Крис Касперски:
«Компьютер как средство решения проблем сам стал одной большой проблемой»

Крис Касперски, специалист по ИБ, хакер и автор «компьютерных» книг, интервью не дает. Ныне Крис живет в США, трудится аналитиком по ИБ в крупной американской компании и по-прежнему видит в работе главный смысл жизни. Паблисити его абсолютно не интересует. Но для нашего издания он сделал исключение — ведь именно в «Системном администраторе» в 2003-2006 годах увидела свет его книга «Записки исследователя компьютерных вирусов»

Беседовал Игорь Савчук

Крис Касперски (Николай Лихачев) – известный хакер российского происхождения, автор популярных книг на русском и английском языках по компьютерной безопасности и низкоуровневому программированию. В настоящее время живет и работает в качества эксперта по ИБ в Редмонде, США. Считает работу смыслом своей жизни. Хобби – астрономия, стрельба из оружия.

– Крис, общеизвестно, вы – образцовый трудоголик. Получается, вся ваша жизнь проходит перед монитором?

– У меня основное время уходит на обдумывание алгоритмов со схематическим изображением квадратиков со стрелочками на бумаге. Вот вам и ответ на вопрос, как не сидеть целый день за компьютером.

Разность ощущений, разумеется, колоссальна. На бумаге значительно меньше знакомест. Даже если брать стандартную консоль (80x25), то нам потребуется целый альбомный лист, а чтобы записать алгоритм в блокноте (не путать с notepad.exe), приходится вспоминать крылатое выражение «словам тесно, а мыслям просторно». Иначе мы будем писать исключительно в write-only-режиме и потом сами не поймем, что это такое и куда оно работает.

Наверное, поэтому я смутно представляю, зачем нужны IDE и рефракторинг, когда есть FAR и – для полного счастья – colorer (впрочем, на Mac я все-таки использую TextMate, но это все же намного ближе к FAR, чем к Visual Studio, тем более что FAR с colorer поддерживает сотни языков, как, впрочем, и TextMate).

– Слагают легенды о вашей верности FAR и его известному плагину, также говорят, что с их помощью вы можете практически все…

– Это не легенды. У меня действительно нет никакого IDE, colorer может не только раскрашивать текст, но и прыгать по парным скобкам, обеспечивает навигацию по функциям (и это еще далеко не все). К тому же он у меня «перепиленный» под себя вдоль и поперек. Вообще у colorer удивительная архитектура, и для расширения функционала даже не обязательно залезать в его исходные тексты.

– Расскажите о вашем рабочем месте и типичном софте. Сколько у вас компьютеров? Каких?

– Сейчас у меня в работе два Mac, восемь «виндовых» лаптопов, стопка «никсовых» серверов, и они укомплектованы обычно следующим образом:

> Под Win: FAR+colorer, HIEW, OllyDbg, IDA-Pro, Python, MS VC.
> Под Mac: TextMate, SynalyzeIt, IDA-Pro, Python, GCC.
> Под Linux: vim, NetBeans, IDA-Pro, Python, GCC.

Мой стандартный комплект влезает на флешку и работает на любой системе, включая *nix и Mac. Компилятор локально не нужен – он стоит за тридевять земель и всегда доступен по ssh. Почему некоторые считают Visual Studio вершиной прогресса, и, кстати, что это за странное слово «рефракторинг»?

Мой вам совет – Festina Lente («поспешай медленно»). Не делай наспех, чтобы потом гарантированно не переделывать. Сначала думай, а потом пиши (программный код), и не пиши заведомо абы как, утешая себя тем, что потом «отрефакторишь». Такой подход формирует привычку, а привычка – это вторая натура.

Впрочем, не нужно зацикливаться на инструментарии и любимых компьютерах. К примеру, я выиграл международный конкурс по обфусцированию JavaScript, сидя при этом в кафе, где у меня с собой был только телефон BlackBerry. Так что не рабочее окружение делает человека. Один хороший знакомый недавно набросал прототип будущей системы и заключил контракт на несколько миллионов долларов на салфетке в таком же прибрежном кафе. Потому что никакой другой бумаги просто не было под рукой. А вот плохому танцору вечно что-то мешает…

– Вы владеете широким спектром языков программирования. Какова разница между низкоуровневым программированием на ассемблере и на высокоуровневых языках?

– Грубо говоря, отличие между языками программирования разных уровней как между тактикой и стратегией. При этом многие люди владеют одним из этих умений и немногие – двумя. Я работаю на низком (тактическом) уровне. На уровне архитектуры движка. Рядом со мной работают стратегические архитекторы, потому как движок без колес и руля никому не интересен.

– Как ассемблерщик и кодокопатель со стажем скажите, есть ли особая романтика у тех ядерных глубин, «куда не ступала нога джависта»?

– Ядро Linux доступно в исходных текстах, исходные тексты ядра Windows сегодня есть уже практически у всех, кому они нужны, потому для этого совершенно необязательно обращаться к дизассемблеру.

Что же касается романтики, вот вы мне скажите: а в армии есть романтика? Не в фильмах, а в реальной жизни? Когда жара под сто сорок, страшно хочется пить, но воды нигде нет, зато везде есть мины и на каждом шагу подстерегает смерть, причем от тренировки в реальном бою мало что зависит…

Все это кажется волшебством только до тех пор, пока не понимаешь, как оно работает, но, чтобы не понять, нужно очень сильно постараться. Достаточно лишь прочитать Modern Operating Systems by Andrew Tanenbaum и Windows Internals by Mark Russinovich.

– Насколько востребованы на рынке труда современных ИТ сильные ассемблерщики и системные программисты?

– Если вы посмотрите на runtime любого компилятора, то найдете там много ассемблера. Шелл-коды сплошь и рядом пишутся не то, что на ассемблере, а чуть ли не в машинном коде. В исходниках Google V8 (движок JavaScript для Chrome) также много ассемблера, причем намного больше, чем под одну платформу. Надеюсь, вы не станете утверждать, что Chrome – это неактуальная, неадекватная, невостребованная и несовременная программа? А это ведь даже не malware и не микроконтроллеры…

Тем не менее мне не знакомы люди, целиком и полностью «обитающие в ядре», равно как не знакомы компании, ищущие таких людей. Знание ядра и ассемблера – это плюс для большинства программистов всех мастей (включая прикладных). Уже хотя бы потому, что исчезает элемент мистики, и транслятору всегда можно заглянуть под капот, вместо того, чтобы гадать: это моя ошибка или компилятора?

В любом случае у меня за плечами порядка двадцати лет работы в этой предметной области. Менять свою специализацию слишком поздно, даже если кому-то где-то больше платят.

– Одна из ваших основных специализаций – анализ вирусов и самого разного malware. Вначале были стелз-вирусы, затем пришла эпоха полиморфов, а что потом?

– …а потом «замысловатые слова» посыпались как из рога изобилия. Advanced persistent threat (или сокращенно APT) обычно включает в себя сокрытие факта своего присутствия в системе (он же Stealth, он же Root-Kit), активное/пассивное противодействие обнаружению и удалению и т.п.

Полиморфизм – это частный случай метапрограммирования. В computer science под метапрограммированием обычно подразумевают программу, результатом работы которой является другая программа. Пассивные детекторы сканируют файлы в поисках уникальных последовательностей символов. Активные (или как их принято называть проактивные) детекторы работают по принципу поведенческого анализа. Грубо говоря, последовательность вызова API функций – это метрика. Поведенческий анализ распознает определенные сценарии (например, инъекцию кода в доверенный процесс) безотносительно того, как именно они реализованы, и последние несколько лет идут кровопролитные бои за видоизменение поведенческих сценариев до состояния, когда они становятся практически не отличимы от легитимных сценариев популярных программ.

Изменились и угрозы. Если во времена MS-DOS вирусы были «проблемой грязных рук» и не затрагивали тех, кто пользовался лицензионным программным обеспечением, то сейчас основная масса вредоносных программ распространяется через документы, эксплуатируя ошибки проектирования.

Дороже всего приходится расплачиваться за ошибки в сетевом стеке. Чтобы подхватить заразу, достаточно всего лишь интернет-подключения, даже браузер запускать

необязательно, хотя ошибки в сетевом стеке – большая редкость, и гораздо чаще хакеры проникают через святую троицу – pdf, jar, swf. По умолчанию браузер загружает их автоматически, и, если не установлены обновления, ждите проблем.

– То есть полиморфическим технологиям сейчас переломили хребет?

– Отнюдь. Во времена MS-DOS вирусы включали в себя генератор кода, доступный для анализа. Сейчас же код генерируется удаленно на хакерском сервере и отдается по HTTP-запросу. Или... не отдается. Сервер проверяет IP-источник запроса, и в случае каких-либо подозрений последующие ответы возвращают 404 или чистую страницу. К тому же хакеры обязательно проверяют IP на принадлежность к антивирусным компаниям и разным правительственным лабораториям. Да и сам генератор в любом случае остается недоступен. В лучшем случае вы можете его купить на черном рынке за наличные деньги, но чаще всего такая возможность недоступна, а потому в распоряжении аналитиков есть лишь отдельные экземпляры работы генератора, в которых необходимо выделить неизменную часть, что существенно затрудняет разработку детектора.

К тому же централизованный генератор хакеры могут обновлять так часто, как им вздумается. Прошли времена, когда вирусы работали только под MS-DOS и только под Intel x86. Сейчас необходимо распознавать не только машинный код x86, ARM, PowerPC, не только байт код (Java, Flash), но и бесчисленное множество скриптовых языков (JavaScript, VBScript, Python). Например, на Mac Python идет предустановленным, что открывает для хакеров новые перспективы. Кстати, Python замечательно распространяется не только в виде скриптов, но и байт-кода.

Мой вам совет — Festina Lente («поспешай медленно»). Не делай наспех, чтобы потом гарантированно не переделывать

– И каковы перспективы традиционного автоматического лечения вирусов?

– Автоматическое лечение (удаление троянцев) неуклонно сдает свои позиции, и зачастую оно сводится к переустановке системы. Кроме того, лечение возможно только на endpoints. Типичный IPS в лучшем случае предотвращает атаку, но не в состоянии обезвредить уже атакованные системы, поскольку IPS находится между атакуемым и атакующим.

Вообще сейчас у хакера другой приоритет – любой ценой передать управление на свой код, например, расположенный в файле документа и не рассчитанный на исполнение. Эта новая доминанта содействовала развитию веера новых технологий от NOP Slides до Heap-Spay и Return oriented programming (оно же ROP).

– Как антивирусная индустрия вообще справляется с огромным потоком новых зловредов? Сколько «дохлых тушек», положенных реверсеру на стол, реально обработать за сутки?

– Этим занимаются специально обученные люди и машины, причем машины все более активно вытесняют людей. Все, что можно автоматизировать, давно автоматизировано. Сейчас этих тушек столько, что никаких человеческих ресурсов на них не хватит. В качестве примера устройства этого процесса могу посоветовать интересную презентацию, ищите ее по ключевым словам: Adobe Malware Classifier.

Вообще дизассемблировать каждую тушку зловреда – это все равно, что хватать вражеских солдат по одному и допрашивать. Оно, конечно, полезно. Добыть языка. Одного. А лучше двух. Но что они могут рассказать? Стратегические планы верховного командования им все равно не известны.

Сегодня зловреды – они уже не сами по себе. Они – пушечное мясо на поле кибервойн, сегодня от них зависит чуть больше, чем ничего. Сейчас важно суметь понять устройство хакерской экосистемы – круговорота машинного кода и наличных денег.

– Вы упомянули о тотальной автоматизации как единственном способе выжить, и я сразу вспомнил о вашем патенте, который получен как раз на тему автоматизации...

– Было время, работал я удаленно. Ну, как работал? Анализировал огромное количество сплоитов, причем анализировал медленно, потому что навыка не было. Порядочно устав это делать, я написал программу, которая автоматически сгенерировала другую программу. И вот эта другая программа анализировала сплоиты со скоростью один гигабайт в секунду. Запустил ее и улетел в Берген (Норвегия) на встречу со знакомой немкой, с которой у меня тогда был роман.

И вот пока я гулял с немкой по сказочно красивой Норвегии, наслаждаясь золотой осенью и местным колоритом старинных замков и фортификационных сооружений, мой компьютер все это время стоял включенным «под нагрузкой».

И когда дней через десять вернулся, программа уже завершала анализ, но у меня хватило ума никому об этом не говорить и до конца года получать «убитых енотов» автоматом. А за пунктуальность и следование намеченным планам на работе мне еще бонусы давали. В конце концов меня заела совесть, и я выслал результаты машинного анализа одним и очень большим куском. В результате эта фирма надолго встала, и теперь мне же пришлось писать еще одну программу, чтобы автоматизировать труд тех, кто разгребал эти результаты, писал к ним тесты и заносил в базу. Собственно, так я и получил свой первый (и пока единственный) софтверный патент.

– Крис, я знаю, что в США у вас было неприятное приключение – однажды к вам нагрянуло ФБР. Как это было?

– Очевидно, меня подозревали и что-то искали, а потому все, что могли, изъяли. Никаких обвинений не предъявляли. Так что, по существу, мне сказать нечего.

– Я знаю, что ваш случай не уникален, подобные инциденты регулярно случаются с известными специалистами по ИБ и бывшими хакерами. Пройдя через все это лично, что вы посоветуете своим коллегам?

– Я бы посоветовал действовать по обстоятельствам. Мне-то было просто – я был уверен в своей невиновности. Возможно, я что-то и совершил по недомыслию, но абсолютно ничего криминального. Собственно, мне ничего и не предъявили, и даже мои адвокаты не знают, что у меня искали. Уверен, я бы и сам выдал им, если бы они сказали что им нужно было.

С тех пор, когда ФБР внезапно постучалось в дверь и изъяло все железо, все флешки и все-все-все, что у меня было, у меня появился ценный жизненный опыт. Теперь время от времени самое важные для меня данные я сбрасываю на «винт» и кладу в банковскую ячейку. Это мои личные файлы (не для чужих глаз). А все, что не представляет секрета, я активно раздаю народу. В тот раз мне пришлось собирать себя по кусочкам, качая файлы назад у тех, кому я их давал ранее. Месяца за три я собрал себя процентов на девяносто, кое-что оказалось утеряно безвозвратно, ну и ладно.

– Крис, вы успешный и легально работающий специалист в области ИБ и теоретически находитесь вне удара, но как поживают люди из андеграунда в наше жесткое время?

– Понятия не имею, никогда не был частью андеграунда. В досовскую эпоху андеграунд выпускал электронные журналы, но потом с появлением компьютерных законов эта деятельность прекратилась, а журналы типа российского «Хакера» стали неустанно мониторить силовые ведомства, и незавидна судьба тех, кто опубликовал информацию о реальных взломах. Сейчас андеграунд – это закрытый клуб, даже на их форумы можно попасть только по инвайту, причем там глубоко эшелонированная линия обороны, и, чтобы туда реально пролезть, нужно очень и очень постараться.

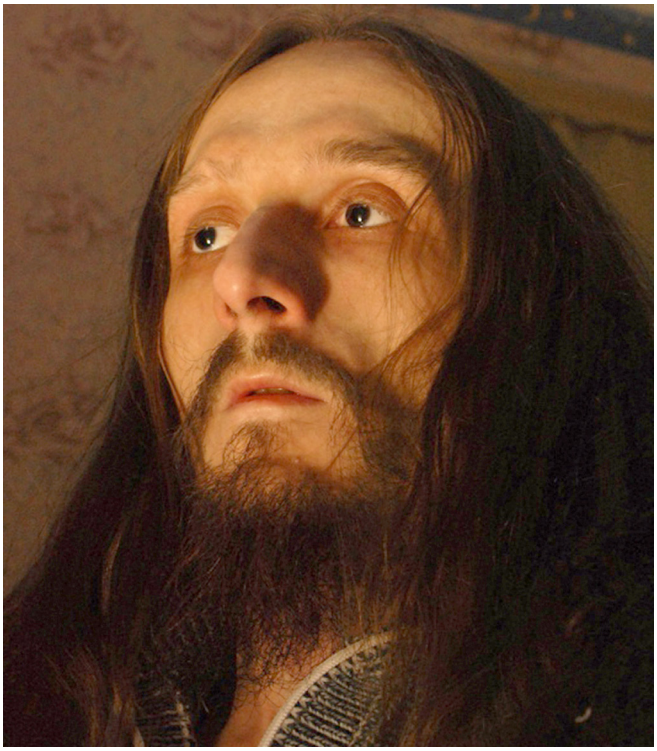
– Государство все более серьезно берется за контроль ИТ и Интернета по всему миру. К слову, что вы можете сказать о нынешнем законодательном регулировании Рунета?

– Во-первых, ничего о нем не думаю, потому что на меня оно не распространяется.

Во-вторых, если кто-то когда-то думал, что Интернет неподконтролен государству, то этот наивный человек даже не представлял, насколько телекоммуникации жестоко зарегулированы, что на каждый чих требуется лицензия, а потому все провайдеры де-факто и де-юре полностью подконтрольны государству. Другой вопрос, что государство совершенно не понимает, как технически устроен Интернет, и потому принимает неадекватные законы, обсуждать которые я не берусь, ибо не юрист.

– Как обстоят дела с контролем Интернета в США?

– В США контролируют Интернет, и этого никто не скрывает, причем в США, кроме федеральных законов, существуют еще и законы конкретного штата, что настолько усложняет картину, что без юристов тут ни за что не разобраться. Но в целом все устроено так, что большинство обычных американцев об этом не задумываются, ибо их это никак не касается.



У меня за плечами порядка двадцати лет работы в этой предметной области. Менять свою специализацию слишком поздно, даже если кому-то где-то больше платят

– Перейдем непосредственно к вашей специализации – информационной безопасности. Каковы сейчас самые общие тренды в этой области?

– Отвечая коротко – основные «тренды» уже сидят, причем сидеть им долго. Лет двадцать, а то и больше. На помощь антивирусам пришли FBI, CIA, US Secret Service и другие страшные слова. Поэтому сейчас маржа везде падает, а посадки растут.

Самый последний писк моды – в прицел атаки попали встраиваемые устройства. В первую очередь это, конечно, роутеры. Зловредный код в роутере очень сложно обнаружить. А тем временем хакеры нашли способ проникнуть внутрь камер наблюдения, подключенных к Ethernet, например, используя процессорные мощности для майнинга битконов. На очереди умная бытовая техника (например, холодильники), а также атаки на бортовой компьютер автомобиля – это фантастика новой реальности.

– Куда идет современный рынок коммерческих решений в области ИБ? Насколько я знаю, это одно из самых быстрорастущих и популярных направлений ИТ?

– У меня двадцатилетний опыт работы в индустрии безопасности, в том числе и на позиции архитектора. Я хорошо знаю рынок и видел множество примеров успешных начинаний, впрочем, неуспешных примеров было еще больше. Рынок систем безопасности действительно очень быстро растет. И растет он потому, что совсем недавно вирусами занимались школьники, «падонки» и прочие «креативные» личности. Затем ПК подключили к банкам, и тут оказалось, что на троянах можно делать деньги.

Рекорд в этом деле – двадцать лет отсидки за шесть доказанных нулей. Накинем еще один нуль за счет недоказанных, но... когда к Интернету подключили госучреждения, когда спецслужбы полностью компьютеризировались, внезапно выяснилось, что хакеры – это не просто «оболтусы с Дерибасовской», а угроза национальной безопасности.

Если изначально выбрать одно из молодых направлений ИТ-индустрии, то лет через пять можно начинать получать конкурентное преимущество

Уже несколько лет действия в киберпространстве США могут официально расцениваться как объявление войны и быть достаточным основанием для введения реальных войск на территорию противника.

Поэтому, как только государство появилось на рынке ИБ, домашние пользователи перестали быть в центре внимания просто потому, что у них нет пары десятков миллионов, с которыми они готовы расстаться (и еще столько же заплатить за поддержку). Причем все государства крайне смутно понимают, что им нужно покупать для своей безопасности, посему покупают они много лишнего.

Сейчас все крупные игроки, ну, то есть абсолютно все, купили огромное количество решений безопасности, и на гребне следующей волны пришли системные интеграторы, пытающиеся собрать эту груду разрозненного барахла воедино.

Но и этот гребень уже пошел на спад, а на горизонте маячит новый, третий. В практическом плане это означает: скоро предстоят сделки на миллионы и миллиарды долларов, но «повезет» здесь только тем, кто к этому уже готов и у кого уже есть готовые решения.

Напомню, что в свое время антивирусы для ПК дали рождение многим нынешним компаниям-миллиардерам, возникшим буквально на пустом месте без каких-либо инвестиций. Но это было относительно давно, в девяностых. Впрочем, суть осталась неизменной – большие деньги зарабатывает тот, кто первым предлагает «спасительную» услугу, когда еще никто толком не осознал своих потребностей и необходимостей.

– Можно ли привести примеры пока не заполненных ниш, чтобы наши читатели, молодые и амбициозные специалисты по ИБ, могли увидеть, где же лежит этот новый и такой вожделенный для многих Клондайк?

– Чего только ни ломают хакеры сегодня. И если на POS-терминале антивирус еще можно представить (хотя с большим трудом), то, например, на surveillance camera антивирус тупо не встанет, потому что это конструктивно не предусмотрено. Хотя де-факто там скорее всего ARM и портированный Linux.

Такая камера вещает потоковое видео, и там хакеры уже нашли дыры, позволяющие заливать шелл-коды со всеми вытекающими последствиями.

Вот мой личный пример из этой оперы. Недавно я прикупил пару Ethernet-камер для своего дома. С камерами идут аккаунты на сервере их производителя с персональным доменом третьего уровня – заходи себе через браузер, введи пароль и смотри удаленно, что там дома у тебя происходит. Два сервомотора обеспечивают свободу наведения, а ИК-подсветка видит даже в темноте – все было бы хорошо, если бы не было так плохо.

Жизнь показала, что эти камеры оказались дырявые, и в них уже поселился ботнет. Сетевым червям даже мозги напрягать не нужно: ваш домен третьего уровня (точка входа в контрольную панель камеры) – это, грубо говоря, число (в данном случае) очень короткое, а потому все камеры сканируются перебором влет и тут же автоматически взламываются. А вот обнаружить такую атаку затруднительно. Ну, то есть не то, чтобы совсем затруднительно... например, если в камере не включен HTTPS, то шелл-коды ловятся сниффером. А если включен? Мне повезло, что в моем случае производитель сделал фейковый HTTPS (ну, практически фейковый – у моей камеры нет ресурсов для шифрования видео, и потому по HTTPS она только пароль с логином передает, а все остальное гонит через HTTP).

Поэтому мне пришлось после работы самолично поковырять такую камеру из-за ее заражения, и я обнаружил, что ботнет откликается на определенные http-запросы к камере. Детектор зараженности, быстро написанный мною на «питоне», укладывается меньше, чем в сотню строк. Если накинуть еще пару сотен, то можно на Squid proxy через ICAP-фильтры давить попытки таких червей проникнуть в камеру, заворачивая их «на юг».

Еще личный пример. Видел в местном магазине микроволновку с Ethernet. По сети она сама выкачивает из Интернета время и режимы приготовления тех или иных блюд, используя сканер штрих-кода с упаковки товара. От наших электронщиков слышал, что там при старте прошивка грузится в ПЗУ, распаковываясь в память, и что холодный рестарт, возможно, спасет домохозяек. Но что такое холодный рестарт для микроволновки, особенно в США? Если черви будут атаковать потоково, просто устанешь перезагружаться.

Подведем итог: через несколько лет на рынке бытовой электроники будут миллиарды (!) подобных «умных» устройств, подключенных к Интернету. Многие из них на самом деле не умные, а очень даже глупые (потому как дырявые и уязвимые). Особенно если они подключены к ПК. Тогда тот, кто заразил ПК, может контролировать весь «умный» дом удаленно.

Но известные мировые производители бытовой электроники разбираются в безопасности, как «Тузик в апельсинах» (смотрите два моих личных примера выше). И потому они будут вынуждены выкупать сторонние решения. Все это огромный, только зарождающийся рынок. И он про-

сто гигантский! Поверьте, что рынок ПК в сравнении с ним «нервно курит в сторонке».

Сюда уже устремились первые и пока «совсем зеленые» поставщики решений ИБ. В первую очередь это стартапы, один из них недавно приобрел очень известный бренд бытовой электроники за деньги, которые лично мне даже не снились. А в том стартапе работают всего несколько человек, и они, между нами говоря, ничего нового почти и не сделали (слегка пропатченная OpenBSD, чуть переделанная OpenJava, а также расширения для отражения атак типа use after free и подобных).

– Есть ли у вас высшее образование в области ИТ?

– Институтов я не кончал. Я сделал свой выбор и бросил вуз сразу после поступления. До сих пор не знаю, что я упустил, и как сложилась бы моя жизнь, поступи я иначе. История не знает сослагательного наклонения.

– Ваш случай не единичен, самообразование становится очевидным трендом. Откуда сегодня можно черпать качественную информацию?

– К примеру, на YouTube можно найти множество видеозаписей лекций по computer science от специалистов из самых разных мировых вузов. По части информатики с большим отрывом лидирует арабский мир, причем, что показательно, лекции почти всегда на английском. За ними следуют США (с большим отрывом от остальных).

При этом легко видеть, что не все лекторы одинаковы: одни объясняют вещи глубоко и понятно, другие же ущербно и загадочно: у таких можно только вызубрить, сдать и забыть, поскольку пользоваться этим все равно не получится.

Отмечу, что, кроме знаний, институт дает еще и связи, а связи решают все. Потому что после вузов народ разбегается кто куда, а, разбежавшись, тянет к себе своих. Впрочем, это сильно зависит от конкретного вуза и страны.

– В наше время также доступно огромное количество книг...

– ... хороших книг и раньше было немного, и даже сегодня их чуть меньше, чем совсем ничего, а классика так и остается классикой. Например, в семидесятых была одна Книга Дракона, а сейчас доступны десятки качественных вариаций на тему, но в них от 70 до 90% – это пересечения и повторения, а потому первую книгу читаем вдумчиво, остальные бегло пролистываем в поисках различий.

– Насколько я могу судить, молодое поколение не очень-то много читает, судя по всему, потерявшись в этом информационном изобилии.

– Согласен. Но сейчас по крайней мере есть документация. Есть SDK и куча примеров. А вот в свое время, чтобы заставить CD-ROM проигрывать диски, мне пришлось дизассемблировать пару программ-плееров, реконструируя протокол, причем так приходилось делать не только мне одному. Информацию собирали буквально по крупицам. Ассемблер x86 я изучал в досовском debug.com путем анализа воздействия команды из реальной программы на флаги, память и регистры процессора.

Но у моих предшественников и этого не было. Пионеры информатики не могли почерпнуть знания в книгах, поскольку эти книги им еще предстояло написать. По сути, с тех пор ничего не изменилось, просто линия фронта стала другой.

Да, сейчас можно набрать в Гугле вопрос, как развернуть список на Java/.NET/C, и получить готовый код для «копи-пасты». Зачастую даже несильно кривой и рабочий. Но если спросить Гугл, как написать Гугл, то ничего полезного он все равно не скажет, т.к. непрерывно совершенствуется, а над проблемой поиска бьются лучшие умы человечества. Лет через n-цать об этом будет можно прочитать также свободно, как сейчас мы читаем принципы построения компиляторов в Книге Дракона, в результате чего появляется огромное множество новых языков и технологий, которые не только создаются, но и выживают в конкуренции.

Компьютеры сегодня — это когда на месте срубленной головы Лернейской гидры вырастают две новые

– Нас читают молодые начинающие айтишники, которые делают первые шаги в ИТ. Какие бы советы вы им дали?

– А давайте вы пойдете по грибы, а я буду давать советы, куда конкретно вам ходить, основываясь на собственном опыте? Ничего, что мы разнесены в пространстве и времени и что моей тропой ходить бессмысленно – именно потому, что я ей уже ходил и собрал все грибы? Это, конечно, абстрактный пример, но его легко превратить в конкретный. Когда компьютеры были большими, а вирусы простыми, я только-только начинал интересоваться этой темой. Вирусы росли, хакерские технологии усложнялись, но ведь и я не стоял на месте.

К тому же хакеры двигались поступательно, из пункта А в пункт Б. Шаг за шагом. Сейчас же зловреды усложнились настолько, что человеку с улицы очень трудно войти в эту область, и со своими 15-20 годами практического опыта я получаю огромное преимущество перед молодым поколением. Поэтому если изначально выбрать одно из молодых направлений ИТ-индустрии, то лет через пять можно начинать получать конкурентное преимущество. Конечно, при условии, что это направление окажется востребованным.

Что же касается успеха и карьеры – для взлета необходимо оказаться в нужном месте в нужное время. Ни знания, ни способности сами по себе этого не обеспечивают. Выражение «если ты такой умный, то почему не богатый» слышали? Оно хоть и едкое, но меткое. Умный не означает успешный, хотя успешный – это скорее умный, чем нет.

– Что лично вас восхищает в современных программировании и ИТ, что заставляет двигаться вперед?

– И вырубает, и восхищает одновременно то, что компьютер как средство решения проблем сам по себе стал одной большой проблемой, и все попытки решения этих проблем лишь порождают новые. Это как на месте срубленной головы Лернейской гидры вырастают две новые. BOF