьями отображались в огромной он-лайн таблице. Всем зрителям выдали распечатанные задания олимпиады, что приятно удивило. Пока команды были заняты задачами, я решила побеседовать с сидящим справа молодым мужчиной, который явно был не просто неосведомлённым зрителем.

Денис, за какую команду болеете?

Наш университет в этом году не участвует, поэтому болеем за все российские команды и за те, которые приезжали к нам на сборы из других стран – поляки, японцы [в Петро-

** Школа Журналистики от газеты Gaudeamus – тренинговые занятия, дающие журналисту и редактору все необходимые знания. О поездке сотрудников газеты на Школу в прошлом году читайте в номере 18.*

заводском ГУ, где преподает *Денис Власов,* регулярно проходят сборы для команд вузов-участников соревнований по программированию – прим. автора].

Расскажите, пожалуйста, о задачах.
Здесь одиннадцать задач, специально подготовленных для финала чемпионата мира. Они достаточно сложные, не бывает такого, чтобы все задачи были решены какой-либо командой: обычно решают восемь, максимум девять задач. Задачи составляются так, чтобы всем было, что решать, но невозможно было решить всё. Этого не могут сделать даже самые-самые крутые.

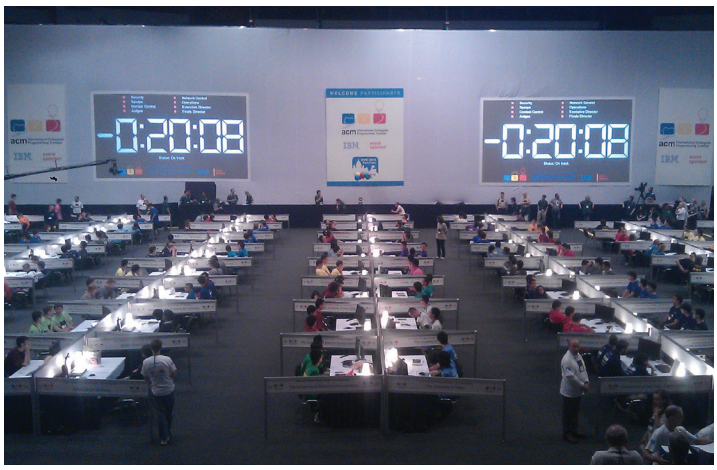
Как распределяются медали, какие призы?
Всего участвует 120 команд, вручается двенадцать комплектов медалей: четыре золотых, четыре серебряных, четыре бронзовых. Иногда бывает путаница, когда говорят, что команда получила серебряные медали, и люди думают: о, второе место, а это на самом деле какое-нибудь восьмое. Некоторые призы, конечно, будут денежными. Есть отдельные премии: если команда первой сдаёт задачу на контесте, они получают денежный приз. Если команда сдаёт задачу, которую до них ещё никто не сдал, они тоже получают денежный приз, и также воздушный шарик, который приносят и за каждую сданную задачу.

ЗАДАНИЯ ОЛИМПИАДЫ МОЖНО СКАЧАТЬ ЗДЕСЬ: goo.gl/5XpS1J

Имеют ли команды доступ к общей таблице результатов?
Конечно, но она обновляется только четыре часа, последний час результаты не показываются. Однако свои результаты участники знают всегда. Решённые задачи проверяются в автоматическом режиме, потому что тесты огромные.

Команды из каких стран считаются самыми сильными?
Россия, Китай, Польша; США, может быть. Топовые команды постоянно в тренировках, это как спортивная форма. Нельзя просто так взять и перестать участвовать, а потом опять включиться. Плюс нужна командная работа, недостаточно просто взять трёх талантливых участников: они будут друг другу мешать, ведь каждый привык сам по себе работать.

КОМАНДА КУБИНСКОГО УНИВЕРСИТЕТА UNIVERSIDAD DE LAS CIENCIAS INFORMATICAS



фотографии автора

УЧАСТНИКИ ЗАНЯЛИ СВОИ МЕСТА. ДО НАЧАЛА СОРЕВНОВАНИЯ ОСТАЛОСЬ 20 МИНУТ

Также я побеседовала с тренером сборной МГУ *Антоном Панкратьевым.*

Антон Евгеньевич, расскажите о нашей команде.
Она состоит из двух мехматян и одного выпускника ВМК, все трое родом из Саратова. Они уже давно тренируются вместе, и последние два года это, пожалуй, лидирующая команда МГУ. Сейчас многие московские команды готовятся на базе Яндекс-тренировок. Мы решаем и задачи прошлых лет разных соревнований, ездим на Петрозаводские сборы – уникальное мероприятие: опыт, который там приобретается, в чём-то играет решающую роль в подготовке.

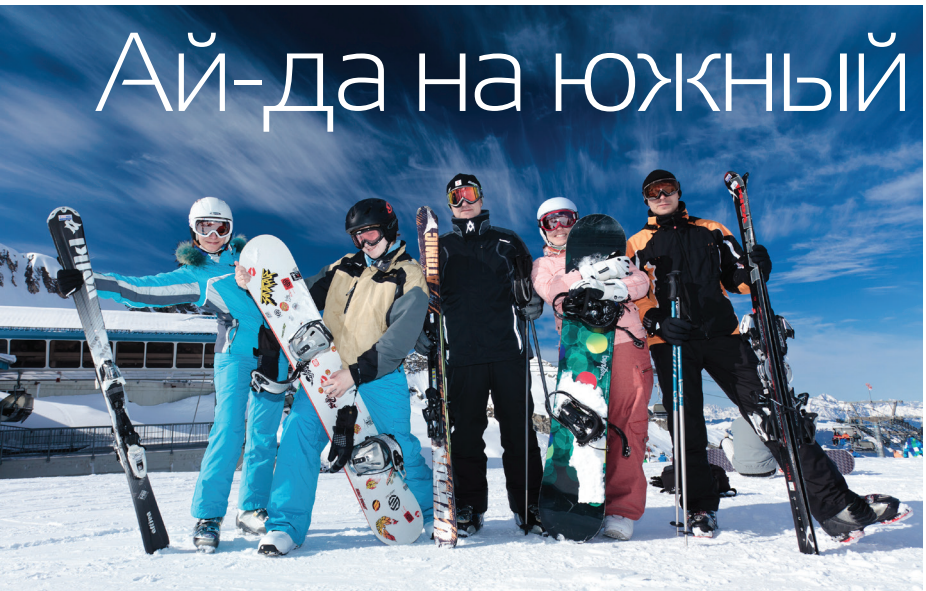
Какие бонусы при трудоустройстве даёт участие в этой олимпиаде?
Ведущие IT-компании пристально следят за этим мероприятием и вообще за олимпиадной активностью. В России она часто называется ACM-активностью, но это не совсем верный термин: ACM – структура вполне конкретная, а речь идет об олимпиадном программировании вообще. Все ребята, которые здесь занимают какие-то места, на виду, и им предлагают неплохое трудоустройство, как у нас, так и за рубежом.

***

Чемпионат можно было смотреть в прямой трансляции на icpclive.com, где есть вся информация о мероприятии, участниках и итогах. Команда ИТМО решила рекордное число задач – 10 из 11-ти – и заняла первое место! Поздравляем ребят из Санкт-Петербурга с неизменным мировым успехом, команду МГУ с почетной бронзой и желаем новых побед!

Наталья Морозова

Ай-да на южный... покатаемся!



«Какой же русский не любит быстрой езды?» – писал классик о езде на тройке. А мы поговорим о горных лыжах и сноуборде. Если живёшь в «снежной» стране, то желание насладиться скоростью, ощущением полёта и пушистым снежком вполне естественно! А чтобы встать на лыжи или сноуборд и покорить новые вершины на зимних каникулах, стоит запастись снаряжением уже сейчас. Итак, кататься: где, как, с чего начать?

Для новичков: лыжи или сноуборд?

Спор, что же круче, бессмысленен: каждому своё. В первом приближении, лыжи – это скорость, а сноуборд – это фишки. Есть мнение, что на лыжи легко «встать», но тяжело научиться технично кататься, а со сноубордом наоборот: период «знакомства» с доской длительный, но зато при уверенном знании азов уже можно делать очень многое.

Обучить технике могут опытные друзья или инструктор, которого можно найти в любом центре катания.

Стоимость часа индивидуального занятия – примерно 1200–1500 руб.

Снаряжение

Вам понадобятся особые крепления, ботинки, одежда и защита. Всё перечисленное различается для горных лыж и сноуборда.

Новичкам-сноубордистам точно стоит обзавестись непромокаемыми штанами, перчатками и шлемом. Сноуборд, в отличие от «знакомых» лыж, поначалу оказывается сложным в управлении, как на поворотах, так и при наборе скорости.

Характеристики снаряжения выбираются в зависимости от того, где и на чём вы собираетесь кататься. Для новичков сноуборд и лыжи должны быть «мягкими», они легче в управлении и дешевле. Когда вы определитесь со стилем, скорее всего, придётся сменить тип лыж или доски.

Прокат

В оборудованных местах катания обычно можно взять всё необходимое напрокат, в том числе одежду и защиту. Другое дело, что цена проката за неделю вполне может превысить стоимость снаряжения как такового, к тому же придётся каждый раз привыкать к выданному оборудованию.

Прокат полного комплекта – около 1,5 тыс./день

Где и что купить, цены

Рассмотрим полную экипировку с наилучшим соотношением цена-качество. Горнолыжные виды спорта – достаточно дорогое удовольствие. В глобальной сети море интернет-магазинов с интересующим товаром. В специализированных салонах часто встречаются компетентные продавцы, способные помочь в выборе, но и цена будет соответствующая. Есть более дешёвые магазины-склады на окраинах Москвы, но их реальный ассортимент может отличаться от выставленного на сайте. Выгодно ловить сезонные скидки, брать «народные наборы» – уже собранные полные комплекты снаряжения со скидкой. При ограниченности средств рекомендуется уделить основное внимание ботинкам. Они должны сидеть очень плотно, не сдавливая ногу. В числе хороших фирм – K2 и Salomon (лыжные), Vans и Burton (сноубордические).

По личному опыту, перед походом за снаряжением необходимо набраться терпения и взять с собой средств с запасом.

Стоимость полной экипировки – от 20 тысяч

Дополнительные сведения

ski.ru – обширный сайт, в наличии FAQ по горным лыжам

onboard.ru – есть карта мест катания по России с отзывами

snowboard.ru – отличный FAQ на форуме, динамичный раздел по покупке-продаже оборудования б/у

mski.ru – список мест катания по Москве с подробными описаниями

Где покататься?

Поездка в горы – отличный способ быстро обучиться. Здесь и длина спуска намного больше, чем на искусственно созданных склонах, и тренировки продолжительнее и интенсивнее. Объединяет горнолыжные курорты всех стран наличие оборудованных трасс, подъёмников, пунктов проката, возможность снять жильё поблизости, а также примерно одинаковая цена на карту для многоразового пользования подъёмником – ски-пасс. Катание в горах может быть всесезонным или зимним, в зависимости от расположения гор и высоты трасс. Итак, куда поехать?

Европа. Главное достоинство европейских центров катания – развитая инфраструктура и хороший сервис. Высокое качество организации трасс разных уровней сложности, специально оборудованные места для катания в разных стилях. Отличными горнолыжными курортами славятся Австрия (долина Циллерталь), Франция (Куршевель, Шамони), Италия (район Доломитовых альп), Финляндия (курорт Леви в Лапландии). Неожиданным открытием может стать Андорра – карликовое государство между Испанией и Францией, живущее за счёт горнолыжного туризма.

Авиабилеты в оба конца – от 14 тысяч руб.

Ближнее зарубежье. Для тех, кто не хочет уезжать далеко, можно найти вариант поближе. Получится дешевле, хотя экономия происходит в основном за счёт дороги и проживания. Это зимние горнолыжные курорты Болгарии и западной Украины (украинские Карпаты). Стоит отметить доброжелательность и радушие жителей курортных мест в Карпатах (Ворохта, Яремче, Буковель) к российским туристам. По отзывам, в ближнем зарубежье места катания в среднем обустроены лучше, чем в России, но, безусловно, уступают по качеству сервиса европейским.

Россия. И у нас, конечно, есть, где покататься! Взять хоть Домбай и Урал. Ближе к столице, в Подмосковье, расположено много зимних горнолыжных курортов. В их числе спорткомплекс Волен, горнолыжный клуб Леонида Тягачёва, спортивный курорт Сорочаны.

Условные обозначения в таблице

К.п. – Кресельные подъёмники
Б.п. – бугельные подъёмники
С-п – Сноуборд-парк
Р. – Раздевалка
Об. – Обучение
Пр. – Прокат
К. – Кафе

Кол-во трасс	*Перепад высот*	*Протяжённость*	*Стоимость подъёма*	*Инфраструктура*
МОСКВА				
«Узкое» Пр. Севастопольский, напротив вл. №66; 8 (495) 978-96-78, 8 (901) 517-96-78				
3	40 м	200 м	20–50 р. в зав. от кол-ва	Б.п., пр., об., к., с-п, р.
«Кант»; kant.ru/pages/sport/; 8 (495) 669 78 49, 8 (499) 317-48-33				
7	25–50 м	135–210 м	15–60 р.	Б.п., пр., об., камера хранения, к., с-п
Северное Бутово; ул. Старокачаловская, д. 22: 8 (903) 796-09-56				
1	35 м	120 м	30 р.	1 б.п., пр., р., об.
«Звёздочка» 700 м от м. Орехово по Шипиловскому проезду				
3	40 м	110–250 м	100 - 250 р. /час	Б.п. (только в вых.: 11:00 – 17:00), с-п
Крылатское («Лата трэк»); lata-track.ru				
6	55–60 м	55–60 м	30–50 р.	Б.п., к.п, в т. ч. детские, пр., об., с-п, к.
Новопеределкино; Проектируемый проезд 635, д. 9, стр. 1; (495) 435-02-68				
4	50 м	460 м	30 р. (буд.), 50 р. (вых.)	Б.п, к.п, пр., об., big air, к.
ПОДМОСКОВЬЕ				
«СНЕЖКОМ» (г. Красногорск) snej.com; 8 (495) 225-22-33, 7 (495) 984-08-65				
1, зато круглый год	65 м	365 м	1 ч – 500 р. (буд.), 750 р. (вых.) 30 п. – 1100 р., доп. 5 – 200 р.	К.п., б.п., в т.ч. детский, пр., р., об., с-п, к.
Парк «Яхрома» (г. Яхрома) ya-park.ru; 8 (495) 981-89-39				
7	40–60 м	100–600 м	30 р. (буд.), 70 р. (вых.)	Всё + проживание
Сорочаны (недалеко от Яхромы) sorochany.ru; 8 (495) 788-85-44				
10	До 90 м	До 1050 м	70 р. (буд.), 150 р. (вых.)	Всё + проживание
Волен (2 комплекса: у Яхромы и у д. Степеново) volen.ru; 8 (495) 981-88-94, 8 (985) 180-43-25				
Я. – 14 С. – 4	Я. – до 70 м С. – до 90 м	Я. – до 450 м С. – до 960 м	балльная система, на сайте парка	Всё + проживание

Данные актуальны на зимний сезон 2012–2013

Фотографии: Евгений Донцов

«Слово не воробей...» – избранные цитаты преподавателей

«Вам ведь хочется раскрыть скобки?! Конечно, хочется! Любому нормальному человеку хочется раскрыть скобки!»
ПОЛОСИН А. А.

«Мы будем жить с вами в линейном пространстве! Надеюсь, что понравится»
ПОЛОСИН А. А.

«Помнится, любили мы в детстве взять какую-нибудь вершину параболы...»
БУДАК Б. А.

«...потому, что другу можно заглянуть в его закрытые члены!»
ВОЛКОВА И. А.

«Я допускаю, что это не совсем понятно, но это тривиально»
ТЫРТЫШНИКОВ Е. Е.

«Ну, вообще, гармонический ряд расходится, но в программировании он сходится!»
СОЛОВЬЁВ С. Ю.

«Нельзя так просто изменить константу. «Ха-ха!» – сказали создатели Паскаля»
СОЛОВЬЁВ С. Ю.

Если вы хотите, чтобы высказывания ваших любимых преподавателей были опубликованы в нашем журнале, присылайте их на почту **vnogus@gmail.com**

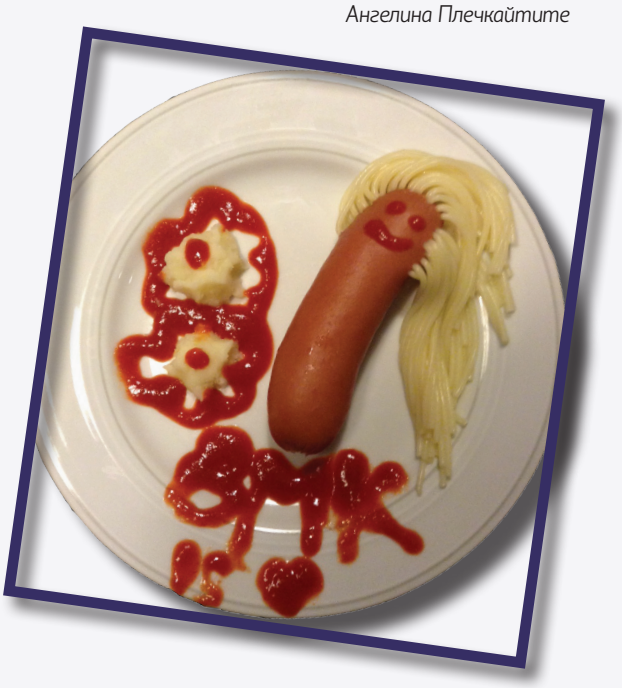
«Всё, что происходит на семинарах, вы стремитесь забыть, как дурной сон, но специфика процесса состоит в том, что вспомнить вас заставят»
АБАКУМОВ М. В.

Вычёркивая из списка отчисленных после первого курса: «Приятно видеть результаты своей деятельности!»
АБАКУМОВ М. В.

«В языке Ада есть пакет Standart. Считается, что любая адская программа вложена туда»
ГОЛОВИН И. Г.

Готовим по-общажному!

Ангелина Плечкайтите



Хотите вкусно поесть, но лень целый день стоять у плиты? Не умеете готовить, а соседка по общаге уехала? Надоели одни и те же макароны и картошка? Тогда вам сюда! Узнайте, как быстро, бюджетно, а самое главное – просто приготовить вкуснятину.

Волосатая сосиска

Вам понадобятся:
- сосиска
- спагетти

Приготовление:
1. Протыкаем сосиску вдоль (или поперёк – как больше нравится) сырыми спагетти.
2. Забрасываем в кипящую воду и варим до готовности (около 10 минут).

Приятного аппетита!