КАК ОБЕСПЕЧИТЬ **КОНФИДЕНЦИАЛЬНОСТЬ ЭЛЕКТРОННОЙ ПЕРЕПИСКИ**

Людовик Пьера (Ludovic Pierrat)

В настоящее время большинство правительств имеют возможность просматривать электронную почту. "Киберполиция" в странах с репрессивными режимами использует эти возможности для ареста политических оппонентов, многие пользователи интернет попадают в тюрьмы за отправление или даже пересылку электронных сообщений. Один из политических диссидентов на Мальдивах был в 2002 году осужден на 15 лет тюрьмы за переписку с Amnesty International. Пользователь интернет из Сирии находится в тюрьме с февраля 2003 года за то, что переслал бюллетень, распространяемый по электронной почте. Я предлагаю несколько советов для обеспечения конфиденциальности электронной почты.

Использование адреса электронной почты, выданной интернет - провайдером (AOL, Wanadoo, Free или любой другой компанией) не гарантирует конфиденциальность. Владельцы сетей, через которые проходит ваша почта, могут с легкостью перехватить ее. Когда власти любой страны начинают следить за интернет - пользователями, провайдеры обычно предоставляют им возможность читать почту.

Адреса web-почты (Yahoo! или Hotmail) более надежны, поскольку не используют серверы местных провайдеров. В таком случае, чтобы отследить, необходимо читать или перехватывать письма в процессе передачи, что технически гораздо сложнее. К сожалению, это преимущество весьма относительно, поскольку полицейские специалисты или хакеры смогут просматривать вашу почту. Шифрование - это основной способ реального обеспечения конфиденциальности сообщений. Существуют два способа шифрования.

КЛАССИЧЕСКОЕ ШИФРОВАНИЕ

Энн и Майкл хотят обменяться секретными сообщениями, поэтому они договариваются о кодах шифровки и дешифровки и о ключах шифрования. Затем они обмениваются сообщениями, используя шифры. Проблема заключается в том, что тот, кто перехватит письма, в которых они обмениваются ключами, сможет читать их переписку. Коме того, этот человек сможет посылать поддельные сообщения Энн и Майклу. Поэтому Энн и Майкл должны обменяться ключами так, чтобы их никто не смог перехватить, при личной встрече, например.

АССИМЕТРИЧНОЕ ШИФРОВАНИЕ

Лучший способ решения проблемы - ассиметричное шифрование. Для этого нужны два ключа - один для шифрования, а другой - для расшифровки. Ключом для шифрования (открытый ключ) можно спокойно обменяться онлайн, поскольку он не может быть использован для дешифровки сообщений. Ключ для дешифровки (закрытый, или секретный) вы никому не сообщаете.

При ассиметричном шифровании Энн имеет два ключа (открытый, который она сообщает, и закрытый, который она держит в секрете). Энн посылает свой открытый ключ Майклу, который с его помощью шифрует свои письма Энн. Однако только Энн, при помощи своего закрытого клоча, может дешифровать письма Майкла. Майкл, в свою очередь, сообщает Энн свой открытый ключ. Конфиденциальность переписки обеспечена.

Но поскольку открытый ключ передается через интернет без всякой специальной защиты, необходимо проверить его достоверность. Каждый ключ имеет "отпечатки пальцев" (короткий набор символов), который можно легко уточнить по телефону.

Непроверенный ключ может быть фальшивым, созданным для того, чтобы третьи лица могли следить за перепиской, что лишает шифрование всякого смысла. Надежность асинхронного шифрования полностью зависит от проверки достоверности открытого ключа и секретности закрытого.

OpenPGP (Open Pretty Good Privacy) - это стандартный способ ассиметричного шифрования. Наиболее популярное программное обеспечение для создания и использования двойных ключей и управления открытыми ключами корреспондентов - это GnuPG (GNU Privacy Guard), которую можно использовать в различных почтовых программах, например, Thunderbird или Outlook, ebmail или instant messaging.

Программы можно загрузить с сайтов:
GnuPG :http://www.gnupg.org/
Специальную версию для Windows:
http://www.stud.uni-hannover.de/~twoaday/winpt.html

Людовик Пьера. Инженер вычислительной техники, владелец компании Wa, занимающейся консультированием и производством в сфере информационных технологий.