

image not found or type unknown



Хакер (от англ. hack) - особый тип компьютерных специалистов. Иногда этот термин применяют для обозначения специалистов вообще - в том контексте, что они обладают очень детальными знаниями в каких-либо вопросах, или имеют достаточно нестандартное и конструктивное мышление. С момента появления этого слова в форме компьютерного термина (произошедшего в 1960-е годы), у него появлялись новые, часто достаточно различные, значения.

Кто такие "хакеры"

Когда компьютеры только появились, слово "хакер" было уважительным. Его использовали для обозначения компьютерных гениев, способных переписать часть ядра операционной системы, чтобы она стала лучше работать или "сбросить" всеми забытый администраторский пароль. Хакеров уважали за умение нестандартно мыслить и находить разумные решения самым сложным проблемам. Однако с течением времени оригинальное значение слова было утеряно, поскольку далеко не все "хакеры" ограничивались изменениями ядер ОС и восстановлением паролей по просьбам своих коллег. Некоторые из них начали вторгаться в плохо защищенные компьютерные системы, чтобы "доказать, что это возможно" и, наконец, перешли зыбкую границу взлома с целью кражи какой-либо важной информации или системных ресурсов. Компьютерное сообщество, столкнувшееся с размыванием значения термина "хакер", ввело в обиход несколько дополнительных терминов, например, "script kiddie" и "cracker". Термин "script kiddie" используется для обозначения людей, не обладающих существенными познаниями в области хакерства и просто использующих для взлома чужие хакерские утилиты - скрипты, эксплойты и т. п. Термин "cracker" обозначает человека, находящегося где-то между script kiddie и хакером по уровню своих знаний. Он умеет взламывать программы и, например, избавляться от защиты от копирования, но недостаточно умен, чтобы самостоятельно находить новые уязвимости или писать хакерские утилиты. Все еще более усложнилось, когда некоторые "кандидаты" в хакеры начали использовать хакерские утилиты, созданные кем-то другим, взламывать программы и воровать сервисы, в то же время, делая нечто общественно полезное, а "крэкеры" перестали ломать программы и удалять защиту от копирования, а принялись взламывать компьютеры в интернете. Из-за всех этих пертурбаций значение термина "хакер" стало гораздо менее "черно-белым", и в итоге были

представлены термины "black hat", "white hat" и "grey hat". "Black hat" - плохой, "черный" хакер, который взламывает программы и иные системы с целью кражи информации, запускает DDoS-атаки и крадет номера кредитных карт. "White hat", "белый" хакер, наиболее близок к оригинальному значению термина "хакер" - много знающий программист и эксперт по безопасности, использующий свои таланты чтобы помогать повышать безопасность компьютерных систем и ловить преступников. Где-то между ними находятся "grey hat", серые хакеры, которые занимаются всем понемногу. Термины "хакер", "крэкер" и "script kiddie" часто используются в интернете и других средствах массовой коммуникации, хотя люди, занятые в области обеспечения информационной безопасности, предпочитают разделение хакеров на "белых" и "черных". Наконец, все эти термины субъективны, зависят от причастности пользующегося ими человека к одной или другой группе и могут провоцировать долгие споры о том, кто же на самом деле "черный", а кто - "белый" хакер.

### Стоит ли бояться хакеров

Не следует думать, что хакеров интересует только крупные фирмы. Всё чаще они атакуют не защищенные (или слабо защищенные) от вторжения домашние компьютеры, подключенные к интернету. Атака может исходить и изнутри - от программы-шпиона, проникшей на компьютер, например, в качестве вложения в письмо со спамом.

### Самые известные хакеры

Здесь содержится краткая информация о наиболее известных хакерах, как "черных", так и "белых". Все они хорошо известны по множеству причин: из-за их поступков - хороших и плохих, - их вклада в разработку программ и технологий, новаторского подхода, умения нестандартно мыслить. Ричард Столмэн (Richard Stallman) известен как отец бесплатного программного обеспечения. Когда Ричард работал в лаборатории исследования искусственного интеллекта в MIT в 1971 году, он, при попытке исправить работу не самой важной программы, столкнулся со множеством "соглашений о неразглашении" и проблемой закрытых исходных программных кодов. После поучительной "битвы" за право обладания исходниками неправильно работающей принтерной утилиты - а это была именно она, - Столмэн сдался и стал одним из основных сторонников бесплатного программного обеспечения, создав в процессе своей дальнейшей деятельности GNU и Free Software Foundation. Деннис Ритчи (Dennis Ritchie) и Кен Томпсон (Ken Thompson) известны благодаря двум важнейшим программным разработкам XX века:

операционной системе UNIX и языку программирования C. Оба начали свои карьеры в Bell Labs в 1960-х, навсегда изменив компьютерный мир своими идеями. Кен Томпсон больше не в компьютерной индустрии, но Деннис Ритчи по-прежнему является сотрудником Lucent Technology и работает над новой, основанной на UNIX операционной системой под названием Plan9. Джон Дрейпер (John Draper), известный как Cap'n Crunch, знаменит своими взломами телефонных сетей при помощи свистка из коробки кукурузных хлопьев Cap'n Crunch (откуда и получил свое прозвище). Помимо заложения основ в деле телефонных фрикеров, Джон известен авторством программы, которая была, пожалуй, первым в мире текстовым редактором для IBM PC. В настоящее время он возглавляет собственную компанию, специализирующуюся на разработке систем защиты от спама, отражения хакерских атак и обеспечения безопасности персональных компьютеров. Роберт Моррис (Robert Morris) знаменит созданием первого в истории интернет-червя в 1988 году. Червь заразил тысячи компьютеров и практически остановил работу интернета на целый день. Помимо прочего, червь Morris был, наверное, первой автоматической хакерской утилитой, использовавшей несколько неисправленных уязвимостей в компьютерах Vax и Sun. Кэвин Митник (Kevin Mitnick), самый знаменитый "черный" хакер, был пойман компьютерным экспертом Цутому Симамура (Tsutomu Shimomura). Кэвин Поулсен (Kevin Poulsen) все еще известен благодаря осуществленному им в 1990 году взлому телефонной сети Лос Анджелеса, после которого он стал 102-м позвонившим на радио и выиграл Porsche 944. Правда, потом Кэвина поймали и посадили в тюрьму на три года. Сейчас он работает колумнистом на сайте SecurityFocus. Владимир Левин, русский компьютерный эксперт, взломавший сеть Citibank и укравший 10 млн USD. Его арестовал Интерпол в Великобритании в 1995 году. Суд приговорил Владимира к 3 годам лишения свободы и штрафу в 240015 USD. Цутому Симамура (Tsutomu Shimomura) - пример "белого" хакера. Он работал в суперкомпьютерном центре в Сан-Диего, когда Кэвин Митник взломал сеть центра и украл информацию о технологиях сотовой связи и другие секретные данные. Цутому начал охоту на Митника, приведшую в итоге к аресту последнего. Линус Торвалдс (Linus Torvalds) известен как создатель Linux, наиболее популярной и широко используемой в наши дни UNIX-подобной операционной системы. Линус начал разработку новой ОС в 1991 году, основав ее на ряде неоднозначных в те времена технологий вроде концепции бесплатного программного обеспечения и публичной лицензии GPL. Он также известен своими спорами с Эндрю Танненбаумом (Andrew Tannenbaum), автором ОС Minix, ставшей источником вдохновения на старте проекта Linux.

Если же поверить в то, что хакеры тоже являются обычными людьми, то классики данной субкультуры предлагают следующее описание обычного представителя этого сообщества. Общий вид. Хакеры чаще всего не злоупотребляют высококалорийной пищей и поэтому всю жизнь остаются худыми и долговязыми. Загар -- чрезвычайно редкое явление для хакера. Длинные волосы и борода встречаются довольно часто (второе касается, естественно, лишь представителей мужского пола). Одежда. Очень редко хакеры похожи на существующий в кинематографе образ молодого человека в костюме, с короткой стрижкой и в очках (а-ля Matrix). Чаще всего футболки, джинсы и сандалии являются обязательными предметами гардероба каждого хакера, в них он предпочитает работать, ходить в университет, спать, смотреть телевизор, читать новости -- словом, жить. У хакеров существует неприятие костюмов и галстуков, и при нынешнем спросе на высококвалифицированных специалистов нередки случаи, когда, если возникала дилемма -- надеть деловой костюм или быть уволенным, хакер выбирал последнее. Интересы (кроме компьютеров). Научная фантастика, логические игры (шахматы и пр.), музыка. Некоторые хакеры старшего поколения были весьма активными радиолюбителями, сегодня, пожалуй, предметом интереса в свободное время становятся карманные ПК и новые сотовые телефоны. Спорт. Хакеры всеми силами избегают командные спортивные игры, и каждую попытку заставить их играть в баскетбол или футбол с ровесниками (чаще всего это навязывается родителями) рассматривают как смертельную пытку. Кроме того, хакеров довольно трудно уговорить смотреть телевизор, пусть даже в это время транслируется финал чемпионата мира по футболу или очередной день Олимпиады. Они предпочитают действовать, а не смотреть, как действуют другие. Чаще всего эти энтузиасты интересуются восточными единоборствами, особенно теми, которые проповедуют медитацию и исследование себя. Некоторые хакеры известны своим пристрастием к штанге, причем по той лишь причине, что скамью и штангу с блинами можно разместить в одной комнате с компьютером. Образование. Чаще всего наиболее одаренные хакеры так никогда и не заканчивают вузов, а отдельные экземпляры при необходимости даже не могут похвастаться школьным аттестатом. Между тем как раз самоучки и люди без дипломов чаще всего приобретают большой авторитет именно благодаря своему желанию учиться и познавать новое. Если же ввиду определенных причин хакер оказывается в университете, то чаще всего предметом интереса становится информатика, физика, математика. Гуманитарии более склонны к философии и лингвистике. Предметы ненависти хакеров. Классики приводят здесь такой уникальный набор элементов окружающей среды, как деловые костюмы (которые уже упоминались раньше), бюрократические работники, продукты Microsoft, мэйнфреймы компании IBM, язык программирования

Basic (а также те, кто замечен за частым употреблением этого языка), легкая музыка, человеческая тупость и некомпетентность, телевидение и все, что связано с поп-культурой. С приходом объектно-ориентированного программирования ругательным словом в среде профессиональных программистов стало слово goto.

Митник Если бы в мире проводился хакерский конкурс, то Кевин Митник (Kevin Mitnick) был бы приглашен на него в качестве председателя жюри. Пожалуй, самое известное имя, которое у широкой публики ассоциируется со словом "хакер", принадлежит именно Кевину. Подросток (сегодня ему, правда, уже за тридцать) отличался своими незаурядными способностями к самообразованию, а также необычайной агрессивностью в технологическом плане. Друзья этого некогда упитанного хмурого парня вспоминают некий жестокий порыв Митника, когда группа студентов подрабатывала продажей "блюбоксов" -- устройств, которые имитировали сигнал телефонной станции и позволяли беспрепятственно пользоваться ее услугами для звонков в любую страну мира за чей угодно счет. Если для большинства студентов телефонный фрикинг (phreaking) был одним из способов заработка (на блюбоксах делали свои первые деньги Возняк и Джобс, впоследствии основавшие Apple Computer), то Митнику всегда больше нравилось бесшабашное баловство, когда на чужие кредитные счета уходили астрономические суммы за телефонные переговоры, все звонки в справочную службу телефонной компании перенаправлялись на домашний телефон Митника, а из компьютеров компании Digital Equipment на жесткий диск Митника ложилась новейшая операционная система, засекреченная даже для большинства сотрудников, не говоря уж о широкой публике. В 1988 году друг и "соратник" Митника сдал его ФБР, на укоризненный взгляд Кевина ответив: "Ты представляешь угрозу для общества". После года заключения Митника выпустили на свободу, однако странные вещи продолжались. Со счета судьи, приговорившего Митника к строгому содержанию, начали сниматься суммы, о которых судья узнавал только лишь из банковского уведомления, у надзирателя по неизвестной телефонистам причине был отключен телефон, а в базе данных калифорнийского суда, где на картотеке числились все заключенные штата, стало на одного человека меньше. В рождественскую ночь 1994 года Митник проник в компьютер Цутоми Шимомуры (Tsutomu Shumomura), известного в США специалиста по компьютерной безопасности и автора многих работ по предотвращению неавторизованных вторжений в компьютерные сети. Через месяц Митник активно использовал компьютеры общества Well, на которые перекачивались документы Шимомуры и номера кредитных карт, украденных с сервера одного из американских провайдеров. Именно тогда в дело включилось ФБР, а поскольку Шимомура представил Митника как угрозу правительственным компьютерным

системам, то персоной хакера заинтересовалось и Национальное агентство безопасности США (NSA), основу которого составляют именно "люди в черном", занимающиеся делами государственной важности. Сегодня Митник, отсидев в тюрьме около четырех лет, вышел на свободу с официальным запретом федеральных властей приближаться к компьютеру. Последние новости о Митнике включают и сообщение о том, что в ближайшем будущем он станет автором собственной колонки на сервере Contentville. Желающие узнать больше о крестере номер один могут ознакомиться с книгой Маркофа и Хефнера "Хакеры". Еда. В основном экзотическая. Китайская и вьетнамская кухня приводят хакеров в состояние экстаза, некоторые предпочитают мексиканские блюда. Несмотря на стереотип "гамбургеры--пицца", хакеры чаще всего довольно требовательны к своему рациону, справедливо считая пищу источником энергии для мозга. Универсальным напитком считается пиво, во время интенсивной работы -- кофе. Расовая и половая принадлежность. В большинстве случаев говорим "хакер" -- подразумеваем "лицо мужского пола", хотя женщины также играли в хакерском движении довольно значительную роль, и сегодня их число среди высококвалифицированных членов этого сообщества растет. В отличие от привычного стереотипа о дискриминации в других областях, хакеры-женщины из-за своей уникальности привлекают к себе большее внимание и уважение. Подавляющее большинство хакеров принадлежит к европеоидной и монголоидной расе, хотя сегодня представители азиатских рас получили некоторый перевес (ввиду высокого уровня эмиграции китайцев и японцев в США и Канаду), однако точной статистики, естественно, ожидать трудно. К тому же если говорить о мировом распределении хакеров, то Россия и Западная Европа, конечно же, делают свой значительный вклад в европеоидную "составляющую". Вероисповедание. Как ни странно, но наименее широко представлена христианская религия -- высокое число запретов, ограничений и своеобразный дидактический тон "документации" чаще всего заставляют хакеров обращаться к восточным религиям. Буддизм и дзэн являются наиболее популярными, хотя многие хакеры, в частности, признают себя атеистами или агностиками. Очень редко в данной культуре встречаются религии с высоким уровнем контроля, например мусульманство или мормонство. Многие хакеры предпочитают различные пародии на религии -- кибологию и дискордианизм. Наркотики. Несмотря на стойкий стереотип, согласно которому хакер представляется обывателю в виде длинноволосого человека с сигаретой, никотин не получил широкого распространения. Сигареты чаще всего используются для подавления стресса, хакеры же получают удовольствие от своей работы и от решения проблем, что стресса практически не вызывает. Алкоголь потребляется чаще всего в виде пива, а наиболее популярным наркотиком

является кофеин, который используется для стимуляции мозга. Что касается "запретных плодов", то здесь преобладают легкие наркотики -- самый известный анекдот гласит, что LSD и FreeBSD были изобретены в Беркли, и это не совпадение. Использование легких наркотиков и марихуаны нельзя назвать широко распространенным, однако в хакерском сообществе к этому относятся с большей толерантностью, нежели, скажем, в учебных заведениях или корпорациях. В начале 2001 года, по данным сайта Nua Internet Surveys, число наркоманов в технологических компаниях достигло рекордных пределов. Левин История, о которой писало практически каждое российское издание, в принципе, довольно банальна. Более того, можно смело утверждать, что таких случаев происходит несколько десятков каждый год, вот только пострадавшие стороны чаще всего стараются держать подобную информацию в тайне. Петербургский математик Владимир Левин, взломав сеть известной финансовой конторы Citibank, перевел на счета в других банках в общей сложности около 10 млн. долл. Те, кто знаком с делом Левина более подробно, говорят, что Левин сам ничего не взламывал, а просто купил сведения о "дырах" в безопасности Citibank у другого питерского профессионала под ником Megazoid. Неосторожно оставив информацию о себе на сервере, Левин стал объектом внимания американских спецслужб, и те в сотрудничестве с британской службой MI-5 находят в Лондоне русских, которые и приглашают Левина в туманный Альбион. В аэропорту питерский математик был арестован. Хельсингиус Мало известный в криминальном плане Йохан Хельсингиус (Johan Helsingius) на свои собственные средства содержал один из самых популярных анонимных римейлеров в Internet -- Penet.Fi. Интересно, что, по признанию Хельсингиуса, сам он никогда не прибегал к услугам анонимного почтальона. Весь сервис работал на компьютере с 486-м процессором и жестким диском объемом 200 МВ. Хельсингиус вынужден был закрыть свой сервер после того, как сайентологи заявили, что анонимный римейлер Хельсингиуса используется для публикации "секретов" сайентологической церкви. Британская газета "Observer" также обвинила Хельсингиуса в распространении, точнее, в соучастии и помощи при распространении детской порнографии в Сети. Животные. Из "стандартного набора" домашних любимцев хакеры выбирают кошек. Поведение кошачьих и их образ жизни во многом напоминают стиль существования самих хакеров, кроме того, они уважают относительную независимость и самостоятельность, демонстрируемую котами, в отличие от раболепства собак. Рыбки, хомячки и черепахи не приобрели особой популярности в хакерском мире. Иногда в доме хакера можно встретить клетку с ручными мышами, чаще всего это дань произведению Дугласа Адамса (Douglas Adams) "Путеводитель по Галактике для путешествующих автостопом" (A Hitchhiker's Guide to the Galaxy), где по сюжету

заказчиками изготовления планеты Земля во вселенской мастерской являются именно мыши. Человеческие качества. Чаще всего хакеры отличаются от остальных высоким уровнем интеллекта, интересом ко всему новому и способностью мыслить абстрактно, не поддаваясь эмоциям. У хакеров-подростков редко бывают друзья, во многом они сохраняют индивидуальность и предпочитают общаться с себе подобными. Хакеры также довольно редко "зацикливаются" на одних только компьютерах, большинство из них могут быть интересными собеседниками на другие темы, однако не стоит ожидать от хакера знания современной политической ситуации в стране и мнения о последних тенденциях в мире высокой моды. Ход мышления хакеров чаще всего является "бинарным" -- люди и события делятся на "плохих" и "хороших", если же какое-то явление не поддается такому делению, то оно разбивается на несколько составных частей, каждая из которых затем окрашивается в белый или черный цвет. Негативные качества. Хакеры иногда бывают грубыми и нетерпимыми к собеседникам, находящимся ниже их по уровню интеллектуального развития. Хакеры, представляющие собой верх организованности и логичности в виртуальном мире, зачастую просто неприспособлены к жизни в привычной обстановке -- их постели чаще всего не застелены, счета не оплачены, а посуда не вымыта. Зачатки аутизма и синдрома дефицита внимания (ADD) также нередки, хотя хакеры с упорством игнорируют все медицинские исследования по этому поводу. Принципы культуры Любой культ или религия базируется на некоем своде принципов, которые определяют нормы поведения, а также наборе правил, позволяющих отличить "плохое" от "хорошего". Хакерское сообщество не является исключением, и с самого начала его существования сформировалась определенная этика, а спустя некоторое время все в том же Массачусетском технологическом институте на свет появился документ Hacker Ethic, который является своеобразной декларацией намерений и идеологии этой субкультуры. Все познается в действии. Чтобы узнать, как работает некий аппарат, нужно его разобрать на части; чтобы понять принципы работы программы, нужно ею воспользоваться; чтобы выяснить, почему операционная система производит именно такие действия, нужно заглянуть в ее исходный код. Вся информация должна быть бесплатной. Идея цифрового коммунизма получила широкое распространение с развитием Internet. Информация является наиболее эффективной тогда, когда ее распространение не ограничено никем и ничем. Этим и объясняется патологическая нелюбовь хакеров к коммерческим софтверным компаниям, правительству и бюрократам. Если в какой-то элемент системы нельзя заглянуть, то в случае его краха может рухнуть вся система, вследствие чего подробная информация о ней и ее исходный код должны свободно распространяться. Mafiaboy Зима 2000 года принесла Internet-компаниям



новые заботы: в виртуальном мире начали все чаще проходить массированные атаки Denial-of-Service. Седьмого февраля прошлого года крупнейшие сайты Сети, в числе которых были Yahoo.com, eBay.com и Amazon.com, испытали небывалый наплыв "посетителей", причем подобные массированные атаки "вешали" сайты на весьма долгое время. Возможность проведения такой грубой, но в то же время весьма эффективной атаки заставила сетевую общественность говорить о несовершенстве сегодняшних технологий передачи данных. Два месяца спустя в Монреале канадские и американские власти арестовали 15-летнего компьютерного любителя, в Сети более известного под кличкой Mafiaboy. После допросов и расследования тинейджер был обвинен в нанесении умышленного ущерба сайтам Yahoo.com, eBay.com и CNN.com. Зловредные программы, написанные хакером (и вирусы в том числе), несут образовательную ценность и распространяются с предупреждением о нежелательности использования данного кода в других целях. Код же, который пишет крекер, чаще всего имеет разрушительный характер и ставит целью получение ценной информации, за которую нередко платит третья сторона. Хакеры в большинстве своем мастера-одиночки, оттачивающие свое искусство программирования и получающие от этого внутреннее удовольствие, в то время как крекеры имеют тенденцию собираться в мелкие группы и команды и попросту заниматься компьютерным воровством и разбоем. Хакеры считают крекеров тупиковой ветвью в эволюции человечества. Компьютерный терроризм в последнее время приобретает все большие масштабы, и свидетельством тому -- прошлогодний разгул таких вирусов и "червей", как Love Bug и Matrix. Сегодня о хакерских историях пишут только в случае громких дел или резонансных судебных процессов, однако сведения об огромной работе, выполняемой ими в сфере промышленного шпионажа и государственной разведки, по известным причинам не доступны для прессы. Ресурсов, посвященных компьютерным атакам в Сети, сегодня, наверное, больше, чем сайтов по компьютерной безопасности, но это как раз хорошо -- чем больше специалист узнает о технике взлома, тем больше опыта он получает по технике защиты. А закончить этот материал хотелось бы словами Джона Мура (John Moore): "Тот, кто в молодости не занимался хакингом на ассемблере, не имеет сердца. Тот, кто занимается этим, будучи взрослым, не имеет головы".