
ДМИТРИЙ
АРТИМОВИЧ
Я - ХАКЕР!
ХРОНИКА ПОТЕРЯННОГО
ПОКОЛЕНИЯ
18+

Дмитрий Александрович. Артимович

Я – хакер! Хроника потерянного поколения

Серия «Звезда YouTube»

http://www.litres.ru/pages/biblio_book/?art=67834608
Я – хакер! Хроника потерянного поколения: Издательство АСТ; Москва; 2022
ISBN 978-5-17-145941-3

Аннотация

Дмитрий Артимович – русский хакер, профессионал в области платежных систем и программирования, автор книги «Электронные платежи в интернете».

Он вышел из тени, когда в 2010 году на всю страну прогремел скандал: кто-то парализовал работу «Аэрофлота», совершив DDoS-атаку на компанию, отвечавшую за проведение транзакций внутри. На то, чтобы реанимировать ситуацию, у специалистов ушло больше недели. Так о Дмитрии Артимовиче узнал весь мир.

Сразу активизировались российские и зарубежные журналисты. Все вновь заговорили о страшных и бескомпромиссных русских хакерах: действительно ли они способны влиять на все, начиная от мировых банков и заканчивая выборами президента США?

Кто же они на самом деле, правдивы ли слухи о них, связаны ли хакеры с государством и как вообще становятся взломщикам?

В своей книге Д. Артимович подробно и обескураживающе отвечает на эти вопросы.

В формате PDF A4 сохранен издательский макет.

Содержание

Вступление	6
Средняя школа	10
Гимназия	30
Конец ознакомительного фрагмента.	58

Дмитрий Артимович
Я – хакер! Хроника потерянного поколения

* * *

Вступление

Я сижу в душном классе и пишу вступительный диктант по русскому языку в местную гимназию. Очень нервничаю, ведь, по словам родителей, в эту школу меня должны были взять без каких-либо экзаменов, потому что сюда перешел работать учителем мой отец. А с гуманитарными предметами у меня всегда было плохо. Русский я еле-еле вытягивал на четверку.

До этого шесть классов я отучился в сельской школе, где также работал мой отец. Время тогда было неспокойное, перестройка: то в соседнем доме кого-то топором зарубят, то на тропинке к автобусной остановке кого-то ножом пырнут. Мать боялась отпускать меня одного в школу, находившуюся далеко от дома. Чтобы вовремя добраться до нее, мне приходилось вставать в 6:30 утра. Я быстро завтракал, умывался. Но спать хотелось ужасно, и если удавалось сделать свои утренние дела быстро, то можно было с огромным удовольствием прикорнуть на диване ещё минут на 15.

Тогда от нашего дома автобусы не ходили. Поэтому нужно было идти примерно километр до остановки на трассу. Потом минут двадцать на автобусе ехать до Кингисеппа, а затем – пешком два километра через лес. Каждый день один и тот же маршрут – остановка, гаражи, речка, мостик, лес.

«Такого дурака взяли», – сказала моя будущая учительни-

ца по русскому языку и литературе. Вступительный диктант я завалил. Но в школу меня все-таки приняли.

У меня никогда не было особой любви к литературе. По крайней мере к той, что заставляли читать в школе. Мне кажется, что детей грузят огромным количеством книг, которые при всем желании не успеешь прочитать. Никто не спрашивает, нравится тебе или нет. Ты должен! Так и формируется отвращение к чтению и письму. Тогда я и подумать не мог, что сам буду писать книги. Вы читаете уже вторую.

Я начал писать эту книгу еще год назад, но забросил. Твердое намерение дописать ее именно в первоначальной задумке у меня родилось, когда я получил предложение от издательства АСТ опубликовать текст про хакеров.

Мировые СМИ очень часто пишут о русских хакерах так: взломали Canon, парализовали американский бензинопровод, а то и просто устроили апокалипсис. И так же часто русских хакеров связывают с нашим правительством. Якобы имея покровительство, они могут безнаказанно нарушать закон во многих других странах. А Голливуд показывает хакеров как неких всемогущих супергероев, катающихся на дорогих авто и живущих в элитных пентхаусах. Только реальность другая. И я покажу ее на своем примере в этой книге.

В 2016 году газета The New York Times сделала меня одним из самых известных русских хакеров. Я попал в центр мировых событий по обвинению России во вмешательстве в американские выборы 2016 года. Только на самом деле я

не получил ни одного предложения о работе – не то что от правительства, а даже от какой-нибудь компании по кибербезопасности. Более того, в 2016 году я был сильно озабочен тем, где найти деньги, чтобы платить за свою убогую съемную однушку на окраине Москвы.

Так кто же они, эти загадочные русские хакеры?

Я из поколения, родившегося во времена перестройки. Получил хорошее физико-математическое образование, которое оказалось никому не нужным в нашей стране. Рос в семье учителей, уважаемых некогда людей, но вынужденных сейчас жить бесправной жизнью низкооплачиваемых рабочих.

В моем детстве все было в дефиците – техника, еда, игрушки. Компьютер, купленный родителями на последние деньги, стал возможностью убежать от реального мира пожелтевших обоев и разваливающейся мебели в мир виртуальный. Там не было границ, и казалось, что все возможно.

В университете я видел, в каких тяжелых условиях живут студенты и наши преподаватели. Родители мне вдалбливали, чтобы я учился хорошо и получил хорошую работу. Я хорошо учился, но видел, что реальность не такая. Я был не нужен здесь и уж тем более своему правительству. Большая часть моих однокурсников уехала из страны. Я очень любил физику в школе, но мой взор все больше устремлялся в сторону программирования. За него платили деньги, хоть и небольшие.

К сожалению, у нас нет своей Силиконовой долины. В основном Россию используют как периферию, с целью разработки программного обеспечения для западного рынка. Каким бы хорошим программистом ты ни был, очень быстро ты достигнешь своего потолка. Что и произошло со мной.

Я – потерянное поколение.

Средняя школа

ZX Spectrum

В детстве я мечтал стать инженером – собирать различные механизмы, схемы. Я зачитывался книжкой «Электроника шаг за шагом» Рудольфа Свореня и пытался понять, как работают транзисторы, логические схемы, радио, кинескопы. В другой книге по физике я читал про устройство лазеров и турбин самолетов.

Дома, еще в детсадовском возрасте, я любил играть с электрическими конструкторами, протягивал провода от радиорозетки к динамику в своей комнате. Позже, в начальной школе, я приделал фару на свой велосипед – когда велосипед ехал, фара работала от динамки[1], когда стоял – от блока батареек. При этом переключение с батареек на динамку происходило через самодельное реле, сделанное из старого трансформатора.

Мой дед был первоклассным мотористом, а в свободное от работы время очень любил перебирать на даче движок

[1] Динамо-машина бутылочного вида, работает на боковой части передней шины велосипеда. Выполнена в виде небольшого генератора электрической энергии, служит для работы заднего фонаря и передней фары велосипеда, а также – для зарядки электронных мобильных устройств.

своего старенького» «ИЖ Юпитер-3». Мы, маленькие, играли рядом и помогали ковырять этого двухцилиндрового зверя.

Karolis Kavolelis / Shutterstock.com

Я хорошо помню некоторые моменты. Например, как дед делал прокладку между двумя половинами двигателя: положив картонку на алюминиевый корпус, он обстукивал ее молотком, пока лишний картон не отваливался. Двигатель же был двухтактным. Вместе с бензином дед заливал в бак еще

и моторное масло. Система смазки в этом мотоцикле была устроена таким образом, что в картере масло используется исключительно для смазывания шестерен коробки переключения передач, а вот коленвал и поршневая группа смазывались за счет масла из топлива. Заводился мотоцикл с таким рёвом, что я от страха всегда прятался в нашем старом домике.

Сколько бы дед ни перебирал двигатель своего мотоцикла, каждый год была одна и та же история – нет тяги то в одном цилиндре, то в другом. Видимо, тогда у меня и появилась эта любовь к механизмам. Очень хотелось понять, что приводит в движение поршень, как же переключаются скорости, как двигаются шестеренки в коробке передач и многое другое.

Помню, в начальных классах я даже всерьез задумывался, а не сделать ли вечный двигатель. Детское воображение рисовало множество вариантов, и я сильно недоумевал, почему никто еще не догадался, как это сделать? Но и у меня не получилось.

И вот, когда я был где-то во втором-третьем классе, родители принесли домой мой первый компьютер – ZX Spectrum. Выглядел он как небольшая черная коробочка с клавишами. Оказалось, эта коробочка подключалась в антенное гнездо телевизора через специальный переходник – модулятор, который формировал аналоговый сигнал из цифрового.

seeshooteatrepeat / Shutterstock.com

Но самое потрясающее для меня было то, что на нем можно было играть в игры. И эти игры были куда увлекательнее, чем старые советские электронные «Ну, погоди», где нужно собирать в корзинку падающие куриные яйца.

Мои родители после развала Советского Союза практически остались без денег. Пришлось распродавать нашу библиотеку. Денег еле-еле хватало на еду и какую-то одежду. Игрушки были в дефиците. Гулять со сверстниками мать меня не пускала, постоянно повторяя, что я маленький, и меня кто-нибудь побьет. Время тогда было неспокойное – «лихие» 90-е. Ее страх я могу понять. Но этот запрет наложил огромный отпечаток на всей моей жизни – я рос застенчивым и необщительным.

Мать много работала, отдавая все силы, чтобы добыть лишнюю копейку. Отцу пришлось устроиться на вторую работу. На выходных он брал меня с собой в местную школу, где подрабатывал электриком.

Летом, во время каникул, меня либо таскали на дачу – сажать картошку, поливать огурцы и помидоры, либо возили с собой в лес за грибами, чтобы не оставлять нас вдвоем с братом, а то мы «подеремся». Грибы родители собирали чуть ли не в промышленных масштабах, а потом сдавали за деньги.

За грибами меня поднимали в 4:30 утра и по любой погоде тащили на корм комарам и слепням – и в тепло, и в холод, и в дождь. Сначала мы ездили в лес на том самом дедовом мотоцикле. Меня сажали в почти прогнившую коляску, что нередко вызывало отвращение. Только меня не спрашивали, хочу я этого или нет. Целый день мы кормили кровососущих, а под вечер я сильно уставал и, как любой ребенок, начинал капризничать. Но на этом мои мучения не заканчивались – родители стелили покрывало на земле, и мы садились перебирать грибы. Тогда начиналось самое ужасное – в движении комары кусали меньше, чем когда сидишь. Хотя были и приятные моменты – все-таки природа и глухой лес. На даче я мог сесть на велосипед и поехать туда, куда меня не пускали, но где была свобода.

За всей этой мешаниной родители сильно уставали. Днями мы с братом просили отвести нас искупаться на речку или сходить на рыбалку, но они всегда говорили – то нет време-

ни, то погода плохая и вода холодная.

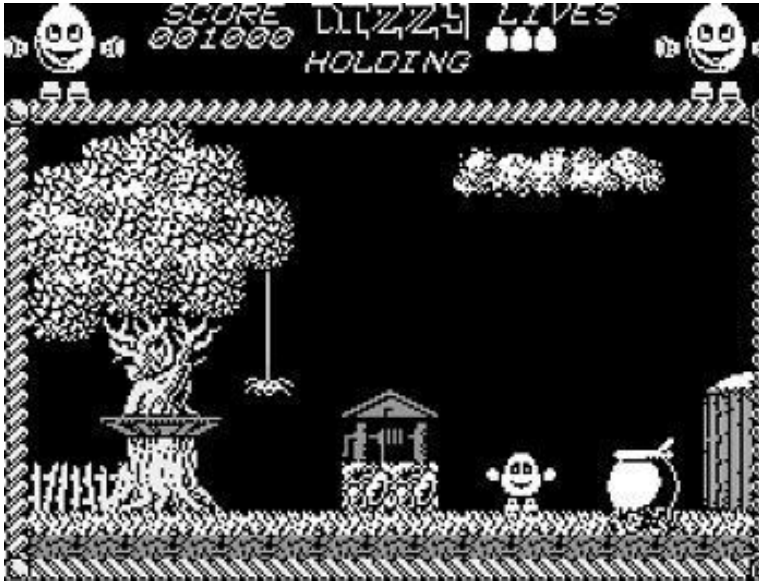
Наверное поэтому ZX Spectrum и захватил полностью мое внимание. Находясь дома, взаперти, я наконец-то мог играть, пусть и с компьютером.

Для того, чтобы загрузить игру, к ZX Spectrum нужно было подключить магнитофон, вставить кассету и ждать минут пять, слушая мелодичное трещание в динамике. Благо родители откуда-то принесли два советских магнитофона «Квазар М».

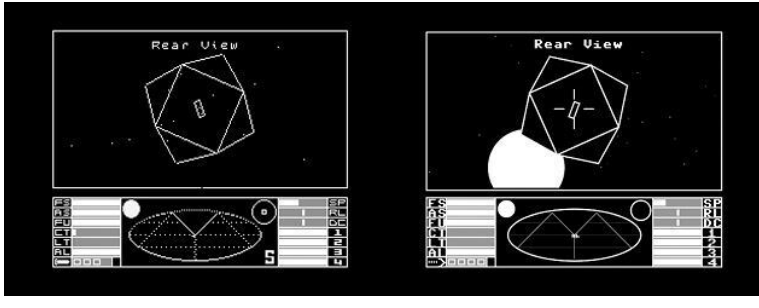
В модели ZX Spectrum 48K был встроен интерпретатор BASIC – простенького языка программирования, адаптированного под этот ПК. Причем команды не нужно было набирать полностью – они выскакивали сами при нажатии на клавиши.

Для загрузки программы использовался Load. Помню, как я сидел на шершавом ковре в комнате родителей перед старым советским телевизором «Горизонт» и увлеченно загружал свои первые игры – Exolon, Elite, Dizzy. Телевизоры тогда были огромными ящиками, ламповыми, а вместо кристаллов – кинескоп.

Exolon, разработчик Raffaele Cecco, издатель Hewson Consultants, 1987



Dizzy, разработчик The Oliver Twins Big Red Software, издатель Codemasters, 1987



Elite, разработчики Дэвид Брэбен и Ян Белл, издатель Acornsoft, Firebird, 1984

Моей любимой игрой для Spectrum была Elite. Игра, написанная еще в 1985 году, завоевала множество поклонников по всему миру. Графика была достаточно примитивной по нынешним меркам – у объектов отображались только грани.

В огромной Вселенной вы управляете космическим кораблем, летаете по Галактике от станции к станции и перевозите товары. Вступаете в схватки с вражескими кораблями или убегаете от погони. Потихоньку докупаете прибамбасы для корабля – щиты, лазеры, стыковочный компьютер.

Стыковочный компьютер – вещь очень нужная. Поскольку все станции вращаются, приходилось очень точно целиться в посадочную шахту и начинать осевое вращение корабля. Пристыковаться была еще та задача – на «попотеть».

Если хотелось заработать быстрее, можно было возить запрещенный товар – рабов, наркотики. Конечно, понижался рейтинг, и на вас могли устроить облаву. Но можно было с помощью гиперпривода улететь в следующую галактику, а там рейтинг законопослушности снова обнулялся.

Сейчас подобная графика выглядит очень примитивной. Даже современный дешевый китайский смартфон тянет куда более реалистичные игры. На тот момент для восьмибитного процессора Z80, работающего на частоте 3,5 МГц, контурная трехмерная графика была пределом. Сам по себе процессор Z80 – очень удачная модель. Например, в его состав входило два набора регистров, между которыми можно было

быстро переключаться. Что-то мне подсказывает, что компания Intel с него подсмотрела свой HT (Hyper Threading). Смысл технологии HT – это быстрое переключение между наборами регистров без их сохранения в медленной оперативной памяти.

Для Spectrum было написано множество игр. Очень многие из них переводились на русский язык. Кстати, игры писали тогда на чистом ассемблере, поскольку малый размер оперативной памяти не позволял использовать что-то другое.

За короткое время ZX Spectrum покорил мир. Секрет успеха был достаточно прост – цена. Блок без монитора, внешнего дисковода и клавиатуры стоил достаточно дешево.

А вы знали, что с ZX Spectrum началась эра персональных компьютеров?

В июле 1979-го Клайв Синклер учреждает компанию Sinclair Research Ltd. Отсюда и начинается история нашего ZX Spectrum. Первый продукт Sinclair ZX80 произведен в феврале 1980 года, это был первый компьютер в мире стоимостью ниже £100. Его размеры были 218×170×50 мм и весил он 340 грамм. ZX80 нельзя было назвать очень удачным, тем не менее он начал довольно хорошо продаваться.

На волне успеха Sinclair Research выпускает свой самый популярный компьютер. Происходит это в 1982 году. ZX

Spectrum 48K имел постоянные запоминающие устройства (ПЗУ) с памятью 16 КБ, в которые был прошит диалект языка BASIC, так называемый Sinclair BASIC. Эта же программа ПЗУ обеспечивала базовый ввод-вывод и пользовательский интерфейс. С выпуском ZX Spectrum были огромные проблемы. На компанию Синклера посыпалось огромное количество заказов – до 40 000. Реальная возможность была производить лишь 5000 компьютеров ZX Spectrum в месяц.

На выпуске модели ZX Spectrum 128K и заканчивается история Sinclair Research. Заканчивается довольно неожиданно. В 1982–1983-х годах прибыль компании Клайва Синклера составила £13,5 млн, при этом ему принадлежало 85 % акций компании. Однако в 1983–1985-х годах амбициозный сэр, уверенный в своей гениальности, спонсировал разнообразные проекты, такие как электромобиль, плоский телевизор и новая модель компьютера (Sinclair QL). Конструкцию автомобиля он доверил компании, которая специализировалась на сборке стиральных машин. Автомобили никто не купил. С плоским телевизором тоже ничего не вышло. Новый компьютер отставал по качеству, по мощности и по цене от своих конкурентов. В 1985-м, чтобы избежать банкротства, Клайв уговорил торговую марку Dixons заключить сделку на £10 млн. Однако 7 апреля 1986 года сэр Клайв Синклер неожиданно уходит из компьютерной индустрии. При продаже компании Клайв получает £5 млн наличными.

У нас в России было очень мало оригинальных ZX Spectrum, в основном клоны. Очень много кооперативов по разным городам паяли такое чудо, ничуть не уступающее оригиналу. А вот с джойстиками всегда была проблема – они быстро ломались.

BASIC

В сельской школе, в которой я учился до 7-го класса, даже был компьютерный кружок, который, кстати, должен был

вести мой отец, работавший там. Но вел я. А сводилось все к тому, что мы с друзьями просто сидели перед двумя огромными ламповыми телевизорами и играли на двух компьютерах Spectrum. У меня все-таки были друзья. Чем больше запрещаешь что-то ребенку, тем больше он будет хотеть это сделать. В школу я ходил вместе с отцом за руку. Мало ли, что могло с ребенком произойти по дороге, считала мать. Пока я дожидался отца после уроков, у меня часто бывало один-два свободных часа, когда я мог свободно бегать с друзьями вокруг школы. Мы играли в «квадрат» на улице, собирали березовый сок в лесу, залезали на спор кто выше, на полуразрушенную трубу старой котельной, взрывали самодельные петарды. Петарды мы делали из магния, смешанного с марганцовкой, а в качестве фителя использовали скрученную из бумаги трубочку с серой от спичек.

Потом у нас в России появились приставки, такие как Sega и Dendy. Мой Spectrum куда-то дели, возможно, отдали в тот самый кружок.

Родители купили Dendy. Она также подключалась к телевизору, но, в отличие от Spectrum, игры к ней шли на картриджах. Решение – гениальное! Игра записывалась в ПЗУ, которое просто подключалось к приставке. Тем самым разработчики усложнили жизнь пиратам, ведь копировать картриджи – куда сложнее и затратнее, чем копировать кассеты или диски. Хотя пиратов это тоже не остановило!

Viiviien / Shutterstock.com

Самая известная игра для Dendy – «танчики». В нее мы играли вдвоем с отцом, так же сидя перед большим телевизором на шершавом ковре.

Но вернемся к Spectrum. Вместе с компьютером родители купили книгу «Как написать игру». Это была моя первая книга по программированию. Описывала она программирование на несложном языке BASIC. Простенькие циклы,

условия, работа с графикой.

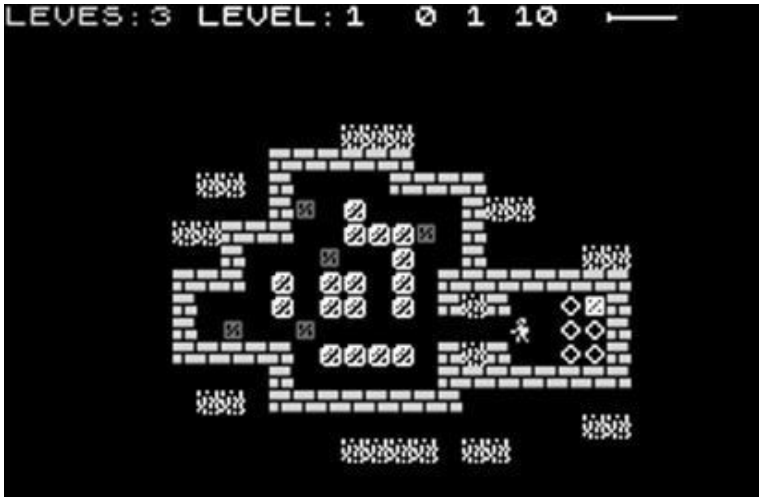
Единственным штатным видеорежимом оригинального ZX Spectrum является графический режим разрешением 256×192 точки. Доступна только одна видеостраница, расположенная в основной памяти компьютера по фиксированному адресу. Информация о цвете задается атрибутами – по одному байту атрибутов на знакоместо 8×8 пикселей, то есть цвет был четырехбитным, всего было восемь значений цвета. Весь экран делился на 32×24 знако-места, для которых можно было задать только два цвета: фона и точки. В одном знако-месте не могло быть три пикселя с разными цветами. В общем, некоторые особенности помогали максимально экономить память.

Но, по большей части, я просто перепечатывал готовые строчки кода из книжки. Например, игру Sokoban в несколь-

ких сотнях строк. Смысл ее – поставить ящики на помеченные места. При этом двигать ящик можно только вперед. Если ящик упирался в угол, его уже нельзя было оттащить назад.

Чего-то своего я тогда не сделал. Хотя сильное желание изучить ассемблер у меня возникло. И я его изучил, но значительно позже и под другую архитектуру.

Но рутина продолжалась – школа, уроки. Мать заставляла учиться и говорила, что я должен учиться, чтобы получить хорошую работу. Должен одеваться так и должен есть это… должен… должен… Мать, родившаяся в Советском Союзе, от всего сердца желала своим детям только лучшего. В ее время, получив высшее образование, можно было рассчитывать на престижную работу. Мои родители были людьми системы.



Мне всегда нравился Spectrum. И я был не один такой! По всему миру появились фан-клубы. Энтузиасты подключают сетевые карты, модемы, соединяют старенькие Spectrum в сеть. У меня до этого не дошло.

Классе в 8-м я выменял Speccy[2] у одноклассника, даже не помню уже на что. Этот блок был меньше – без встроенного динамика и модулятора. А это проблема – как подключить Speccy к телевизору? Ведь монитора у меня тогда не было.

Логически поразмыслив, я решил, что модулятор должен быть у Dendy. Ведь Dendy подключался в антенное гнездо телевизора. Значит, была возможность перевести цифровой

[2] Speccy – так сокращенно называют ZX Spectrum его фанаты.

сигнал в аналоговый.

Полный энтузиазма, я раскурочил корпус приставки и методом тыка, или перебора, подсоединяя провода из графического порта Spectrum, я все же смог добиться четкой картинки на экране телевизора! С удовлетворением вырвал плату из корпуса приставки и закрепил свой результат раскаленным паяльником. Сам не знаю как, но оно работало.

К сожалению, к тому времени мать уже не замечала моих маленьких побед. Работа в две смены поглотила ее полностью. И дома все ее время было занято: с утра она собирала нас в школу, днем готовила обед, помогала делать уроки, вечером проверяла тетради. И так повторялось каждый день.

Гимназия

Класс

«Такого дурака» все-таки взяли в Кингисеппскую гимназию в 7-й класс. И с самого начала класс, в который я попал, меня не принял. Там были дети «крутых родителей», и они всячески стали меня задирать. Назвав своих одноклассников дебилами, я полностью с ними разругался. Меня перевели в параллельный класс. Здесь ребята были проще, без понтов. С некоторыми я дружу до сих пор.

Учился я в физико-математическом классе. Как следует из названия, с углубленным изучением физики и математики. Только вот физику у нас в классе понимали единицы, я был в их числе. Директор Симонова требовала, чтобы в образцовой районной школе были медалисты, и медалистов делали – и по физике, и по математике… в физико-математическом классе.

Школу я не любил. Мать заставляла делать уроки, настаивая на то том, что я должен хорошо учиться, иначе меня заберут в армию. Свободного времени было очень мало – воскресенье, да и то неполное. При шестидневной учебной неделе в воскресенье нужно было готовить уроки на поне-

дельник.

Больше всего я ненавидел русский язык и литературу. Грамотностью я никогда не отличался, а по литературе всегда задавали читать очень много. Интересно, когда? Встаешь в 6 утра, едешь в школу, учишься с 9 до 16 часов, едешь домой, возвращаешься к 5–6 часам вечера, ешь, делаешь уроки, ложишься спать. А тут, оказывается, вы должны успеть прочитать три томика «Войны и мира». Нет, спасибо.

Моя мать всю жизнь работала учителем русского языка и литературы. С ее точки зрения, ребенок учителей, а тем более учителя русского языка, просто обязан быть грамотным и писать отличные сочинения по литературе. Поэтому сочинения за меня писала она. Этим она напрочь отбила у меня желание делать это самому и на долгие годы поселила во мне неуверенность при любых начинаниях. А вдруг я не справлюсь, вдруг я не смогу? С ее же слов, я был маленьким и несамостоятельным, кого обязательно побьют на улице. Хорошие вводные для ребенка!

Как оказалось, в моей новой школе изучали два иностранных языка: английский и немецкий. Какой в этом смысл? Я не понимаю до сих пор. При этом мои одноклассники уже учили немецкий два года, а я не знал ни слова. За лето я несколько раз садился за учебник со словарем, но далеко мои познания в немецком не продвинулись.

В гимназии было два преподавателя по немецкому, обе женщины. Как оказалось, учительница постарше на уроках

любила рассказать про свою жизнь, а занятиям отводила очень мало времени. К ней-то мне и посоветовали идти мои новые одноклассники. Что сказать, школьную программу по немецкому языку я так и не выучил. Кстати, домашние задания и по немецкому языку за меня также делала мать.

А вот с точными науками дело обстояло иначе. Мне достаточно легко давались математика, физика и химия. При этом у меня никогда не спрашивали домашнее задание у доски, поэтому я, в общем-то, обходился прочтением очередного урока в учебнике, без зубрежки.

Сейчас я считаю, что школьная программа, построенная по принципу, что ты должен знать все предметы, – неправильная. Талантливые во всем люди встречаются редко. В детях нужно развивать то, что им самим нравится и что у них лучше получается. А загрузка детей лишними предметами, которые никогда не пригодятся в жизни, не оставляет у них времени на увлечения.

А вот что касается родителей. Родители должны укреплять в детях уверенность в своих силах, подчеркивать даже небольшие их победы. Честно, я не помню, за что меня хвалили родители. За учебу? Хорошие оценки воспринимались как данность, за плохие меня ругали.

Как-то я забыл сдать тетрадь с диктантом по русскому языку. Просто положил в портфель и пошел домой. Дома, разбирая учебники, я достал ту самую тетрадь. Какой же скандал устроила моя мать, переживая, что о ней теперь по-

думают! Как я мог не сдать тетрадь! А я мог так сделать, я же был ребенком. Но тогда я очень испугался. Позже брат мне сказал: «Надо было просто кинуть тетрадь в парту на следующий день».

Несколько раз я просил отца сделать что-то вместе. Например, собрать машину с двигателем от мотороллера по чертежам из журнала «Моделист-конструктор». Но, опять же, – у него то не было времени, то денег, то чего-то еще. Хотя уже в старших классах мы нашли общие увлечения – охоту и рыбалку.

Зато я очень хорошо помню один яркий эпизод из детства. Родители уехали в лес за грибами и оставили меня одного дома. Когда они вернулись, сломанные механические часы на стене вдруг решили пойти. Мать сказала:

– Какой молодец, починил часы!

– Я не трогал их. Они сами.

Мне не поверили. Дело дошло до скандала.

– Я их не трогал! Я их не трогал! – повторял я.

Logo

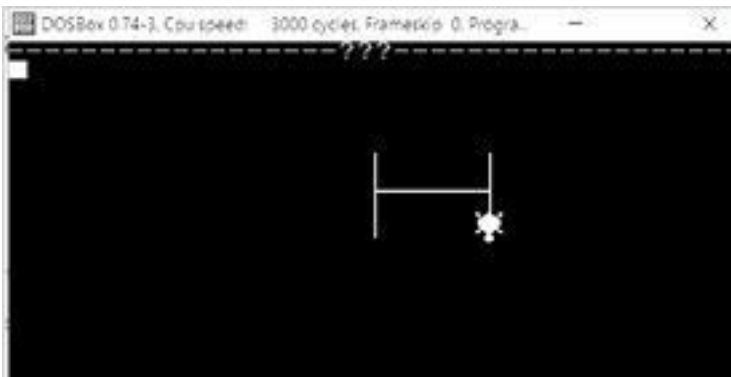
В этой гимназии у нас был компьютерный класс. Там стояли старенькие 286-е процессоры с MS-DOS и Norton Commander. Поскольку я пришел в эту школу сразу в 7-й класс, то абсолютно не знал, как всем этим пользоваться. Помню, во взглядах одноклассников читался вопрос, не ду-

рак ли я, когда в первый раз на уроке я сел за IBM PC и спросил, как им пользоваться. Все мои познания в Spectrum тут не годились, я был полным ламером[3].

Программирование мы начали изучать с забавного языка Logo. Суть этого языка – давать команды Черепашке: поверни налево, пройди вперед. А она чертит линию. Тут у меня и проявились способности – я мог заставить Черепашку начертить все что угодно. Мой первый и самый толковый преподаватель информатики по прозвищу Борода[4] сказал, что у ребенка есть способности.

[3] Ла́мер (от англ. lame «увечный, хромой») – на компьютерном сленге так называют человека, плохо умеющего обращаться с компьютером, неспособного или принципиально не желающего хорошо освоить работу на компьютере.

[4] Борода – так мы с одноклассниками называли учителя информатики, потому что тогда еще не каждый второй выглядел лесорубом, и густая растительность на лице была скорее исключением, чем нормой.



Позже нашей школе подарили второй компьютерный класс – несколько машин IBM PC на базе процессора Intel Pentium. Там была установлена Windows 95! Я впервые увидел окна и графический интерфейс. Потом я узнал, что в старом классе была Windows 3.11, которую мы ни разу не запускали.

Более того, компьютеры были включены в локальную сеть! Это было что-то, мы с друзьями играли в «Червы»[5]

[5] «Червы» – популярная карточная игра для четырех игроков, главной задачей в которой является набрать наименьшее количество очков. Каждая игра состоит из нескольких раундов, и количество очков, полученных игроком в раунде, определяется количеством черв во взятках, собранных данным игроком. Для игры используется обычная колода из 52 карт.

вчетвером.

Черепашка плавно перешла в Pascal. Дома я тут же прочитал книгу про программирование на Pascal'е. Скажу честно, Pascal мне не нравится, но задачки в школе мы решали на нем.

В то время мне очень нравилось читать книги типа «Самоучитель Windows 95», «Pascal» – хотя бы в книге ты мог прикоснуться к этим новым, захватывающим технологиям.

Мой интерес к программированию рос, и родители решили, что детям нужен компьютер. Поскольку денег тогда не было совсем, мы продали дачу, на которой я летом поливал огурцы и помидоры.

IBM PC

На вырученные от продажи дачи $700 мой старший брат и мать отправились в Санкт-Петербург за компьютером. На тот момент в продаже уже было следующее поколение процессоров Intel Pentium II. Но денег на полноценный второй «пень» не хватило, поэтому пришлось взять Celeron 266. Видеокарта была ATI Rage 4 Pro. Примечательна она тем, что поддерживала Direct 3D, но не поддерживала OpenGL. А Quake, о котором я напишу позже, работал как раз на OpenGL. Тогда я уже перешел в 9-й класс.

Через какое-то время слабомощную ATI-шку мы все-таки заменили на NVIDIA Riva TNT2 Vanta-16. И опять это была

обрезанная версия полноценного на тот момент ускорителя Riva TNT2. Что было, то было. Кое-как играть можно было и на Vanta.

Тогда для увеличения мощности многие любили разгонять и процессоры, и видеокарты. Так сделали и мы с братом – увеличили частоты процессора с 266 до 333 МГц. Мате-

ринская плата на нашем ПК была простенькая, но позволяла увеличить частоту шины. Вместе с частотой шины разгонялся и CPU, и оперативная память.

Видеокарту я разогнал тоже, для этого уже использовался специальный софт. Но была проблема – видеокарта сильно грелась. На GPU стоял обычный алюминиевый радиатор без вентилятора. Решение напрашивалось само собой. Отломав штатный радиатор, я приклеил обычным суперклеем на графическое ядро кулер от процессора и воткнул его в свободный разъем для кулера на материнской плате.

В общем, решение работало. Правда, один раз кулер все-таки отвалился и пришлось клеить его снова.

Итак, на моем первом IBM PC стояла MS-DOS. Поэтому мы с братом решили установить Windows 95. Вы знаете, что Windows 95 реализовывала многозадачность не полностью? Любой процесс мог единолично захватить процессор и делать что угодно, например, подвесить машину. А еще были такие программы, как Nuke, которые эксплуатировали сетевые уязвимости Windows 95 и позволяли подвешивать машины удаленно.

Конечно же мы сразу установили игры: Age of Empires, Doom. Позже – Blood и Quake.

За игрой в Age of Empires я провел много часов. Было увлекательно отстраивать империю, создавать армию, воевать с соседями.

Age of Empires, разработчик Ensemble Studios, издатель Xbox Game Studios, 1997

Мне все больше и больше нравились компьютерные игры. Моей мечтой стало их писать.

Компьютер захватил меня полностью. Для меня эта была новая вселенная, в которой ничего не понимали мои родители. Здесь не было «ты должен», здесь меня никто не ограничивал. Здесь я мог играть или писать программы сам. К этому времени у меня уже окончательно пропало желание показывать что-то маме и папе, чтобы те мной гордились.

Почта для хакеров

Интернета у нас тогда не было. Сети между домами еще не появились. Основным способом связи были модемы, работающие по наземным телефонным линиям. Скорость в таких «игрушках» достигала максимум 56 Кбит, что равноценно скачиванию файла со скоростью 7 КБ в секунду. Как раз через такие модемы мы и играли в Age of Empires, Blood, Quake.

Через знакомых у нас появилась электронная почта. Работала она совсем не так, как почтовый клиент у вас на смартфоне.

Специальная программа MiniHost дозванивалась до сервера, по протоколу UUCP (UNIX-to-UNIX Copy Protocol) отправляла и забирала письма, после чего вешала трубку, чтобы не занимать линию.

Сервер размещался на некогда советском заводе «Фосфорит», удачно приватизированном, разворованном и названном «ЕвроХим».

У нас была общая конференция между всеми пользователями почты.

Мы с братом нашли почтовые службы для размещения файлов по всему миру. Вы отсылаете запрос по определенному почтовому адресу на список файлов, а потом – запрос на скачивание какого-то файла. Учитывая, что весь софт продавался на компакт-дисках, а денег катастрофически не хватало, – это было неплохой альтернативой. Правда, скачивание больших файлов требовало много времени, что вызывало негатив других пользователей, – телефонная линия все это время была занята.

А вот с безопасностью на почтовом сервере было совсем плохо. Пароли представляли собой просто номера телефонов владельцев. Дома у нас лежал телефонный справочник города. Например, ящик crb принадлежал Центральной рай-

онной больнице. В общем, я взял себе про запас три ящика.

Позже стало понятно, что это было правильным решением. Будучи молодым и горячим, я поссорился с одним из пользователей общей конференции, и мой почтовый ящик заблокировали. Я имел три резервных, и мне было абсолютно наплевать.

При этом люди, администрировавшие почту, решили, что хорошо было бы поменять пароли с номеров телефонов на нормальные. Они попросили всех придумать себе новый пароль и скинуть по почте! Я, конечно же, тоже отправил, со всех трех.

Я жаждал расплаты и решил отомстить за блокировку. Для этого нужно было пожертвовать одним из ящиков. Написав простенького трояна на Pascal'е, я разослал его под видом «крутого скринсейвера» на общую конференцию.

Троян должен был стащить файл с паролями от почтового клиента и отправить на мой адрес.

Настройки почтового сервера позволяли подменять отправителя в письме, что я и сделал. К сожалению, человек, от имени которого я разослал это письмо, оказался дома, и всю затею мне испортил.

Электронная доска объявлений: первый взлом

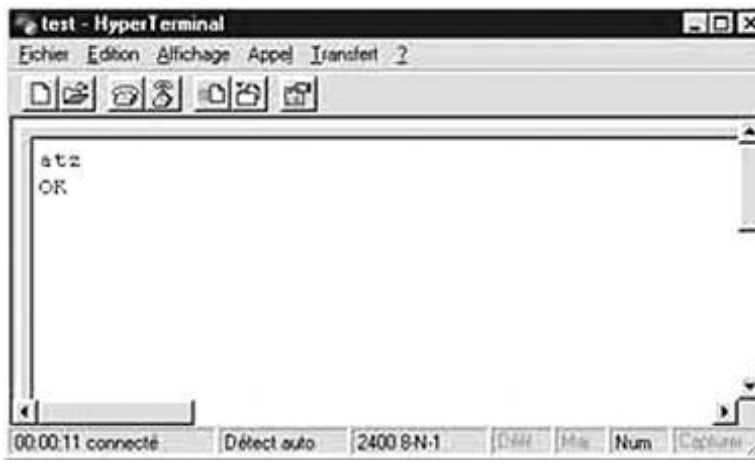
Кроме электронной почты, у нас в городе работала BBS (Bulletin Board System). Это электронная доска объявлений,

проще говоря, система, которая использовалась для общения пользователей по телефонным линиям – через модем.

У нашей BBS телефонная линия была одноканальная, то есть общаться можно было только с оператором системы, сисопом[6].

Подключались к BBS с помощью так называемого модемного терминала. Это текстовое окно, похожее на Telnet. Вы отправляете команду напрямую модему, например, ATDP 8945444333 – набрать в импульсном режиме номер 8945444333 (Dial Pulse). После соединения на экране появлялось приветствие в виде разноцветного текста.

[6] Сисоп – системный оператор.



Там можно было поболтать, залить или, наоборот, скачать файлы. У этой BBS-ки был режим командной строки – практически тот же MS-DOS. Вы могли ходить по каталогам, где лежали файлы для скачивания. Еще там была та же досовская команда «type»[7]. А вот команда «cd C:», смена диска на C:, от непривилегированного пользователя, естественно, вызывала ошибку «недостаточно прав».

Разговорившись с сисопом, я скачал софт, который он использовал, – Tornado BBS.

Запустив Tornado BBS у себя на компьютере, я занялся исследованием. И практически сразу обнаружил две ошибки. Во-первых, при вводе неверного пароля Tornado BBS пи-

[7] type – вывести содержимое файла под MS-DOS.

сал в лог следующее: «Введен пароль X вместо Y», где Y – истинный пароль. Во-вторых, команда type (вывод содержимого файла) не проверяла привилегии пользователя. То есть можно было легко прочитать любой файл на диске C:.

Пазл сложился, вот оно! Достаточно было совершить неудачную попытку входа в BBS от админа, после чего под обычным пользователем вывести лог. Это я и сделал ночью.

Имея пароль админа, я получил доступ ко всему диску компьютера. Но, честно говоря, ничего интересного там не нашлось. И, скачав файл с паролями других пользователей, потерев лог, я, полный удовлетворения, отключился.

Подсоединившись к BBS на следующий день, я зашел в систему под чужим аккаунтом. Решил поболтать с сисопом:

– Привет, как дела? – написал я.

– Да вот, меня вчера похакали.

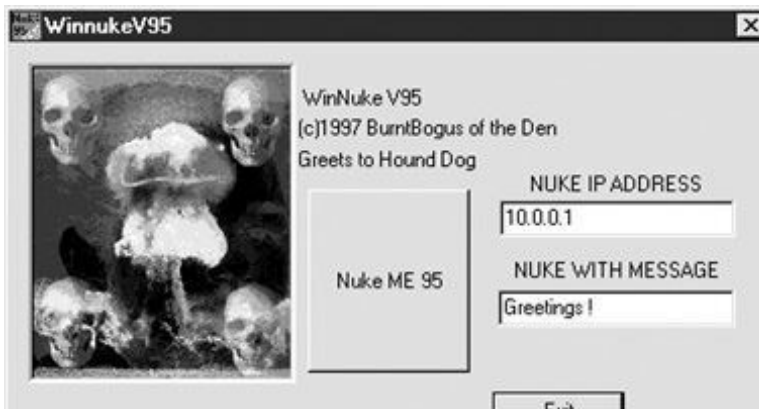
– Неужели? Что-то стащили?

– А вот, ты и попался. С человеком, чей это аккаунт, я говорил час назад по телефону!

– Ладно, раскусил.

В общем, мы подружились. Я рассказал про ошибки. Позже мы частенько играли с ним по модему в Quake World.

На нем же я попробовал Win95 Nuke – и он отлично сработал. Windows просто вылетала в синий экран.



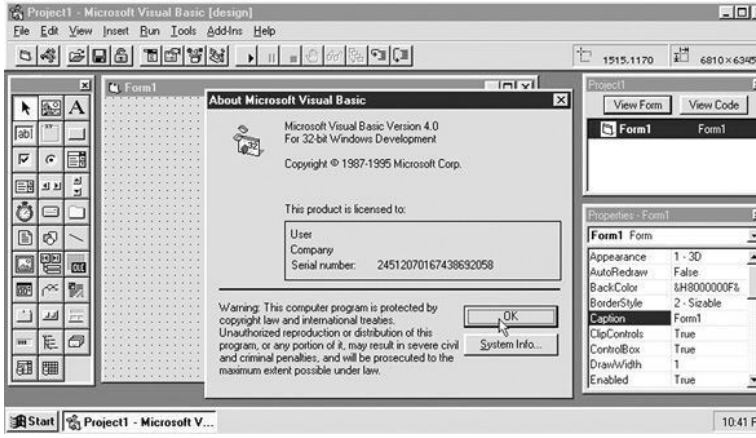
Visual Basic

После Pascal я взялся за язык программирования Visual Basic. Мой брат купил книжку по Visual Basic 6.0. Подкупало тем, что на нём можно было визуально рисовать окна и элементы на них. И очень просто обрабатывать события: щелчки мышкой, ввод с клавиатуры и т. д. Щелкаете по любому элементу, в открывшемся окне выбираете событие, пишете его обработчик.

Позже, как только я перешел на Visual C, я не мог понять, как же тут добавить окно и написать обработчик его событий? Почему он тоже «вижуал», но тут все по-другому.

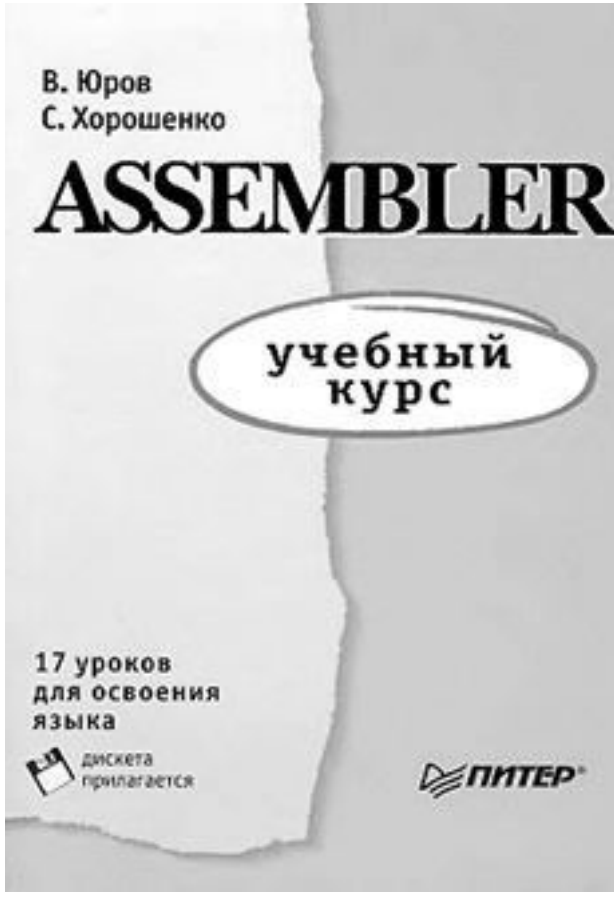
На Visual Basic было легко написать простейший калькулятор, редактор текста. Но для серьезных проектов он не годился – он был медленный и тащил кучу библиотек с собой.

Хороший язык… для детей. Так пришло понимание, что для серьезного программирования нужно что-то еще.



Хакеры выбирают ассемблер и C/C++

Линус Торвальдс написал Linux на C и ассемблере. Выбор был очевиден.



Сначала я осуществил свою детскую мечту и стал изучать ассемблер. Компилятором был выбран TASM (Turbo Assembler). Для тех, кто не знает, ассемблер – язык програм-

мирования низкого уровня. Это система обозначений, используемая для представления в удобочитаемой форме программ, записанных в машинном коде. Другими словами, это самый низкий уровень. Здесь нет стандартных функций «вывести строчку на экране», «получить ввод от пользователя». Все это доступно через вызовы к операционной системе. Например, в MS-DOS, с чего я и начал изучение ассемблера, вызовы к ядру были реализованы через прерывание INT 21H.

Любая ошибка на языке ассемблера может привести к краху всей программы. Поэтому, если вы хотите стать настоящим профи, – вы обязаны понимать, как функционирует CPU, как он обращается к памяти, как он работает с устройствами и многое другое. Этот хороший опыт помог мне потом писать высоконагруженные и производительные системы при минимуме системных требований.

Как раз хорошим дополнением к учебнику по ассемблеру стала книга про архитектуру x86-процессоров. Вы знаете, что Биллу Гейтсу приписывают фразу «640 КБ памяти всем хватит»? Откуда взялось ограничение в 640 КБ памяти, как процессоры, начиная с 286-го, его обходили, как появилась многозадачность и защищенный режим работы процессора, скалярность и суперскалярность? Все это должен знать настоящий профи.

Конечно, на ассемблере сейчас уже не напишешь игру, да и хоть сколько-нибудь сложный проект. Этот язык в основном используется для тех случаев, когда нужно сделать что-то очень небольшое, элегантно, на низком уровне, и обычно в виде вставок в код C/C++.

Уже давно даже новые версии компиляторов языка C пи-

шут на самом C.

Поэтому я принялся изучать язык C и сразу C++ по книгам Герберта Шилдта.

Первое мое более-менее серьезное творение – мини-операционная система. Загрузчик, написанный на ассемблере, записывался на первую дорожку дискеты размером 3,5 дюйма и загружал ядро, написанное на C. Ядро на C переводило процессор в многозадачный 32-битный режим. И на этом, в общем-то, все.

Но это реально круто. Я был горд собой! Даже такая простая вещь требовала хороших знаний системного программирования и архитектуры процессора.

Half-Life

В 1998 году выходит игра Half-Life. Эта игра поменяла очень много в отрасли. В отличие от темного Quake, коридоры и комнаты в Half-Life выглядели светлыми и совсем как настоящие.

Half-Life,разработчик Valve Corporation, издатель Valve Corporation, 1998

Подавляющая часть игр использует технологию Lightmaps.

Lightmap – метод освещения пространства в 3D-приложениях. Он заключается в том, что создается текстура, содержащая информацию об освещенности трехмерных моделей. Метод значительно экономит ресурсы компьютера, поскольку приложению не приходится рассчитывать падение света в режиме реального времени.

Так вот, первые игры, в которых начали считать освещение, подобные Quake, были ужасно темными – рядом с источником света светло, а в тени ничего не видно. Всё потому, что освещение рассчитывалось до первого падения луча на поверхность, без отражения. И мозг постоянно говорил, что здесь как-то нереалистично, что-то здесь не так.

Quake,разработчик id Software, издатель GT Interactive, 1996

А вот Half-Life одним из первых стал рассчитывать Lightmaps, учитывая отраженный свет. То есть тень теперь не была идеально черной, она стала реальной, «живой». Алгоритм расчета отраженного освещения называется Radiosity.

Суть Radiosity состоит в том, что все поверхности сцены разбиваются на небольшие фрагменты – патчи, каждый из которых наделен свойствами излучать, поглощать и от-

ражать свет. Процесс вычисления освещения по алгоритму Radiosity состоит из набора итераций[8], каждая из которых уточняет результат расчета. Для отдельного патча на сцене подсчитывается полученная им от других патчей энергия, а также доля этой энергии, которая будет излучена патчем на следующей итерации.

В результате алгоритм Radiosity позволяет получать реалистичные эффекты вторичных отражений, неточечных источников света, мягких теней и т. д.

Half-LIfe получился настолько удачным, что к нему создали даже несколько модов, некоторые из которых показывали сюжетную линию глазами других персонажей. Один из самых удачных модов для игры по сети – это Counter-Strike.

Несколько лет спустя вышел Half-Life – 2. И опять разработчики из Valve сделали прорыв – они добавили реалистичную физику на движке Havok. Теперь брошенная банка из-под газировки не просто падала и прилипала к полу, а реалистично отскакивала, ящики плавали на воде, а убитые противники эффектно перекатывались по ступенькам лестницы.

---

[8] Итерация в программировании – в широком смысле организация обработки данных, при которой действия повторяются многократно, не приводя при этом к вызовам самих себя (в отличие от рекурсии). В узком смысле – один шаг итерационного, циклического процесса.

Олимпиада

10-й класс. Мы сидим в кабинете физики, ждем начала урока. Заходит Виктор Валентинович, наш учитель: «Ребята, сегодня вы будете решать олимпиадные задачки. Кто наберет больше баллов, тот пойдет выступать за школу в район».

Задачи я решил достаточно быстро. А вот будущие золотые медалисты осадили меня и чуть ли не вырывали тетрадь: «Дай списать! Дай списать!». Внутренний голос завопил: «Это же не контрольная! Это олимпиада!». И тут я во весь голос закричал: «Отстань! Решай сам!». Сработало. Учитель обратил на нас внимание. А я заработал больше всех баллов в школе и в районе. Мне предстояла поездка в Питер на Ленинградскую областную олимпиаду.

В областной центр нас отправили группой на «девятке» – трое детей с 9 по 11-й класс и учитель. Было это зимой. Выезжали мы рано утром. Всю дорогу мело – видимость почти нулевая. Олимпиада проходила два дня – теория и практика. В первый день вечером мы возвращались домой, на следующий опять ехали в Питер. Ко второму дню остался только я и мой учитель физики. Ехать туда было страшно, внутренний голос постоянно нагнетал, что я не справлюсь и что хочу домой к маме. Позже, в следующем году, я ездил туда на олимпиаду и по информатике, и по физике.

Два раза я занимал призовое третье место в Ленинград-

ской области по физике и четвертое место – по программированию. Места по программированию обычно занимали ребята из Выборга. Причем победитель прошлогодней олимпиады приезжал вне конкурсного отбора, поэтому от Выборга было два претендента, так они и спихнули меня на четвертое место.

На следующий день я увидел в холле школы поздравление с призовым местом. Это была моя личная победа. Я вспомнил все те же слова – «такого дурака взяли». А может, и не дурака?

Конец ознакомительного фрагмента.