ОТКУДА БЕРУТСЯ ХАКЕРЫ И ЧТО С НИМИ ДЕЛАТЬ?

Хакерское движение наносит тяжёлый урон современному обществу и грозит неимоверно большими неприятностями в будущем. Чтобы отвести эту беду, надо использовать все средства, включая возможности обучения и воспитания школьников.

Иосиф Гликман,
профессор Московского городского педагогического университета

Мы живём в век информатизации, которая в значительной мере определяет сейчас прогресс человечества. Выдающиеся программисты сейчас ценятся так же, как лет 50 назад ценились физики-ядерщики. Поэтому восхищение талантливыми программистами вполне оправдано, но трудно понять восхищение хакерами.

— У нас есть клуб хакеров!

— В России выходит свой журнал хакеров!

— Написать такую сложную вирусную программу, которую не может обезвредить ни одно антивирусное устройство, — это же какие способности надо иметь!

— Российские хакеры — одни из сильнейших в мире! Они без труда взламывают мощнейшие защиты американских и английских банков и изымают оттуда миллионы долларов! И даже в состоянии разрушить работу громадных финансовых компьютерных сетей, без которых банки просто задохнутся!

— Для того чтобы стать хакером, нужна сложнейшая подготовка! Это так стимулирует развитие информатики!

Я не разделяю таких восторженных оценок этого явления. Однако давайте попытаемся в нём разобраться.

В 60-е годы XX века хакерское движение не преследовало корыстных целей, поэтому не носило деструктивного характера. В нём участвовали американские профессора и студенты, стремившиеся экспериментально исследовать потенциальные возможности компьютеров и Интернета. Это было демократическое, но претендующее на элитарность сообщество. Его идеолог Джон Барлоу, обращаясь к правительствам мира, писал: «Мы творим мир, в который могут войти все без привилегий и дискриминации, независимо от цвета кожи, экономической или военной мощи и места рождения. Мы творим мир, где кто угодно и где угодно может высказывать свои мнения, какими бы экстравагантными они ни были, не испытывая страха, что его или её принудят к молчанию или согласию с мнением большинства... Мы сотворим в Киберпространстве цивилизацию Сознания. Пусть она будет более человечной и честной, чем мир, который создали до того ваши правительства»[1].

Однако к началу XXI века объединения хакеров превратились в преступные сообщества компьютерных взломщиков. Произошло это в результате слияния с теневыми и криминальными структурами, поэтому романтический ореол избранности и гениальности хакеров уходит в прошлое, сохраняясь в душах лишь очень наивных людей.

Но не все согласны с отрицательной оценкой действий современных хакеров. *Хакер*, как пишет Максим Олейников, — это «энтузиаст программирования, получающий удовольствие от самого процесса программирования». Он обнаруживает слабые места в безопасности компьютерных систем, чтобы помочь разработчикам программ повысить эту самую безопасность. А вот *кракеры* — это «бывшие хакеры, ставшие на путь нарушения закона». Он выделяет среди них вандалов, шутников и профессионалов. *Шутники* — наиболее безобидные кракеры, которые, чтобы добиться известности путём взлома сетей, достигают различных юмористических эффектов. *Вандалы* — самая ненавидимая всем компьютерным миром часть кракеров —

1

Цит. по: *Скородумова О.Б.* Хакеры как феномен информационного пространства // СОЦИС. 2004. № 2. С. 73–74.

ломают систему для её разрушения. Наконец, *профессионалы* — это те кракеры, которые взламывают сеть для кражи или подмены информации[2].

Я полагаю, что сейчас эти различия между течениями хакерства не столь существенны, ибо очевидно, что любой не санкционированный прокуратурой взлом чужих сетей является преступлением. В нашей прессе публиковались цифры о громадных экономических потерях мировой экономики от вирусных программ и хакерских атак. Я сошлюсь на капитальное исследование А.В. Соколова и О.М. Степанюка «Защита от компьютерного терроризма», вышедшее недавно в Петербурге[3]. Они приводят несколько примеров из жизни Лондона 1993–1995 годов.

«6 января 1993 года деятельность одной из брокерских контор была полностью парализована после угрозы вымогателей и созданной ими аварийной ситуации в компьютерной системе. Выкуп в размере 10 миллионов фунтов был переведён на счёт в Цюрихе. 14 января 1993 года один из первоклассных банков выплатил вымогателям 12,5 миллиона фунтов. 29 января 1993 года одной из брокерских контор пришлось заплатить 10 миллионов фунтов отступных после аналогичных угроз. 17 марта 1995 года одна оборонная фирма была вынуждена откупиться 10 миллионами фунтов стерлингов.

Во всех четырёх случаях компьютерные террористы угрожали высшим руководителям и демонстрировали имеющиеся у них возможности разрушить компьютерную систему. Все жертвы уступали требованиям вымогателей через несколько часов и переводили деньги на счета банков, находящихся в оффшорных зонах, откуда злоумышленники снимали их в считанные минуты.

Далее авторы пишут, что «только в США ежегодный ущерб, наносимый электронными преступлениями, составляет около 100 миллиардов долларов» и с каждым годом резко возрастает. Да и эта цифра занижена: по данным ФБР, 85–97% нападений на корпоративные сети не только не блокируются, но и не становятся известными, поскольку администраторы корпораций скрывают их от общества, чтобы не провоцировать дальнейших нападений и не раскрывать способов защиты! Сейчас нормальная жизнедеятельность общественного организма определяется уровнем функционирования и безопасности информационной среды[4].

Кто-то легкомысленно полагает, что это «их» проблемы и нас они не касаются! Но в современном мире всё взаимосвязано, потери мировой экономики обязательно скажутся на наших ценах и на нашем бюджете. Кроме того, компьютерные преступления совершаются и в России. При этом их число неуклонно растёт. В 2002 году было зарегистрировано 3,5 тысячи компьютерных преступлений, это в 3,5 раза больше, чем в 2001 году, а только в первом квартале 2003 года их насчитывалось уже 2850[5].

Потери от компьютерного вандализма несёт не только экономика, но и наука, которая базируется на открытиях учёных. Сколько материалов научных исследований пропадает в инфицированных вирусами компьютерах! И далеко не все из них удаётся восстановить. Поэтому учёные напрямую страдают от бесчинства хакеров. То же можно сказать и о деятелях культуры: писателях, композиторах, художниках, архитекторах и т.д. Многие из них сегодня уже работают на компьютерах. Можно ли оценить в рублях, во сколько обходится обществу разрушение их творческого труда? Почти любая практическая деятельность может сегодня понести потери от внедрения компьютерного вируса. Приведу пример.

Я работаю в педагогическом университете. Наш математический факультет оснащён большим количеством компьютеров. В начале марта прошлого года в результате внедрения вируса компьютеры были испорчены и работа не только кафедры информатики, но и всего факультета была нарушена. Вирусом было уничтоже-

2

Олейников М.А. Internet для всех. М.: Познавательная книга плюс, 2000. С. 410–414.

3

Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. СПб.: БХВ-Петербург, Арлит, 2002.

4

См.: Там же. С. 10.

5

Скородумова О.Б. Хакеры как феномен информационного пространства // СОЦИС. 2004. № 2. С. 76.

но примерно 10 000 файлов (различные документы, таблицы, рисунки и фотографии) объёмом приблизительно 5 гигабайт. Это огромный объём информации. Потерянные файлы принадлежали нескольким сотням студентов (задания, которые они выполняли по изучаемым курсам), преподавателям (планы лекций, иллюстративный и раздаточный материал, задания и вопросы для студентов и многое другое) и деканату (различного рода документация). Можно представить, сколько было потеряно времени и труда... Только на восстановление нормальной работы сервера факультета и локальной сети (это 70 компьютеров) сотрудниками кафедры информатики было затрачено 10 дней.

Теперь уже можно сказать, что только в нашей стране от компьютерного вандализма страдают миллионы людей. А сомнительная польза, приписываемая некоторыми людьми хакерству, безусловно перекрывается вредом, которое оно приносит человечеству.

Чтобы преодолеть это зло, надо уяснить его

Причины

Полагаю, что есть несколько причин, порождающих это явление. Прежде всего, можно провести параллель между действиями хакеров и подростков, которые пытаются найти применение своим возрастающим силам и возможностям. Опытные учителя и родители знают, что от некоторых ребят в этом возрасте можно ожидать весьма странных поступков: попыток залезть на крышу дома и прыгнуть оттуда вниз, положить металлическую вещицу на трамвайный рельс и посмотреть, что с ней будет, когда пройдёт трамвай, без билета пройти в метро, театр или кинотеатр (не потому, что нет денег, а для пробы своих сил и возможностей), бросить камень в окно проходящего поезда т.д. Многие из этих «экспериментов» и «шалостей» требуют резкого противодействия со стороны взрослых, вплоть до наказаний. Однако это ещё не говорит о том, что перед нами преступник. Иногда после соответствующих объяснений с родителями, милиционером или соседями такие проступки не повторяются: человек приобрёл опыт и получил урок.

Но разве вирусные программы создают ученики 7-х классов? Скорее всего, нет. Однако особенности поведения, присущие подросткам, сохраняются у некоторых людей довольно долго. Это может быть вызвано депривацией (неудовлетворением) важных потребностей некоторой части молодёжи и её неспособностью к самореализации[6]. По мнению автора известной антивирусной программы Е.В. Касперского, вирусы пишут некоторые студенты, иногда даже школьники. И делают они это по разным причинам: чтобы попробовать свои силы, самоутвердиться, преодолеть комплекс неполноценности, иногда сочетающийся с неуравновешенной психикой. Среди авторов вирусов встречаются и «исследователи», стремящиеся глубже изучить возможности компьютеров и Интернета[7].

Другая причина может заключаться во вполне обдуманных злонамеренных поступках. Желание кому-то отомстить и навредить может появиться у человека, получившего отличное компьютерное образование, **которое не сопровождалось воспитанием гуманности и ответственности.** Учитывая, что с каждым десятилетием возможности одного человека влиять на благополучие и даже жизнь других людей увеличиваются, требования к воспитанию должны возрастать. Нельзя исключить также и стремление отдельных людей использовать Интернет как политическое средство. К сожалению, немало нездоровых или просто чрезвычайно зацикленных на политике людей пытаются таким путём что-то навязать обществу, воюя с «глобализмом», с неугодными политиками или государствами.

Ещё одна причина — прямая экономическая выгода. Создание вирусных программ, как мы уже отмечали, — это преступление. Когда совершается преступление, ставят вопрос: кому это вы-

6

Ватова Л.С. Психологический срыв. Условия, причины и формы проявления // Мир психологии. 2003. № 1. С. 206–210.

7

Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. М.: СК-Пресс, 1998. С. 16–18.

годно? Студенты, специализирующиеся на информатике, с которыми я обсуждал эту проблему, рассказали, что на чёрном рынке оригинальная вирусная программа стоит дороже, чем антивирусная! Это удивительно, поскольку антивирусная программа требуется миллионам людей для защиты их компьютеров. Но мне объяснили, что вирусные программы пользуются большим спросом у некоторых богатых фирм, которые используют их для нечестной конкурентной борьбы. Запустив такой вирус в компьютерную сеть, скажем, крупного банка, можно существенно подорвать его кредитоспособность, а возможно, и разорить. Кроме того, появление компьютерных вирусов может быть выгодно компаниям, которые специализируются на продаже антивирусных программ. Ведь чем больше будет вирусов, тем чаще придётся покупать продукцию антивирусных компаний. Помните фильм Чарли Чаплина «Малыш»? Герой фильма, бедный стекольщик, заранее посылал мальчишку с рогаткой бить стёкла, а затем сам как бы случайно оказывался со своими материалами и инструментами в этом дворе. И хозяева разбитых стёкол обращались к нему за помощью. Не хотел бы таким предположением обидеть честных и респектабельных программистов. Однако жизнь учит нас, что всегда находятся люди, а то и целые фирмы, для которых деньги куда важнее, чем совесть и честь...

Мы рассмотрели возможные причины распространения в Интернете компьютерной чумы. Теперь попытаемся ответить на вопрос, какими способами можно бороться с этой болезнью.

Противодействие

Полагаю, что для обуздания этого зла надо объединить силы деятелей науки, культуры, просвещения и государственной власти. Прежде всего, силами учёных разных специальностей — социологов, философов, математиков, психологов, педагогов, экономистов, юристов — разобраться в истоках, особенностях и перспективах развития этого явления. Не менее важна адекватная правовая оценка хакерства. Следует разработать и как можно скорее принять в Государственной Думе соответствующие законы. А на их основе создать, если потребуется, государственный центр по противодействию компьютерному терроризму. Помощь в решении этой проблемы может оказать международное сотрудничество. Интернет — система международная, поэтому его болезни эффективнее лечить совместными усилиями разных стран.

Нельзя забывать и о формировании негативного общественного мнения по отношению к тем, кто создаёт вирусные программы. Каждый день пишут, сообщают, показывают деяния мошенников, воров и грабителей. Почему в этой галерее мы не видим хакеров? Разве они причиняют меньшее зло? Думаю, что средства массовой информации ещё не выработали подходы к освещению этой проблемы. Но доносить до зрителя или читателя результаты действий компьютерных вандалов и способы борьбы с ними необходимо.

Особое, на мой взгляд, внимание следует уделить педагогическим средствам противодействия компьютерному терроризму. Ведь хакеры — это молодые люди, которые или учатся в школах и вузах, или недавно закончили обучение. Если склонность к противозаконным действиям складывается в школе, то кто несёт за это ответственность? При этом, конечно же, не следует всю вину возлагать на педагогов. Переход к рыночной экономике вызвал общее снижение нравственности в нашем обществе. Мы уже говорили о том, что некоторые хакеры извлекают прямую экономическую выгоду из создания разрушительных вирусных программ.

Знание школьниками информатики, свободное владение компьютером, навыки работы в Интернете показались многим преподавателям столь важными задачами, что о параллельном *воспитании ответственности* они как-то забыли. Вряд ли можно говорить об особом «антихакерском» воспитании. Но формировать стойкие *принципы и убеждения* необходимо. Они должны строиться на неприкосновенности чужой жизни и собственности, на недопустимости обогащения за чужой счёт. Надо формировать такие *эмоционально-волевые качества* у школьников, чтобы им не нравилось компьютерное пиратство, чтобы оно вызывало у них чувство брезгливости.

И современная методика воспитания обладает для этого достаточным арсеналом средств. Надо просто рационально использовать это методическое богатство: вовлечь школьников в увлекательную коллективную деятельность; создать условия для самореализации и самоутверждения каждого ребёнка; использовать такие методы стимулирования деятельности, как соревнование, поощрение, создание ситуации личного успеха и радости совместных достижений, доверие и многое другое[8]. НО

[8] Подробнее см.: *Гликман И.З.* Теория и методика воспитания. М.: Владос-Пресс, 2002.