ПИРАТЫ? ВРЕДИТЕЛИ? ШПИОНЫ? ХАКЕРЫ...

А.О. Давидюк[1], *Н.А. Малевич*[2]

[1]-студентка 1 курса, факультета МЭО, группы УВЭД-2, Белорусского государственного экономического университета

[2]- научный руководитель, доцент кафедры информационных технологий, Белорусского государственного экономического университета, Минск, 220672, Партизанский пр. 26, тел.(8017) 249-19-81, e-mail: malevich@bseu.minsk.by

Аннотация. Если верить апокрифам, хакеры появились практически одновременно с изобретением компьютера. Оно и понятно. Ведь в изначальном значении хакер — высокопрофессиональный и (что немаловажно) весьма любопытный программист, способный к нетривиальным решениям. Недаром самым известным в компьютерном мире человеком после Билла Гейтса стал хакер Кевин Митник.

К хакерам многие относятся неоднозначно. В настоящее время слово «хакер» используется почти исключительно в негативном значении, является синонимом слова «взломщик» в применении к компьютерам и сетям. Хакинг еще не является профессией (пока?) в полном смысле этого слова. Однако для многих это стало вполне определенным родом деятельности, стилем жизни, образом мышления. Причем популярность хакеров постоянно растет. В Интернете можно найти множество хакерских сайтов, для хакеров издаются специализированные журналы, о них даже снимают фильмы.

Ключевые слова: хакер, МИТ, фрикер, крэкер, хардер, В.Левин, взлом, Кевин Митник, файл, безопасность, Билл Гейтс.

Введение

Годы спустя, когда народилась армия любителей и пользователей персональных компьютеров, хакеры неожиданно превратились из героев узкопрофессионального фольклора в персонажей мифа, сотворенного средствами массовой информации.

Но популярность слова не проясняет его смысла. Более того, его современное употребление вступило в противоречие с прежним, программистским. Обыватели считают хакеров компьютерными преступниками и террористами. Юные романтики, взращенные на триллерах, представляют их себе благородными разбойниками - этакими рэмбо и терминаторами компьютерных сетей. Программисты старой закалки приписывают им гениальность, высочайший профессионализм и самозабвенное увлечение программированием. Такой разнобой лишний раз свидетельствует, что понятие окончательно размылось. Поэтому в своей работе я попытаюсь разобраться, что же такое настоящий «хакер» и какова его роль в современном компьютерном мире.

ПРОИСХОЖДЕНИЕ ХАКЕРОВ И СЛОВА "ХАКЕР"

Источников информации в наше время предостаточно, и, начав разбираться, что к чему, сразу обнаруживаешь две легенды. Ту, что поновее, творят для широкой публики телевидение, газеты и журналы. С ней мы все более или менее знакомы. Другую легенду можно услышать от зрелых программистов. Речь в ней о "настоящих" хакерах и, что типично для рассказчиков, чья молодость уже позади, она окрашена грустью о "добрых старых временах". Вот ее краткое изложение. Принято считать, что хакеры впервые

появились в Массачусетском технологическом институте (МИТ). Так называли участников клуба железнодорожного моделирования. У них был свой жаргон, непонятный непосвященным, и они до фанатизма увлекались конструированием. Кроме того, хакерами называли студентов, склонных к незамысловатым шуткам и розыгрышам.

Когда в МИТ появились первые компьютеры, хакеры-конструкторы перенесли свою страсть на них. Среди хакеров были не только студенты, но и преподаватели с аспирантами, не на шутку увлекшиеся новой игрушкой. Именно в МИТ хакерами была написана первая графическая компьютерная игра (сражение в космосе) и изобретен джойстик. Хакеры просиживали ночи напролет в машинном зале и спали на лекциях. Похожая картина наблюдалась в других институтах и университетах США. Из этих людей сформировалось первое поколение программистов, бывших по духу скорее учеными и исследователями-первопроходцами, чем поденщиками. С них началась новая индустрия, и Меккой хакеров стала Лаборатория искусственного интеллекта МИТ.

Первые компьютерные коммуникации, возможности которых сводились к передаче файлов и работе с компьютером при помощи удаленного терминала по телефонным линиям, объединили разрозненные группы университетских хакеров в своеобразное сообщество. Чуть позже, выпуск набора деталей "сделай сам" для микрокомпьютера "Альтаир" открыл эру персональных компьютеров. Сообщество хакеров пополнилось членами самодеятельных клубов любителей компьютеров.

Компьютерная связь по-прежнему имела важнейшее значение, поскольку только благодаря ей группы энтузиастов вливались в единое целое. Естественно, у хакеров сложился свой жаргон и неписаный кодекс поведения. Например, уважения товарищей можно было добиться только глубоким знанием компьютера и самозабвенным программированием, мотивируемым радостью интеллектуального свершения. Самой сутью сообщества был свободный и бескорыстный обмен информацией и программами. Это был "золотой век" хакеров. А потом их сообщество, по мере роста, стало расслаиваться. Так, были заметными интеллектуальные хакеры первой волны: ученые, исследователи и профессиональные программисты. Их даже называли не хакерами, а нердами, то есть "умниками". Среди остальных выделялись хакеры, разделявшие идеологию хиппи. Это они щеголяли длинными волосами, не отличались опрятностью, баловались травкой, увлекались восточными религиями, эпатировали почтенную публику своей асоциальностью и анархизмом. Однако всем хакерам одинаково не нравилась нарастающая коммерциализация программирования. Для одних она означала ограничение свободы обмена информацией, другие по идеологическим соображениям отвергали буржуазное торгашество. В исторической перспективе заметным событием той поры стало открытое письмо тогда еще юного и малоизвестного Билла Гейтса. Он одним из первых во всеуслышание обвинил хакеров в краже интеллектуальной собственности и приравнял к преступникам. Дело в том, что Гейтс рассчитывал немало выручить на розничной продаже компилятора Бейсика для персональных компьютеров, но программа разошлась по хакерским каналам сотнями экземпляров. Не исключено, что широко распространенная среди программистов неприязнь к "Майкрософту" и лично Уильяму Гейтсу отчасти объясняется описанным событием. А борьба хакеров с коммерсантами от программирования продолжается и в наше время. Одни пишут и бесплатно распространяют программы высокого класса, а другие "из принципа" вскрывают защиту коммерческих программных продуктов.

По словам одного знаменитого хакера:

“Многим программистам не по душе коммерциализация операционных систем. Возможно, что они смогут больше зарабатывать, но от них потребуется считать других программистов противниками, а не товарищами.

Основное проявление дружбы программистами - обмен программами, но существующие рыночные отношения не позволяют программисту иметь друзей. Покупатель программы должен выбирать между дружбой и послушанием закону.

Естественно, многие выбирают дружбу, но тем, кто верит в закон, приходится нелегко, что бы они ни решили. Они становятся циниками и приходят к выводу, что программирование - лишь способ зарабатывать деньги...

Я ищу людей, которые считают, что создание духа сообщества так же важно, как и зарабатывание денег... Нет ничего дурного в желании получить вознаграждение за труд или увеличить свои доходы до тех пор, пока для этого не используются разрушительные методы. Но в области разработки программ нынешние методы разрушительны. Выкачивание денег из пользователей программы путем ограничения ее применения разрушительно, поскольку ограничивает число и разнообразие возможных применений программы. А это снижает выгоду, которую человечество может извлечь из нее. Когда намеренно создаются запреты, их последствием становится разрушение. Причина, по которой достойный гражданин не прибегает к средствам увеличения своего благосостояния за чужой счет в том, что если бы так поступили все, то все бы обеднели во взаимном противостоянии. Такова кантианская этика, ее Золотое Правило. Лично мне не понравились бы последствия всеобщего утаивания информации, следовательно, я должен считать это вредным и для всех остальных. В частности, желание получить вознаграждение за свой творческий труд не оправдывает лишение всего или почти всего мира возможности воспользоваться плодами этого труда..."

На этом, пожалуй, можно закончить пересказ легенды о "настоящих" хакерах.

Теперь остается только перевести слово "hacker". Словарей, в которых упоминаются хакеры, я нашла всего пять: "Словарь по программированию и информатике" А.Б. Борковского, "Англо-русский фразеологический словарь" А.В. Кунина в двух томах, бессменный словарь Мюллера, "Оксфордский толковый словарь современного английского языка" А.С. Хорнби, "Словарь американского сленга" Р.А. Спиерса. Кроме того, пригодилась книга Э.С. Реймонда о жаргоне англоязычных хакеров и кое-что из хакерского фольклора. Ничего нового не оказалось в толковании из словаря по программированию. Оно содержало два варианта: во-первых, хакер - это "программист, способный писать программы без предварительной разработки детальных спецификаций и оперативно вносить исправления в работающие программы, не имеющие документации", а во-вторых, "пользователь вычислительной системы (обычно сети ЭВМ), занимающийся поиском незаконных способов получить доступ к защищенным данным". Негусто, но словарь-то специальный. Часто слова, используемые в качестве технических терминов, утрачивают свой исконный смысл, приобретая в техническом контексте новые значения. В результате, их употребление в узкоспециальном смысле, но в общем контексте, зачастую просто ошибочно.

Классический тому пример - слово "файл", известное каждому пользователю. При переводе выясняются поразительные вещи: "файл", в зависимости от контекста, означает напильник, пилочку для ногтей, отделку, полировку, оглоблю, дышло, ловкача, скоросшиватель, скрепку, досье, подшивку газет, картотеку, ряд, шеренгу, колонну, очередь... Компьютерный "файл" - далеко не то же самое, что "file" бытовой.

С "хакерами" дело обстоит точно так же. Вот значения "hacker" из словаря американского сленга: водитель такси, небрежный или неспособный программист, неудачливый во всех отношениях человек. Насколько могу судить, "неудачник" звучит для американцев одним из худших определений, как "никудышный человек".

В остальных словарях слова "hacker" не нашлось. Но "hacker" образовано от "hack", как "пловец" или "певец" от "плыть" или "петь". Переводы "hack" в роли глагола и существительного кое-что проясняют.

Так, много прямых значений существительного "hack" связано со словами кирка, мотыга, топор, удар, зарубка, ссадина на ноге, резаная рана... "Hack" означает простые инструменты, которыми ударяют, которыми можно пораниться и так далее. Очевидно, отсюда происходит намек на небрежность хакеров. Сравните с русским выражением "топорная работа". Другая группа прямых значений "hack" тоже интересна: верховая или упряжная лошадь, лошадь напрокат, наемный экипаж, такси, таксист. Интересна

она потому, что вполне проясняет группу переносных значений "hack": кляча, литературный поденщик, наемный писака, журналист, халтура. И еще: тяжелая неинтересная работа, особенно писательская, изнурительный труд ради пропитания.

Напрашивается вывод, что программистов, пишущих программы, впервые назвали хакерами, подметив сходство их работы с трудом профессиональных литераторов средней руки, "писак". Ядовитое прозвище. Связь со значениями "hack" налицо: люди заняты тяжелым, неблагодарным трудом, работают как лошади, за гроши пишут топорные программы, халтуру... Но и это еще не все. Трудно представить, чтобы само название имело презрительную окраску и было уничижительным. Очевидно, кличка "хакер" для самих хакеров однажды зазвучала иначе, став символом цеховой принадлежности и предметом гордости. Подтверждает такое предположение нерд и хакер Э.С. Реймонд. Он пишет: "Сами хакеры не любят называть себя хакерами, но счастливы, когда их называют этим славным именем. Дело в том, что хакеры считают себя элитой программистского сообщества, а кричать о своей элитарности свойственно лишь идиотам. При этом хакеры не замкнуты в себе, они всегда рады каждому новому члену в своих рядах".

Что касается толкования слов "хакер", "хак" и "хачить", то согласно Реймонду, "хакер" это:

1. Программист, которому изучение тонких и неочевидных свойств системы доставляет огромное удовольствие, в отличие от основной массы тружеников, обходящихся в работе минимально необходимыми знаниями.
2. Программист-фанатик, которому практическая работа доставляет несравненно больше радости, чем теоретические разговоры о компьютерах.
3. Тот, кто способен оценить и понять значение хака.
4. Программист, умеющий очень быстро работать.
5. Знаток конкретной системы, задачи, языка. Например, "UNIX-хакер".
6. Эксперт или фанатик в любой области. Например, "хакер-ботаник".
7. Тот, кому решение сложных задач доставляет истинное наслаждение, кто любит действовать нестандартно, в обход традиций и ограничений.
8. Тот, кто всюду ищет защищенную информацию (парольный, сетевой хакер, кракер).

А вот что такое "хак":

1. Программа, которая очень быстро, но не очень качественно выполняет свою задачу.
2. Программа, великолепно выполняющая свою задачу, но на которую затрачено слишком много сил и времени.
3. Сокращенная форма слова хакер.
4. Хак как таковой, безотносительно к здравому смыслу, функциональности и тому подобному. О хаке говорят как о джазе: "Если ты спрашиваешь, что это такое, то никогда этого не поймешь".

Наконец, "хачить" означает:

1. Испытывать физические или нравственные мучения.
2. Увлеченно работать.
3. Развлекаться грубыми шутками, "откалывать номера".
4. Развлекаться изучением неизвестных тонкостей компьютерной системы.
5. Полностью отрешиться от мелких земных делишек, погрузившись в Проблему.
6. Отлаживать программу, шлифовать ее реализацию.
7. Программировать на скорую руку, ставить "заплатки".

РАЗНОВИДНОСТИ ХАКЕРОВ

Как было уже сказано, слово «хакер» употребляется в основном для характеристики тех, кто внедряется в чужие системы. Однако существуют разновидности хакеров. В частности, фрикеры, знающие как управляться с телефонной станцией на расстоянии, или ломающие сотовые телефоны; крэкеры (не путать с крекерами), взламывающие программы с защитой (например, игры); и, наконец, кардеры, живущие за счет чужих кредитных карточек. Последние, похоже,

вольготно чувствуют себя только у нас в стране, поскольку на Западе их «отлов» уже хорошо отработан. Впрочем, прецедент по поимке компьютерного преступника создан и у нас. В прошлом году на скамье подсудимых оказался 21-летний студент Белорусского государственного экономического университета, обвиненный в совершении многочисленных хищений из Интернет-магазинов мира. Суммарный ущерб от его преступной деятельности составил около 30 тысяч долларов. Студент был приговорен к четырем годам лишения свободы. Он стал первым человеком, осужденным в Беларуси за совершение краж с использованием компьютерных технологий. Кстати, если верить сообщению информационного агентства «Интерфакс», которое, в свою очередь, ссылается на оценки западных специалистов, более 50 процентов преступлений, совершаемых хакерами из стран СНГ, имеют как раз минский след.... Следует отметить, что у хакеров (особенно в их «крэкерской» разновидности) нет никакой этики. Главный принцип, которым они руководствуются — «каждый за себя и все против всех». Если и существует какая-то хакерская солидарность, то она больше похожа на солидарность воров и грабителей, образовывающих временные союзы для совершения преступления, нежели, скажем, на классовую солидарность трудящихся. Хакеров можно также сравнить с богемой. У тех и других своя этика (или отсутствие таковой с «внешней» точки зрения) и свой образ жизни: те и другие противопоставляют себя серой «толпе» — обывателям или «пользователям», которые, в свою очередь, опасаются и не любят хакеров, считая их вырожденцами и изгоями. Недаром именно хакеры составляют ядро так называемого «компьютерного подполья». Впрочем, все не так просто. Дело в том, что, как и в случае с «хорошими хакерами», двигающими компьютерный прогресс, мотивы деятельности «крэкеров» и ее конкретные формы достаточно многообразны. В этой связи условно разделим хакеров на четыре основные группы.

1. ЭКСПЕРИМЕНТАТОРЫ

К этой группе относится пытливая молодежь, осваивающая киберпространство и стремящаяся до всего дойти на собственном опыте. Подобно детям, которые усваивают нормы человеческого общежития, экспериментируя с этими нормами и намеренно делая «как нельзя», чтобы посмотреть, что из этого получится, они взламывают компьютерные системы из чистого любопытства. Злонамеренности или стремления к выгоде здесь нет — чистое баловство, в более широкой перспективе весьма к тому же полезное: именно из таких «экспериментаторов» и вырастают со временем настоящие компьютерные специалисты.

2. ПИРАТЫ

Хакеры этого типа занимаются тем, что воруют свежие программы (или коммерческие версии программ, доступных как «shareware»). Их, в свою очередь, можно разделить на несколько подгрупп. Одни специализируются на взламывании компьютерной защиты; функция других состоит в скачивании ворованного «софта» на свой компьютер (на хакерском жаргоне такие люди называются «курьерами»); третьи же — «дистрибьюторы» (которые в принципе вообще могут не знать, что такое компьютер и как он работает) занимаются распространением ворованных программ. Корыстная мотивация людей, входящих в пиратские группы, вполне очевидна. Но речь не обязательно идет о деньгах — в качестве платы за свежие программы (warez на жаргоне) принимается либо другой warez, либо адреса компьютеров со взломанной защитой. Поскольку дыры в компьютерной защите выявляются и, соответственно, «штопаются» довольно быстро (как правило, от нескольких часов до недели), адреса взломанных систем и пользуются таким спросом.

3. ВРЕДИТЕЛИ

Это настоящие компьютерные хулиганы, совершающие акты бессмысленного вандализма, только не на ночных улицах, а в киберпространстве. Они реализуют через компьютер свои криминальные наклонности — навязчивое стремление бить, громить, поджигать, насиловать, издеваться над другими, уничтожать то, что не ими создано. Именно такие парни запускают вирусы или иным способом разрушают компьютерные системы, в которые им удалось пролезть. Читают чужую переписку с целью в дальнейшем

навредить людям, к чьим письмам они получили доступ и т.д. Надо отметить, что сегодняшний компьютерный вредитель вовсе не обязательно высокопрофессионален — существует огромное количество готовых инструментов для взлома компьютерных сетей и серверов, доступных для применения любым желающим. К сожалению, желающих обычно предостаточно, так что взлом на сегодня является вполне серьезной проблемой.

4. ШПИОНЫ

К этой группе относятся охотники за секретной информацией. Обычно они работают на заказ и за очень большие деньги — на военных, разведку и т.п. Одна из самых известных историй здесь — разоблачение западногерманского хакера, работавшего на КГБ, описанное в автобиографическом романе Клиффорда Столла «Яйцо кукушки». Зацепкой, приведшей к его поимке, оказался дисбаланс в 75 центов на счету одного калифорнийского банка. Конечно, вторжение в компьютеры, «отвечающие» за национальную безопасность, — любимое развлечение «экспериментаторов», однако, как считают эксперты, за внешне невинными и хаотичными опытами могут скрываться и организованные разведывательные акции.

Перечень хакерских типов можно значительно расширить. Например, Дэвид Айков и Карл Зегер, авторы книги «Борьба с компьютерной преступностью», кроме прочего, выделяют такие виды компьютерных преступлений, как «бизнес-атаки на конкурентов», «финансовые атаки на банки» (на постсоветском пространстве этот способ получения легких денег становится, судя по сообщениям прессы, все более популярным), «атаки из мести, совершаемые работниками или бывшими работниками на обидевшие их компании», «террористические атаки на правительственные и иные компьютеры». По каждому из этих типов уже накоплен материал, который мог бы составить содержание многих томов. Очевидно одно: чем больше будет компьютеризироваться общество, тем большие возможности будут открываться перед хакерами. Компьютерные сети — не только кладезь информации и развлечений, но и поле для реализации самых разных человеческих склонностей, в том числе и деструктивных.

ВЗЛОМЫ КОМПЬЮТЕРНЫХ СИСТЕМ: ТАК ЛИ ЭТО ПРОСТО?

Подготовка. Начитавшись статей, к примеру, о деле Владимира Левина, выкачавшего через компьютер у американского Сити-банка от 400 тысяч до 3 миллионов долларов, можно подумать, что работать хакеру проще простого: сел за клавиатуру, постучал по ней - и дело в шляпе. На самом деле операция взлома необычайно сложна, в нее, как правило, вовлечены несколько десятков людей в разных странах.

Взлом никто из профессионалов не производит из своего дома или офиса. Для этого снимается квартира где-нибудь в тихом месте и на подставное имя, обычно на месяц. Попутно собираются, а проще говоря, покупаются свои агенты в банке, который собираются взломать. Они должны указать время, когда проходят электронные платежи, сообщить главный серийный номер местной АТС, по возможности узнать сетевой пароль банка, а также пароль сервера (главного компьютера внутренней сети банка). Нужен человек и в банке, куда будут переведены деньги, чтобы обеспечить их беспрепятственный прием и перевод на специальный счет. Надо иметь агента даже и в МГТС. В случае засечения взлома службой безопасности может последовать запрос в МГТС на определение телефонного номера взломщика. Агент и должен сообщить службе липовый номер. То есть, нужна подстраховка на всех возможных уровнях. Вышеупомянутый Владимир Левин, судебный процесс по делу которого еще не закончен, не входящий по неофициальному рейтингу даже в первую сотню хакеров России, по мнению специалистов, пренебрег правилами техники безопасности и допустил кучу ошибок, достойных новичка. Во-первых, он все взломы совершал с одного компьютера из одного места, каковым оказался к тому же офис его собственной фирмы. Во-вторых, он взламывал сеть банка через абсолютно прозрачную компьютерную сеть Интернет. Наконец, он не позаботился даже о введении по окончании взлома программы заметания следов. Не поймать подобного

дилетанта такому гиганту антихакерской борьбы, как ФБР, было бы просто стыдно. Но осудить тогда в России Левина не могли: статьи УК о компьютерных преступлениях действуют только с 97 г., а у США с Россией нет договоров об экстрадиции, то есть взаимной выдачи преступников. Но тут Россияне позволили ФБР пригласить хакера в Англию на компьютерную выставку, где Левин и был арестован прямо у трапа самолета, так как у Англии и США договор об экстрадиции давно есть.

КАК ЭТО ДЕЛАЕТСЯ? (ИСТОРИЯ ОДНОГО ВЗЛОМА)

Только после нескольких встреч в непринужденной обстановке мне наконец-то удалось уговорить нового знакомого подробно рассказать об операции, связанной с компьютерным взломом, в которой он сам принимал непосредственное участие.

В назначенный день около восьми вечера все "заинтересованные лица" собрались в главной штаб-квартире. Главный хакер прочитал охране инструктаж, после чего им выдали бронежилеты и рации. Каждый получил свой позывной. Хакер с ассистентом стали налаживать по рации связь с оператором группы ресурсной поддержки (всего в операции было задействовано 9 компьютеров в разных концах Москвы). На противоположной стороне улицы виднелись в полумраке силуэты двух милицейских машин - основная охрана, которая выполняя свою работу даже не знала, кто ее нанял и для каких целей. Внизу у подъезда стояла иномарка с антенной, где сидели двое мужчин - представители заказчика - одной из крупнейших московских бандитских группировок.

Исполнителям нужно было решить не совсем обычную задачу. Один европейский банк "кинул" дружественную группировке коммерческую структуру на солидную сумму. Его решили наказать, запустив во внутреннюю компьютерную сеть вирус. Последний должен был вывести из строя всю сеть минимум на сутки. Задача это не простая, поэтому работа началась уже в 9 вечера с поиска входных паролей. Основной взлом сети обычно производят рано утром, когда дежурный офицер компьютерной безопасности в банке либо спит, либо теряет бдительность. В 6 часов по рации была объявлена готовность №1. "Первый готов, второй готов, третий готов", - понеслось в ответ. Охране было приказано занять позиции по углам дома и не выпускать из виду никого входящих в дом, а также друг друга. А тем временем в квартире среди опустевших пивных банок главный хакер дал по рации ассистентам команду "Поехали!".

9 "отравленных" программ наперегонки устремились через 3 границы в атаку на главный сервер банка. Автоматическая программа электронной безопасности пыталась было их остановить, но была связана блокировочной программой и затем вообще смята превосходящими силами противника. Вырвавшиеся на оперативный простор остальные программы учинили в банковской сети погром. В результате, получив сигнал о проникновении вирусов, главный сервер просто отключил всю сеть и заблокировал ее.

РЕЗУЛЬТАТЫ И ЗАТРАТЫ

Пока срочно вызванные банковские специалисты вылавливали из сервера злобные вирусы, прошли почти сутки. В таких случаях только прямой ущерб от непрохождения платежей составляет не менее 100 тыс. долларов. А моральный ущерб в виде подмоченной репутации, которой на Западе очень дорожат, естественно, окажется еще существеннее.

Недешево обошлась операция и самим заказчикам. Свои охранники получили по 400 тыс. рублей на нос. Милиция, которая выполняла договор с "обычной коммерческой фирмой", соответственно, по 200 долларов, главный хакер заработал 5000, ассистенты, большинство из которых даже не знали, в какой операции они участвовали, получили куда меньше. Ну а техническое обеспечение влетело заказчикам в 20 тыс. долларов с небольшим. Таким образом, операция себя вполне окупила.

КНИГИ О ХАКЕРАХ

Из многочисленной литературы о хакерах, на мой взгляд, особый интерес представляет книга Клиффорда Столла "Яйцо кукушки или преследуя шпиона в компьютерном лабиринте." Она написана системным администратором компьютерного центра обсерватории в

Беркли, который, однажды обнаружив неполадки в системе, около пяти месяцев выслеживал хакера (Маркуса Гесса, описанного в книге "Хакеры"), который через его компьютер пытался пробраться в компьютеры министерства обороны США. Несмотря на то, что книга К.Столла посвящена в основном ходу слежки за хакером, она представляет особый интерес для изучения психологии хакеров как пример настойчивости, упорства, волевых беспрецедентных качеств автора.

Интересной представляется "ответная характеристика" Дж.Маркофа и К.Хефнер, которую они дают К.Столлу на страницах своей книги "Хакеры". Авторы подчеркивают, что "охота (Столла) чем-то была сродни попытке взлома"(Маркоф, Хефнер, 1996, с.183), хотя бы по тому, что установление факта проникновения требует огромного терпения и настойчивости. К.Столл следил за хакером в течение пяти месяцев, почти все свое время уделяя этому расследованию, оставляя на свою основную работу в Обсерватории гораздо меньше времени и сил, чем того требовало начальство. Все друзья и коллеги автора отговаривали его от этой затеи, правительственные службы, чьей обязанностью является расследование такого рода случаев, не отвечали на его просьбы. Длительное время "хакер" представлял для К.Столла чуть ли не большую часть его жизни: автор подключил свой карманный пейджер к компьютерной сети, так что он подавал звуковой сигнал каждый раз, когда "хакер" подключался к сети.

Таким образом, книга Клиффорда Столла будет очень интересна и познавательна для любого читателя.

Заключение

Таким образом, популярность хакеров бесспорна. Что касается их полезности для общества, то она не однозначна. С одной стороны, хакеры в своем смысле являются «двигателями технического процесса», с другой стороны они же могут создавать массу неприятностей. Одно несомненно - большинство из этих «компьютерных монстров» является действительно профессионалами в своем деле, что не моет не вызывать уважения. Конечно, хотелось бы, чтобы их деятельность была направлена по возможности только на благо человечества.

Кстати, в конгрессе США рассматривается законопроект, ужесточающий наказание для компьютерных взломщиков: власти страны намерены обезопасить компьютерные сети от проникновения в них хакеров, что может создать риск для безопасности населения. Согласно новому законодательному акту, хакеру может грозить пожизненное заключение, тогда как нынешнее законодательство ограничивает наказание десятью годами лишения свободы. Однако «в современном мире невозможно полностью исключить угрозу, связанную с компьютерной безопасностью, поскольку всегда найдутся люди, способные найти уязвимые места в системе и воспользоваться этим». Эти слова принадлежат самому известному в мире хакеру — американцу Кевину Митнику, несколько раз сидевшему в тюрьме по обвинениям в компьютерных взломах. В сентябре 2000 года он выступил с докладом, посвященном компьютерной безопасности, на конференции в Лос-Анджелесе. Там уже бывший хакер заявил, что до тех пор, пока абсолютно все сотрудники фирмы не будут знать, каким образом и с какими целями хакеры совершают свои атаки, корпоративные сети и веб-сайты не будут защищены от взлома. Кевин Митник подробно описал образ мышления, цели и методы хакеров, взламывающих корпоративные сети, и разъяснил, каким образом каждый сотрудник должен бороться с возможным проникновением взломщиков в систему. «Самое слабое место — это люди. Заставьте их понять, что безопасность — это динамический процесс, полностью развивающаяся и живущая по своим законам система»...

ЛИТЕРАТУРА

1. Дмитрий Ермак, «Работа для вас» № 10, 2002 г.

2.Алекстандр Какоткин, «Сетевые решения», АиФ, 1997г.

3.Клиффорд Столл "Яйцо кукушки или преследуя шпиона в компьютерном лабиринте".

4.Дж.Маркоф и К.Хефнер «Хакеры».