История хакерского движения

Значение термина «хакер»

Ха́кер (от англ. hack — разрубать) — чрезвычайно квалифицированны IT - специалист, человек, который понимает самые основы работы компьютер ных систем [10].

Первоначально появилось жаргонное слово «to hack» (рубить, кромсать) Оно означало процесс внесения изменений «на лету» в свою или чужую про грамму (предполагалось, что имеются исходные тексты программы). Отгла гольное существительное «hack» означало результаты такого изменения Весьма полезным и достойным делом считалось не просто сообщить автор программы об ошибке, а сразу предложить ему такой хак, который её испра ляет. Слово «хакер» изначально произошло именно отсюда.

Хак, однако, не всегда имел целью исправление ошибок — он мог ме нять поведение программы вопреки воле её автора. Именно подобные скан дальные инциденты, в основном, и становились достоянием гласности, а по нимание хакерства как активной обратной связи между авторами и пользова телями программ никогда журналистов не интересовало.

Затем настала эпоха закрытого программного кода, исходные тексты многих программ стали недоступными, и положительная роль хакерства нача ла сходить на нет — огромные затраты времени на хак закрытого исходног кода могли быть оправданы только очень сильной мотивацией — такой, ка желание заработать деньги или скандальную популярность.

В результате появилось новое, искажённое понимание слова «хакер» оно означает злоумышленника, использующего обширные компьютерные зна ния для осуществления несанкционированных, иногда вредоносных действи в компьютере — взлом компьютеров, написание и распространение компью терных вирусов.

По иронии судьбы хакерами сейчас в шутку называют программистов отлично разбирающихся в компьютерах и программном коде, даже если он ни в каких информационно-технологических преступлениях не были замеша ны. А ведь когда-то их так называли не в переносном, а в прямом смысле. Вс дело в том, что достоянием общественности становились лишь противоправ ные действия хакеров. В самом деле, что интереснее: узнать, что хакер испра вил ошибочный фрагмент кода, заставив программу работать, или выяснить что написанный хакером код можно использовать для перевода денег с одног банковского счёта на другой?[6]

Иногда этот термин применяют для обозначения специалистов вообщ — в том контексте, что они обладают очень детальными знаниями в каких либо вопросах, или имеют достаточно нестандартное и конструктивное мыш ление. С момента появления этого слова в форме компьютерного термин (произошедшего в 1960-е годы), у него появлялись новые, часто достаточн различные значения.

Второе и первое определение можно считать очень близкими или одни целым. Ведь без первого второе невозможно. Чтобы что-то сломать, над знать, как это построить.

Зарождение и развитие хакерства

В начале были Настоящие Программисты. Они не называли себя "хаке ры". Прозвище "Настоящий Программист" не было распространено до конц 1980. Но, начиная с 1945 г. технология вычисления привлекала и привлекае наиболее яркие и творческие умы мира. С этого времени начинает существо вать более или менее продолжительная и саморазвивающаяся техническа культура программистов-энтузиастов, людей, которые устанавливали про граммное обеспечение и свободно им владели.

Настоящие Программисты обычно заканчивали инженерные или физи ческие факультеты, составляли программы на машинном языке ассемблере ФОРТРАНЕ и половине дюжины древних языков, забытых теперь. Они был предшественниками культуры хакеров и, в значительной степени, остались не воспетыми героями предыстории.[3]

Мировая история хакерства ведет свое начало с 60-х годов XX века, ко гда студенты Массачусетского технологического института (MIT) стали про изводить первые манипуляции с компьютерными программами. Именно тогд и вошло в обиход слово “hack” в новом значении. Некоторые члены группы обращают свой пытливый ум на новый университетский компьютер, начинаю манипулировать с программами.

1970г. Телефонные фрикеры. Фрикеры взламывают местные и междуна родные телефонные сети, чтобы звонить бесплатно. “Отец” фрикеров - участ ник войны во Вьетнаме Джон Дрэйпер (известный как Cap’n Crunch) - обна ружил, что игрушечный свисток-сувенир, который он нашел в коробке овся ных хлопьев Cap’n Crunch, издает звук с частотой 2600 герц, совпадающей частотой электрического сигнала доступа в телефонную сеть дальней связ AT&T. Он построил первую “голубую коробку” Blue Box со свистком внутри который свистел в микрофон телефона, позволяя делать бесплатные звонки.

Вскоре журнал Esquire опубликовал статью “Секреты маленькой голу бой коробки” с инструкциями по ее использованию. Это вызвало волну мо шенничеств с телефонными сетями в США. Производством “голубых коро бок” в домашних условиях и их продажей занимались друзья по колледж Стив Возняк и Стив Джобс, основавшие в последствии Apple Computer.

1980г. Хакерские доски сообщений и сообщества хакеров. Телефонны фрикеры начинают заниматься компьютерным хакерством, возникают первы системы электронных досок объявлений (BBS), предшественников групп но востей Usenet и электронной почты. BBS с такими названиями, как “Sherwoo Forest” и “Catch-22″, становятся местами встреч хакеров и фрикеров, обмен опытом по краже паролей и номеров кредитных карт. Начинают формировать ся хакерские группы. Первыми были “Legion of Doom” в США и “Chao Computer Club” в Германии.

1983г. Детские игры. Первый фильм про хакеров “Военные игры” (”Wa Games”) представил широкой общественности это явление. Главный персонаж хакер проникает в некий компьютер производителя видеоигр, который оказы вается боевым симулятором ядерного конфликта, принадлежащего военным. В результате возникает реальная угроза ядерной войны, и военные переходят

режим “Def Con 1″ (Defense Condition 1 - высшая степень состояния боеготов
ности). Начинает формироваться образ хакера-кибергероя (и антигероя).

В том же году были арестованы 6 подростков, называвших себя «бандо
414». В течение 9 дней они взломали 60 компьютеров, среди которых машин
Лос-Аламосской лаборатории ядерных исследований.

1984г. Хакерские журналы. Регулярно начал публиковаться хакерски
журнал «2600». Редактор Эммануил Голдштейн (настоящее имя Эрик Корли
взял псевдоним от главного героя произведения Джоржа Оруэла «1984». На
звание журналу, как легко заметить, дала свистулька первого фрикера Cap’
Crunch. 2600, а также вышедший годом раньше онлайновый журнал «Phrack
публиковали обзоры и советы для хакеров и фрикеров. Сейчас «2600» прода
ется в самых больших и уважаемых книжных магазинах.

1986г. Признание взлома компьютеров преступлением. Обеспокоенны
нарастанием количества взломов корпоративных и государственных компью
теров, Конгресс США принял “Computer Fraud and Abuse Act”, который при
знал взлом компьютеров преступлением. Однако на несовершеннолетних о
не распространялся.

1988г. Червь Морриса. Первый значительный ущерб от вредоносно
программы. Саморазмножающаяся программа студента Корнельского универ
ситета Роберта Морриса вывела из строя около 6000 университетских и прави
тельственных компьютеров по всей Америке, причинив огромный ущерб. Сы
директора по науке одного из подразделений Агентства национальной безо
пасности Роберт Моррис был исключен из университета, приговорен к 3 года
испытательного срока и 10 000 долларов штрафа. По его словам, программу о
написал в целях исследования распространения информации в UNIX-среде се
ти ARPAnet, прародительнице Интернета.

1989г. Первая история с кибершпионажем. Хакеры из ФРГ, тесно свя
занные с Chaos Computer Club, проникли в правительственные компьютеры
США и продали полученные оттуда данные КГБ. Хакеры были арестованы
приговорены к испытательным срокам и штрафам.

1990г. Операция Sundevil. В 14 городах США прошла массовая облав
на хакеров, обвиняемых в воровстве номеров кредитных карт и взломе теле
фонных сетей. Арестованные активно дают друг на друга показания в обме
на судебный иммунитет. По хакерским сообществам нанесен сильный удар.

1993г. Состоялся первый Def Con в Лас-Вегасе - самый крупный ежегод
ный съезд хакеров. Изначально Def Con планировался как разовая встреча, по
священная прощанию с BBS. Впоследствии мероприятие стало ежегодным.

Во время викторины - розыгрыша автомобилей в прямом эфире на од
ной из радиостанций хакер в бегах Кевин Паулсен и двое его друзей так забло
кировали телефонную сеть, что на радио проходили звонки только от них. Та
они выиграли два автомобиля “Порше”, турпоездки и 20 000 долларов.

1994г. Хакерские утилиты перемещаются на веб-сайты. Появление брау
зера Netscape Navigator делает веб более удобным для просмотра и хранени
информации, чем BBS. Хакеры со своими программами, утилитами, советам

и технологиями переезжают с досок объявлений на веб-сайты. Все это богат
ство становится общедоступным.

1995г. Арестованы Кевин Митник и Владимир Левин. Главный серий
ный киберпреступник - неуловимый Кевин Митник - наконец пойман ФБ
Судебные разбирательства длятся 4 года. Все это время хакер номер 1 сидит
тюрьме. Пресса делает из него человека-легенду. Когда в марте 1999 года су
выносит обвинение, оно поглощает уже отсиженный срок. Митника выпуска
ют, запретив заниматься некоторыми видами деятельности.

Российский хакер - 30-летний Владимир Левин - крадет из американско
го Citibank 10 миллионов долларов. Его ловят и передают США. Приговор -
года тюремного заключения. Из похищенного возвращено все, кроме 400 00
долларов.

1997г. Взломы AOL. Свободно распространяемая хакерская программа
издевательским названием “AOHell” (”America-On-Hell”) стала кошмаром дл
America Online – крупнейшего интернет-провайдера. С ее помощью даже са
мый непродвинутый пользователь мог подкладывать многомегабайтные поч
товые бомбы в e-mail-сервисы AOL и обрушивать потоки спама в чатах. Тако
го рода программы способствовали зарождению сообществ неквалифициро
ванных хакеров или, как их еще называют, “скриптовых детишек” (scrip
kiddies), у которых хватает ума лишь пользоваться чужими хакерскими утили
тами. В том году сотни тысяч пользователей AOL оказались жертвами спам
бомбардировок.

1998г. Программа для взлома Windows 95/98. Хакерская команда “Куль
мертвой коровы” (Cult of the Dead Cow) создает программу “Back Orifice
(”Черный ход”) для взлома Windows 95/98. Эта мощное средство захвата кон
троля над удаленной машиной через засланную троянскую утилиту. Програм
ма представлена на съезде Def Con.

Во время очередного обострения ситуации в Персидском заливе десятк
компьютерных систем, принадлежащих Пентагону, подверглись хакерско
атаке. Заместитель министра обороны Джон Хэмр назвал эту атаку самой хо
рошо организованной и методичной из всех, каким ранее подвергались воен
ные компьютеры США.

Американское командование заподозрило в атаке происки Ирака с це
лью помешать высадке американских войск в Персидском заливе. Однако, им
оказались не иракцы, а два израильских тинейджера. Главным был 19-летни
Эхуд Тенебаум, известный под именем “The Analyzer”. Оба были арестованы
обвинены в компьютерном взломе, совершенном по предварительному сгово
ру. Сейчас Тенебаум работает главным техническим специалистом одной и
компьютерно - консалтинговых фирм.

После ядерных испытаний Индии и Пакистана международная групп
хакеров-пацифистов взламывает их ядерные центры, крадет оттуда и публику
ет мегабайты закрытой информации.

2000г. В обслуживании отказано. В пике популярности распределенны
атаки типа “Отказ от обслуживания” (denial-of-service или DDoS-атаки). По

их натиском падают крупнейшие сайты eBay, Yahoo!, CNN.com, Amazon
другие.

Некие хакеры крадут из корпоративной сети Microsoft и публикуют ис
ходные коды последних версий Windows и Office.

2001г. DNS-атаки. Жертвой масштабного взлома DNS-серверов стано
вятся сайты Microsoft. Корпорация проявляет чудеса нерасторопности. Многи
ее сайты остаются недоступными для миллионов пользователей от нескольки
часов до двух суток.

В 2001 году 30 стран, включая США, подписали «Конвенцию о кибер
преступлениях», устанавливающую общие для стран-участников методы
борьбы с нарушителями закона в Сети. Конвенция конкретизирует уголовны
и гражданско-правовые санкции за хакерство, нарушение авторских прав
детскую порнографию. Договор содержит также меры предосторожности, вве
денные в связи с сентябрьскими терактами в США, что дает странам
участникам равные права для контроля информации о подозреваемых в терро
ризме, передаваемой через Интернет.[12]

2 Последствия хакерского движения в сфере информационных тех
нологий

Информационные технологии (ИТ, от англ. information technology, IT) –
широкий класс дисциплин и областей деятельности, относящихся к техноло
гиям управления и обработки данных, в том числе, с применением вычисли
тельной техники. [10]

Именно в этих сферах деятельность работают высококвалифицирован
ные специалисты, в том числе и хакеры, как специалисты, обладающие об
ширным и полным представлением об устройстве компьютера и программны
кодах и имеющие достаточно нестандартное и конструктивное мышление.

Мотивы деятельности хакеров.

Практически все, кто серьезно занимался проблемой хакерства, отмеча
ют их незаинтересованность в нанесении какого-либо ущерба и разглашени
конфиденциальной и тем более секретной информации. Хакера мало привле
кают данные, перерабатываемые компьютерной системой. Его интересует са
ма система как сложный программно-аппаратный комплекс, способы проник
новения в систему, исследование ее внутренних механизмов и возможност
управления ими, а также использование этот системы для доступа к други
системам.

Современные компьютеры представляются хакерам чрезвычайно умны
и сложным механизмом, бросающим интеллектуальный вызов человеку, н
ответить на который истинный исследователь не в состоянии. Кроме того, са
процесс проникновения в систему и исследование архитектур операционно
системы и приложений дают намного большее удовлетворение, чем чтени
защищенных файлов данных.

Между различными участниками “компьютерной субкультуры” сущест
вуют вполне определенные отношения. Так, например, хакеры признают опре
деленную степень профессиональной подготовки у компьютерных пиратов
авторов компьютерных вирусов, но при этом недолюбливают и тех и других.

авторами вирусов у хакеров связаны крайне неприятные ассоциации, поскольку первые нарушают практически все принципы хакерской этики: вирус лишает массы надежного инструмента; вирус разрушает информацию, принадлежащую всем; вирус мешает свободному обмену программами и т.д.

У любого пользователя ПК, который имеет хоть какое-то отношение к компьютерным сетям, есть шансы стать жертвой компьютерного преступления. Но что же именно толкает хакеров на противоправные действия? Чтобы понять это и многое другое, стоит сначала разобраться с мотивами действий компьютерных злоумышленников; понять, что именно может сделать вас мишенью атаки.

Конечно, практически каждый человек рассчитывает на то, что как раз он не станет жертвой злоумышленника. Но хакеры руководствуются своими собственными соображениями, и мнения и желания простых пользователей их в большинстве случаев совершенно не интересуют. Итак, каковы же основные мотивы хакерских атак на компьютерные сети организаций, отдельные серверы и даже частные компьютеры? Сегодня специалисты по компьютерной безопасности выделяют следующие группы мотивов.

Шутка. Самые распространенные шутки — использование различных программ, имитирующих сообщения об ошибках, взломах или даже удалении системы или иных важных данных с жесткого диска.

Любопытство. При этом собственно содержимое объекта атаки хакера интересует мало, для него важнее «испытать на прочность» защиту, проверить свой интеллект.

Материальная выгода. Хакерские атаки с целью получения материальной выгоды также можно разделить на несколько типов. Первый тип — это атаки, которые в случае их успешной реализации принесут хакеру деньги «на прямую». Второй тип атак — это атаки, целенаправленно проводящиеся для похищения информации, которая впоследствии будет продана. Как правило, такие акции проводятся «под заказ». Третий тип — атаки, направленные на нанесение ущерба конкуренту и получение таким способом преимущества на рынке.

Известность, признание, слава. Взлом компьютерных систем для таких людей — способ возвыситься как в собственных глазах, так и в глазах окружающих, и в первую очередь — «коллег по ремеслу».

Политика, идеология, религия. Все три этих мотива — непосредственные причины явления, называемого кибертерроризмом. Причины его могут быть самыми различными, а вот методы реализации особо большим разнообразием не отличаются.

Месть, недовольство. Эти мотивы, как правило, чреваты хакерской атакой на корпоративную сеть изнутри. Причины могут быть различными: отсутствие продвижения по служебной лестнице, низкая заработная плата, слишком низкий статус в корпоративной иерархии.

Прочие мотивы. Перечисленное выше — это, разумеется, не все мотивы, которыми руководствуются в своей деятельности современные хакеры. Иногда бывает вообще трудно выявить мотив. Случается, что причина атаки ока-

зывается совсем уж экзотической — например, экологические проблемы. Ил
весьма банальной — зависть, ревность. Кроме того, определенный процен
атак — это обыкновенный компьютерный вандализм.

Негативные проявления хакерства

Восьмидесятые годы были для хакеров не самым лучшим периодом
Именно в это время они столкнулись с непониманием, неблагодарностью
даже страхом со стороны окружающих.

В начале 80-х внимание общественности привлек еще один “компьютер
ный” феномен - компьютерная преступность.

Статистика таких преступлений ведется с 1958 года. Тогда под ним под
разумевались случаи порчи и хищения компьютерного оборудования; кража
информации; мошенничество или кража денег, совершенные с применением
компьютеров; несанкционированное использование компьютеров или кража
машинного времени. Записи велись в Стэнфордском исследовательском ин
ституте и долгое время не представляли большого интереса.

В 1966 году компьютер впервые был использован в качестве инструмен
та для ограбления банка. Случилось это в Миннесоте. В 1968 году во всех Со
единенных Штатах было зафиксировано 13 преступлений; в 1978 году - 85, а
1985 году институт прекратил ведение и публикацию статистики ввиду слож
ности определения достоверности событий, число которых быстро росло.

Абсурдно ставить знак равенства между компьютерной преступностью
хакерством. Но именно это и было сделано. Пройдет немало времени, пок
специалисты не укажут на то, что получать неавторизованный доступ и ис
пользовать его в преступных целях - далеко не одно и то же.

Немалую лепту в создание негативного образа хакера внесли средств
массовой информации, для которых сенсационность компьютерных преступ
лений оказалась “золотой жилой”. Броские заголовки, вольная трактовка по
лицейских протоколов, заумные размышления социологов привели к форми
рованию и утверждению в общественном сознании нового штампа: хакер
главное действующее лицо всех преступлений, связанных с компьютерами. П
предложению Пентагона была создана группа специалистов в области компь
ютеров (знаменитая CERT - Computer Emergency Response Team), которая бы
ла бы способна в чрезвычайных ситуациях быстро принимать адекватные ме
ры.

Отношение к хакерам изменилось - и далеко не в лучшую сторону. Вес
ной и летом 1990 года США охватило некое подобие хакерской истерии: был
проведено более 30 рейдов против компьютерных пользователей, а через не
сколько месяцев последовала вторичная волна розысков и арестов, чтобы лик
видировать предполагаемую преступную организацию, занимающуюся неза
конным проникновением в корпоративные большие ЭВМ, кражами программ
ного обеспечения, несанкционированным использованием номеров кредитны
карточек и кодов телефонной связи, а также манипуляциями с компьютерны
ми записями в системах экстренной связи с госпиталями и полицией. Поводо
к расследованию послужила “колоссальная волна жалоб” деловых людей и ор

ганизаций, чьи информационные системы подверглись атакам. Эта операци получила ласковое имя “Солнечный зайчик”.