# Шаги в будущее
# Шаг 10: попытка защититься

***Александр ГОЛЫШКО, канд. техн. наук, г. Москва***

*В этом мире есть все, но нет покоя от всего этого.*

## Иллюзии и страхи

Говорят, не все люди произошли от обезьяны — некоторые пока задерживаются... И любят портить жизнь другим людям. В соединении с цифровым хайтэком все это дает гремучую смесь, способную нарушить любую систему информационной безопасности (ИБ). И чем дальше человечество погружается в "цифровой мир", тем больше потенциальные угрозы. Поэтому так востребованы сегодня на рынке соответствующие специалисты.

"Бизнес — увлекательнейшая игра, в которой максимум азарта сочетается с минимумом правил", — сказал однажды Билл Гейтс. Воровство с электронных платежных карт, вирусы, мошенничество в электронных магазинах, видеопираты, кража конфиденциальной информации, работа в сети под чужим именем или несанкционированная работа в чужом ПК — звенья одной цепи. Фортуна вообще любит тех, кого не замечает Фемида.

Вот так всеобщий переход на "цифру", создание "дружественных" интерфейсов для широких масс пользователей вместе с глобальным охватом телекоммуникационными сетями и информационными системами создает человечеству не только глобальные возможности, но и глобальные проблемы. Поэтому пока остается без разрешения одна из наиболее сложных задач — обеспечение в современном обществе ИБ, находящейся между интересами бизнеса, личности и государства и еще раз бизнеса. Хотя бы просто потому, что в современную эпоху ни один человек, какое бы место он ни занимал на иерархической общественной лестнице, не может быть уверен в своем будущем, не имея определенных гарантий ИБ.

## Самое слабое звено

Все мы знаем, что на рынке активно продаются и быстро совершенствуются антивирусные программы, что любая уважающая себя компания защищает свои локальные сети специальными экранами, что любая деятельность по обеспечению безопасности ныне не обходится без подразделения по ИБ, что проблемой обеспечения ИБ занимаются не только "гранды" рынка информационных технологий, но и спецслужбы всех развитых стран.

И несмотря на появление все новых и новых программ по ИБ, человеческий фактор по-прежнему остается самым слабым звеном в цепи оборонительных заграждений. Даже самые современные и близкие к совершенству технологии защиты не могут обезопасить компании от проблем с безопасностью. И если, как показывает статистика, ущерб от внешних угроз можно минимизировать, то потери от инсайдерского вмешательства, когда "засланный казачок" или просто разгильдяй работает в самой компании, становятся все масштабнее. К примеру, ущерб, который может нанести собственный системный администратор в процессе какого-нибудь улучшения информационной системы предприятия, вряд ли сравним с "нападением" хакера. Впрочем, и обижать системных администраторов администрации компании не стоит — а вдруг он и в самом деле обидится.

В США в прошедшем году ущерб от проблем с безопасностью вырос практически вдвое, дойдя до отметки в 350 тыс. долл. на одну опрошенную организацию. И это заметно больше результата, показанного годом ранее (168 тыс. долл.).

Как показало исследование, проведенное в США Национальным альянсом кибербезопасности (NCSA) и аналитической фирмой McAfee, 87 % опрошенных потребителей считают, что на их компьютерах установлен антивирус, между тем при сканировании этих систем обнаружилось, что лишь у 52 % действительно имеется обновленное за последний месяц антивирусное программное обеспечение (ПО). При этом более девяти десятых участников опроса уверены, что их компьютеры защищены от вирусов. Аналогично 70 % потребителей убеждены, что на их компьютерах установлено антишпионское ПО, но только 55 % установили его на самом деле. А 61 % утверждает, что у них есть защита от спама, хотя фильтры обнаружены лишь у 21 %. Почти 90 % респондентов хранят персональную информацию в своих компьютерах и в то же время пользуются онлайновыми услугами банков, совершают операции с ценными бумагами и занимаются другой подобной деятельностью.

Собственно само подключение к Интернету и использование его служб и услуг само по себе не создает принципиально новых проблем в области обеспечения ИБ, отличные от тех, что существуют при взаимодействии компьютеров по открытым каналам связи. Возникновение самой проблемы обеспечения ИБ компаний при подключении к глобальным сетям напрямую связано с их основными достоинствами: оперативностью, открытостью и глобальностью. Потому угрозы безопасности возникают ежедневно и ежечасно, а пять из шести компаний, которые установили системы обнаружения вторжений, получили подтверждение того, что в их сети пытались проникнуть пользователи, не имевшие на то соответствующих прав доступа.

## Мусор веером

Вероятно, нет сегодня более серьезной и "раскрученной" проблемы в информационной сфере, чем спам. Он мешает, раздражает, затрудняет обработку информации и перегружает сети связи. Кое-где он уже составляет до 80 % электронной почты. И тут тоже есть слабое звено, которым может стать каждый.

Где-то спамеры используют броские заголовки электронной почты, а где-то и виртуальную стриптизершу в качестве приманки, поддавшись на которую, люди помогают им обходить защиту, чтобы рассылать спам или паразитировать на web-сайтах.

"Спам — это архиважная проблема, грозящая свести на нет большую часть преимуществ электронной почты", — написал однажды Билл Гейтс в одном из своих регулярных электронных обращений к заказчикам.

И разослал этот спам по всему миру...

## Усугубление опасности

Меж тем инциденты, связанные с нарушением безопасности, становятся все серьезнее — профессионалы по информационным технологиям регулярно сообщают о росте своих расходов на внедрение систем безопасности, обучение и сертификацию. К примеру, в 2007 г. доля ассигнований на обеспечение безопасности в бюджете компаний превысила 20 %, вместо 15 % в 2005 г. и 12 % в 2004 г. Почти 80 % опрошенных сказали, что теперь их руководство считает защиту информации высшим приоритетом. Главной угрозой для ИБ 55 % опрошенных профессионалов по информационным технологиям назвали шпионское ПО, за которым следует недостаточная осведомленность пользователей (54 %). Почти половина считает, что вирусы и черви по-прежнему представляют опасность, а около 44 % назвали главной угрозой злоупотребления авторизованных пользователей.

Инциденты, вызванные ошибкой человека, произошли в 42 % организаций, тогда как год назад их было 59 %. В числе других проблем называют атаки через браузеры (41 %), дистанционный доступ (40 %), беспроводные сети (39 %) и недостаточное соблюдение правил безопасности (36 %). Свыше половины всех организаций утверждает, что угрозы для безопасности, связанные с использованием карманных устройств, шпионским ПО, технологией "голос поверх IP" (VoIP), беспроводными сетями и удаленными/мобильными устройствами, значительно усиливаются ежегодно.

По данным Ассоциации производителей вычислительной техники (CompTIA), средняя стоимость одного взлома в 2006 г. составила 369 388 долл., а средняя экономия от проведения тренинга по безопасности для персонала оценивалась в 352 тыс. долл.

Обнаружить злоумышленников действительно трудно, и многие атаки происходят незамеченными, ибо имеется очень много свободно распространяемых, в том числе и через Интернет, довольно мощных средств вторжения в сети. Для работы с ними не требуется специальных знаний, они хорошо замаскированы, да и многие атаки осуществляются за очень короткое время. Так что стопроцентная ИБ — не более, чем иллюзия.

## Фобии и профилактика

Мания преследования — это вообще-то болезнь, но, очевидно, не стоит ее провоцировать паранойей. У страха глаза велики, поэтому и кажется, что злые хакеры охотятся за каждым: "...вот подключишься к сети и тебя сразу "хакнут", деньги украдут, Web-сайт обгадят, "аську" угонят, "винт" отформатируют, насуют вирусов и в особо циничной форме плюнут в душу прямо с собственного экрана...".

Однако прежде, чем пугаться, вспомните старый анекдот про неуловимого ковбоя. На самом деле обычный интернет-пользователь никому не интересен. Если кто-то и будет пытаться его "хакнуть", так разве что его же знакомые, которым он чем-то насолил и у которых нет возможности (или извилин по этой части) отомстить другим способом. Элементарные меры предосторожности, конечно, соблюдать необходимо, но и в манию величия по поводу собственной значимости для хакеров впадать не следует. Часто свежего антивируса оказывается достаточно.

Что касается иллюзии конфиденциальности, то этого у всех хватает с избытком. Очень часто сетевой администратор хранит информацию о пользователях. А грамотный администратор их еще и анализирует. Стоимость хранения гигабайта невелика и продолжает уменьшаться — вдруг эти данные пригодятся? Эти сведения доступны тому, кто имеет на это право. Или, как бывает, достаточное количество денег.

Что же до появляющихся сообщений об очередном успешном акте хакинга (практически всегда он совершается против какой-то крупной корпорации), то не следует путать хакерство с информационными диверсиями и информационным шпионажем. Это специфическая отрасль промышленности, использующая сложившийся в обществе образ хакера, чтобы меньше возникало мыслей об истинных причинах и заказчиках.

В общем, хакер, взламывающий www.microsoft.com в перерыве между двумя бутылками "Клинского", чтобы начертать там: "Windows MUST DIE!" — скорее всего, красивая сказка. И если она вдруг становится былью, то все гораздо серьезнее: ведь тот же хакер — и хорошее прикрытие, и хороший объект для вербовки. Ну, вы понимаете...

## Кибервойны

Иногда в СМИ просачиваются сведения о кибервойнах, которые идут практически постоянно. В частности, в июне 2007 г. китайские хакеры взломали информационную систему Пентагона, вывели из строя 1,5 тыс. компьютеров и довели дело до того, что пришлось отключить часть компьютерной системы, обслуживающей управление главы Пентагона Роберта Гейтса. Открытых доказательств, что атака производилась именно с территории Китая, у американских властей нет и по сей день (результаты расследования засекречены), но близкий к расследованию чиновник однажды сделал заявление в том смысле, что есть "высокая степень вероятности... близкая к полной уверенности". Вскоре появились сообщения об атаках китайских хакеров на содержимое компьютеров германского правительства. Аналогичные заявления по поводу интереса к компьютерным базам, но уже в адрес сразу 20 стран, делало и британское правительство.

В прошлом году китайский корреспондент журнала "Time" провел журналистское расследование, в котором проследил судьбу хакера по имени Тан Дайлин. Китайские военные регулярно устраивают общенациональные олимпиады с большими денежными призами для поиска и найма талантливых хакеров. Тан как победитель одной из таких олимпиад получил от командования военного округа провинции Сычуань предложение поучаствовать в учениях по атакам и защите компьютерных сетей. Позднее его с товарищами включили в команду на общенациональном уровне, а в Интернете появилась новая хакерская группа NCPH, возглавляемая Таном и, по утверждению корреспондента, финансируемая военными. Вот ее-то и обвинили американцы в скачивании важных документов. Аналитическая компания iDefense утверждает, что в Китае действует не меньше нескольких сотен подобных групп, поддерживаемых Народно-освободительной армией Китая. Но Китай, как мы понимаем, — лишь один из примеров.

## Глобальный подход

К глобальным проблемам есть и глобальные подходы. В частности, в недрах Пентагона разрабатывается принципиально новая система глобального слежения — тысячи компьютеров и камер смогут в городах мира наблюдать, записывать и анализировать передвижение буквально каждого транспортного средства.

Об этом мы уже говорили ранее — сегодня все мы живем под постоянным наблюдением — достаточно лишь вспомнить видеокамеры в банке. И согласитесь, это детские игрушки по сравнению с приборами биометрического контроля, способными проводить идентификацию по чертам лица, коже человека, его жестам. Или по вшитому под кожу гражданина чипу. Пора привыкать к тому, что за нами постоянно следят и вспоминать о тотальном наблюдении каждый раз, когда захочется совершить что-нибудь недозволенное. Например, нарушить одну из библейских заповедей. Но поскольку в данном случае наблюдателем является отнюдь не Всевышний, быть может, настало время защищать себя от захватывающего интернет-шпионажа. Ведь никогда прежде частная жизнь человека, подавляющую часть которой составляет именно ИБ, не находилась в такой опасности. В особо богатых, добавим, странах мира.

И вот уже ФБР США намерено израсходовать 1 млрд долл. на создание крупнейшей в мире компьютерной базы биометрических данных, которая откроет перед государственными ведомствами США новые возможности по идентификации людей как в стране, так и за рубежом.

Очевидно, мысль о том, что за любым гражданином страны следят с утра и до ночи, тоже граничит больше с паранойей (мало нам, больным, хакеров), чем с пристальным анализом происходящего. Но нет никакого сомнения в том, что все вышеперечисленные источники информации об отдельном индивидууме могут быть объединены в гигантскую систему наблюдения, стоящую на службе того же Пентагона.

Решением проблемы обеспечения ИБ называется порой создание "параллельной глобальной сети" с иной идеологией построения. В "альтернативном Интернете" будет что-то подобное компьютерным паспортам для возможности идентификации всех интернет-пользователей, которые должны "разоружиться перед партией" (единым Центром паспортизации, очевидно). Правда, последствия подобной "паспортизации" для сети, чей бурный рост во многом как

раз и был основан на принципе "абсолютной свободы", также могут быть нерадостными.

## Угрозы на каждый день

Угрозы ИБ формируются чуть ли не ежедневно. В странах, наиболее продвинувшихся по пути в "цифровой мир", сегодня уже многому не удивляются. Проверка финансовой истории партнера или жалоба на соседа, не соблюдающего "правила капиталистического общежития", — сегодня само собой разумеющиеся и вполне рядовые вещи. Какие невиданные возможности открываются сейчас перед владельцами информации.

Тем временем всевозможная информация о вас уже давно "расползлась" в виде паспортных, телефонных, жилищно-коммунальных, налоговых, банковских, торговых, медицинских и пр. баз данных, не говоря уже о всяческих следах в Интернете от электронной почты до электронных магазинов, счетчиков посещений сайтов и пр. и пр. Помимо известных (и даже немного привычных нам) указанных выше хранилищ информации создаются новые и новые. К примеру, в магазине вам предлагают дисконтную карту, для получения которой необходимо представить полные паспортные данные, включая прописку. Конечно, вам будут присылать по этому адресу рекламу, но сформированная база данных может быть интересна не только для маркетологов.

С другой стороны, согласно исследованиям компании Harris Interactive, восемь из десяти англичан считают, что современные средства идентификации личности имеют серьезные проблемы с безопасностью. А ведь с этого и начинается работа в сети.

Существенное место в обеспечении ИБ должна занимать защита интеллектуальной собственности. Однако в информационную эру "столбить" придется практически все. Мы уже говорили о том, что успехи компьютерной техники таковы, что скоро компьютер может вытеснить даже живых актеров. Здесь, пока не поздно, было бы неплохо запатентовать свою внешность (наравне с логотипами и товарными знаками), дабы исключить ее использование в неподобающем виде в абсолютно любом сюжете.

## Поиски решения

В общем, все новые и новые проблемы, связанные с обеспечением ИБ, возникают сразу же, как только, казалось бы, решены старые. Быть может, целесообразно доверить кое-что пользователю?

Когда-то на диком Западе наблюдалась похожая правовая неопределенность, и съехавшийся туда со всего мира по большей части криминальный элемент творил, что хотел. В определенный момент многим это надоело и все предпочли договориться путем принятия соответствующей Конституции, которая с минимальными изменениями действует и поныне. Поэтому американцы любят повторять, что Господь Бог создал всех одинаковыми, а господин Кольт уравнял всех в правах. Это, как говорится, присказка, но суть притчи в том, что если дать возможность каждому пользователю информационно "закрыться" от всех и вся, то потом он сам "приоткроется" для того, что ему нужно. Тогда и создадутся условия для формирования законов информационного взаимодействия. Основная проблема тут в необходимости наличия самого широкого набора криптостойких шифров или, по-другому, множества никому не известных языков.

Однако все существующие системы шифрования и криптографии имеют свои технологические ограничения. В частности, они либо весьма надежны (требуют от "взломщика" слишком много машинного времени, в течение которого интересующая его информация, скорее всего, устареет), но относительно дороги для массового использования, либо наоборот. Но все они не дают стопроцентной гарантии от взлома и дешифрации, поскольку в применяемых в них алгоритмах присутствует все же элемент корреляции между отдельными фрагментами кодируемой информации. Выявив эту корреляцию, можно извлечь и всю информацию. К тому же грядущие успехи молекулярной компьютерной техники позволят мобилизовать для этого поистине колоссальные вычислительные ресурсы. То есть на самом деле инфокоммуникационный мир не может быть спокоен и ежесекундно чувствует на себе последствия борьбы за ИБ.

К примеру, информационная криптоизбыточность "бьет" и по каналам связи, и по стоимости самой информации. Чтобы обеспечить шифрование изображения со спутника-шпиона, необходимо дополнительно отправить в космос гипотетический контейнер с несколькими тысячами CD.

А вот одно квалифицированное мнение: "...Современная криптография с открытым ключом практически целиком опирается на гипотезы о вычислительной трудности двух хорошо известных теоретико-числовых преобразований – факторизации целых чисел и дискретного логарифмирования. Такое положение дел не может быть признано удовлетворительным, поскольку открытие новых, более эффективных алгоритмов для этих задач или создание квантового компьютера может оставить от всей криптографии с открытым ключом одни лишь теоретические результаты..." (Варновский Н. П. Математическая криптография. Несколько этюдов. — Материалы конференции "Московский университет и развитие криптографии в России". МГУ 17—18 окт. 2002 г.). Оказывается, "под Богом ходит" не только ИБ, но и защита информации вообще. Быть может, все решится по мере построения глобального информационного общества?

## Притча напоследок

На самом деле многогранная проблематика обеспечения ИБ всегда присутствовала и "во глубине веков", а в наше "цифровое" время просто обострилась и получила дополнительные грани. К примеру, необходимость в криптографии возникла параллельно возникновению конкуренции человеческих сообществ. В течение тысячелетий стало понятно, что проблему обеспечения ИБ люди могут решить только сообща. Вот только большинство проблем находится внутри них самих.

А теперь для закрепления вышеизложенного просто расскажем сказку 1002-й ночи.

"Когда же настала следующая ночь, то Шахразада разлепила струны лютни, разомкнула свои уста и продолжила дозволенные речи.

Дошло до меня, о, великий, что в далекие времена правил Аль-Гадиром царь по имени Абд-Аллах, что означает "Благословенный Богом". Он был счастлив в браке, был справедливым судьей своих подданных и жил в полнейшем довольстве и радости.

Так продолжалось до тех пор, пока царь не пожелал навестить своего брата, правившего страной, что в десяти днях пути от Аль-Гадира, и снарядился в путь. Он велел вынести свои шатры, снарядить верблюдов и мулов, слуг и телохранителей и поставил своего визиря правителем в стране, вручив тому ключ от пояса верности, который носила любимая жена царя.

И вот царь велел кликнуть клич о выезде, и огромный караван выступил за город и стал подниматься по склону холма, приветствуемый своим счастливым народом.

Вдруг из ворот дворца вылетел всадник и устремился вдогонку за уходящим караваном. Облако пыли, поднятое копытами коня, было так огромно, что заволокло солнце и привлекло взор царя Абд-Аллаха, который узнал вдруг во всаднике своего визиря. Когда же визирь приблизился и осадил коня прямо у царских ног, все увидели, что он был необычайно взволнован и вид его был так страшен, что в большом удивлении царь воскликнул: "Ну и рожа у тебя, Шарапов (или что-то в этом духе). Заклинаю тебя Аллахом, что случилось?"

"О, мой повелитель, случилась ужасная вещь, — молвил визирь, падая ниц перед царем, — ты оставил не тот ключ!"...

Но тут Шахразаду застигло утро, и она прекратила дозволенные речи."