АНОНИМНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ КОММУНИКАЦИЙ ПРИ ИСПОЛЬЗОВАНИИ ОФФШОРНОЙ КОМПАНИИ

"Цена свободы - вечная бдительность" Томас Джефферсон.

Введение

Проблемы конфиденциальности покупки оффшорной компании и обеспечение анонимности права собственности уже не раз обсуждались в различных публикациях. Используя известные приемы эти проблемы решить относительно просто. Гораздо труднее сохранить конфиденциальность и анонимность в процессе ее использования. Взаимодействие с обслуживающей компанией и с банком невозможны без современных средств коммуникации. Именно здесь риски наибольшие. Всем известно, что проблему всегда лучше предупредить, чем решить. Поэтому превентивные меры по сохранению конфиденциальности информации весьма актуальны.

Один из основных принципов теории безопасности информации состоит в том, что любая система безопасности не прочнее, чем ее самое слабое звено. Поэтому, внедряя систему безопасности, всегда следует начинать с поиска этих самых слабых мест и в первую очередь укреплять их. Другой, не менее очевидный постулат гласит – абсолютной безопасности достичь невозможно. Поэтому применение сложных и дорогих средств защиты информации не всегда оправдано.

Рассмотрим наиболее общедоступные, недорогие и простые в использовании технологии. Они не требуют дополнительного оборудования и переучивания персонала.

Рассмотрим наиболее часто используемые способы коммуникаций:

- телефон,
- телефакс
- электронная почта
- Web.

Проводная телефонная связь

Уязвимость проводной телефонной связи очевидна. Собеседники контролируют лишь несколько метров телефонной линии, расположенных в пределах квартиры или офиса.

Рассмотрим основные участки канала связи, к которым может получить доступ вероятный противник.

1. "Последняя миля" - участок от телефонной розетки в офисе до телефонной станции. Этот участок канала связи наиболее доступен и привлекателен для конкурентов и преступников. Здесь возможно подключение специальных устройств негласного съема информации. Они позволяют получить запись разговора и идентифицировать участников. Такие устройства можно обнаружить визуально или с помощью специальных средств контроля состояния линии.

2. Телефонная станция. Теоретически, доступ к каналам связи могут получить только правоохранительные органы при наличии постановления суда. Немного статистики: В США в год суды выдают несколько сот разрешений на прослушивание телефонов. В Украине таких разрешений выдаются десятки тысяч.

Средства мониторинга телефонных переговоров входят в стандартное оборудование телефонных станций. Обнаружить мониторинг на этом участке практически невозможно. Находясь на телефонной станции, можно определить все номера телефонов, на которые осуществляются звонки или отправляются факсы с данного номера. По базе телефонов банков и иностранных компаний можно собрать статистику о всех украинских абонентах, которые туда звонят.

Мобильная телефонная связь

Как и в проводной связи, операторы мобильной связи обязаны предоставлять правоохранительным органам возможность прослушивать переговоры, а также статистику звонков.

Несколько лет тому произошел скандал, когда оказалось, что изобретатели алгоритма шифрования для мобильной связи умышленно его ослабили, чтобы облегчить доступ правоохранительным органам.

Кроме того мобильная связь дает дополнительные возможности для мониторинга. Каждый мобильный телефон имеет уникальный идентификационный код и его местоположение может определяться с точностью до 10-20 метров.

Мобильные телефоны могут дистанционно переключаться в режим разговора и таким образом использоваться для подслушивания.

Некоторой конфиденциальности мобильной связи можно достичь используя анонимные предоплаченные услуги (Sim-Sim, Ace&Base). Но если вы используете этот номер для повседневной связи, то, если за вами наблюдают, он очень скоро будет известен противнику.

Имеющиеся на рынке средства шифрования голоса для мобильных телефонов стоят очень дорого и реальный уровень их криптоустойчивости определить невозможно.

Интернет-телефония

Проблему конфиденциальности голосового общения можно решить с помощью технологий IP-телефонии и криптографии. В Интернете можно найти несколько бесплатных программ (например, PGP-phone, Speak Freely), которые используют сильную криптографию и могут работать даже на некачественных линиях связи. Для установления связи необходимо, чтобы ваш собеседник был подключен к Интернету и на его компьютере была установлена аналогичная программа.

А как быть, если необходимо позвонить на обычный номер телефона за рубежом? К счастью, проблему анонимных звонков за рубеж можно решить очень просто. Для этого необходим мобильный телефон с предоплаченной карточкой и предоплаченная карточка IP-телефонии. Важно, чтобы качество мобильной связи и IP-телефонии было высоким, иначе наложение недостатков мобильной связи и IP-телефонии сделают связь невозможной. Но даже при использовании «дорогих» провайдеров мобильной связи и IP-телефонии стоимость связи по Северной Америке и Европе в большинстве случаев будет от $0.6 до $1 за минуту. К сожалению, на практике передача и прием факсов таким образом невозможны.

В последнее время приобрела система оперативной текстовой и голосовой связи Skype. Она позволяет бесплатно общаться с любым пользователем Интернет. За небольшую плату можно звонить и на обычные телефоны. Возможны также звонки с обычных телефонов на Skype. Skype использует криптографическую защиту передаваемой информации. Используемые Skype технологии защиты данных получили благоприятные отзывы криптоаналитиков.

Анонимность и конфиденциальность электронной почты

Электронная почта сегодня наиболее дешевый и удобный способ связи. В зависимости от используемых технологий она может быть как легко доступной для посторонних, так и анонимной и конфиденциальной. Когда вы нажали кнопку "Отправить", сообщение сначала попадает на почтовый сервер Интернет провайдера. Затем, через несколько промежуточных компьютеров оно доставляется в почтовый ящик получателя. Если вы отправляете сообщение традиционным способом в открытом виде, администратор провайдера и администраторы любого из этих промежуточных компьютеров могут легко его скопировать и прочитать.

К счастью для пользователей, электронную почту довольно легко защитить от посторонних глаз. Для этого существует множество бесплатных или условно-бесплатных программ шифрования. Наиболее распространенная и надежная среди них PGP (Pretty Good Privacy). Самые новые, проверенные версии PGP можно получить на официальном

международном сайте программы PGP - www.pgpi.com. Здесь также можно получить документацию по PGP (в том числе и на русском языке) и ряд других полезных программ. Установка и использование PGP не вызывает проблем. В Интернете есть множество ресурсов, в том числе и на русском языке, посвященных использованию PGP. Пожалуй, самая большая сложность заключается в том, чтобы убедить своих корреспондентов также начать использовать PGP.

Применяя криптографические средства защиты информации, следует помнить, что для их установки и использования требуется лицензия СБУ (департамент ДСТСЗИ). Однако, это одно из не работающих на практике положений. Нарушают его все без исключения владельцы компьютеров, поскольку любая современная операционная система содержит криптографические программы.

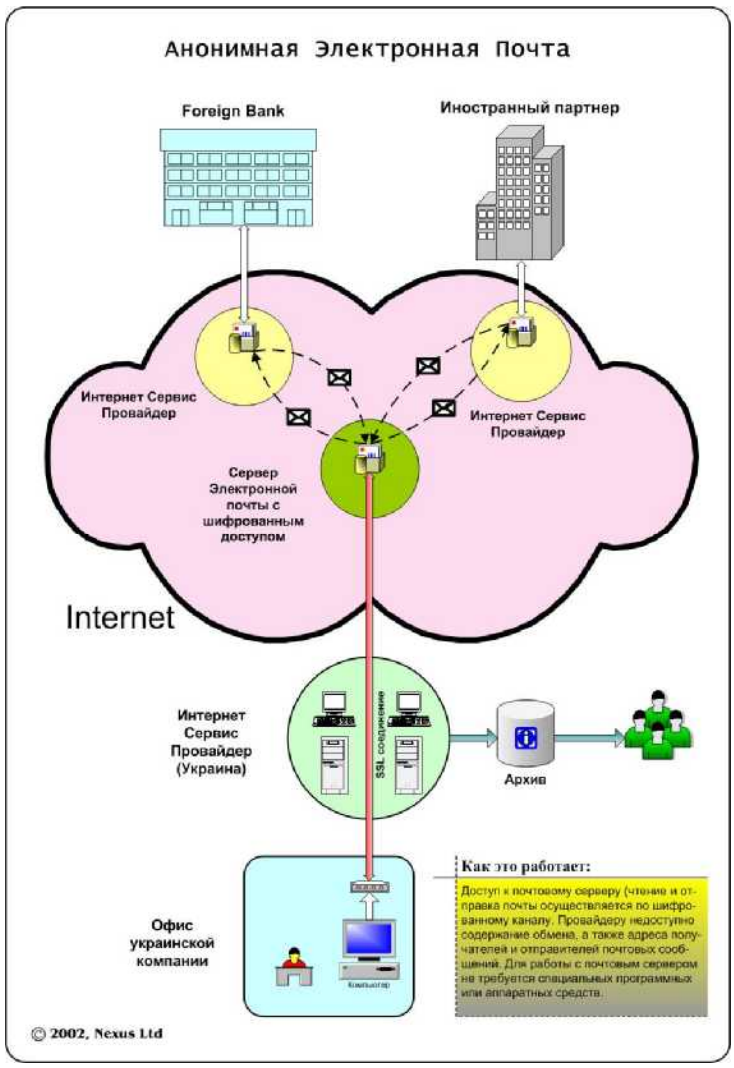
Криптография не решает другой важной проблемы конфиденциальности коммуникации - анонимности. Хотя противник, который наблюдает процесс вашего общения, не может прочитать ваши сообщения, он видит адреса ваших корреспондентов и заголовки ваших сообщений. Эту информацию также можно использовать вам во вред. Один из лучших способов обеспечения анонимности переписки основан на использовании бесплатных анонимных ремейлеров. Применяя криптографию и анонимные ремейлеры можно добиться практически полной конфиденциальности и анонимности. Услуги ремейлеров и необходимое программное обеспечение совершенно бесплатны. К сожалению, освоение этих технологий требует некоторых усилий и более глубоких познаний в области криптографии и компьютеров. Подробную информацию о работе анонимных ремейлеров можно получить на сайте http://www.eskimo.com/~turing/remailer/FAQ/. Некоторые из них имеют Web-интерфейс и позволяют отправлять анонимные сообщения с помощью Web-броузера (например https://riot.eu.org/anon/remailer.html.en), но принимать электронную почту анонимно таким образом невозможно.

Столь популярные бесплатные почтовые службы (Mail.ru, Hotmail, Yahoo и др.), как правило, не защищены от контроля со стороны провайдера и имеют ограниченный размер почтового ящика - обычно несколько мегабайт. Большинство из них также не позволяют получать почту автоматически с помощью программ почтовых клиентов (Outlook Express, The Bat!, и др.).

Разумный компромисс - использование недорогих платных услуг шифрованной электронной почты. В Интернете можно найти немало таких компаний, например Hushmail, Securenym, Cotse и др. При этом даже нет необходимости устанавливать на ваш компьютер PGP. Все необходимые для этого программные средства уже существуют в стандартной поставке MS Windows. Наилучший результат можно достичь, совмещая услуги таких компаний с шифрованием почты с помощью PGP. В этом случае вам не придется полагаться на добросовестность

Впервые услуги шифрованной анонимной почты начала предоставлять компания Hush Communications (www.hush.com). Недорогой сервис несколько омрачается необходимостью загружать обьемистые Java-апплеты для работы с почтой. Услуги компании Securenym немного дороже, но они удобнее и лучше согласуются с другими средствами связи. Пожалуй, наиболее полный комплекс платных услуг по обеспечению анонимности и конфиденциальности предоставляет компания со странным названием Church of the Swimming Elefant (Церковь Плавающего Слона). Ее сайт можно найти по адресу www.Cotse.com. Стоимость общего комплекса услуг составляет $6 в месяц, что несколько выше чем у аналогичных компаний. Но за эту цену вы получите анонимный шифрующий прокси-сервер, ящик электронной почты с шифрованным доступом, анонимные ремейлеры с Web-интерфейсом, анонимный доступ к Usenet, 50 мегабайт дискового пространства для хранения данных или размещения Web-страницы и огромное количество самой свежей информации по компьютерной безопасности.

Один из вариантов построения системы конфиденциальной электронной почты приведен на Рис. 1.



Телефаксная связь

Современные средства перехвата телефаксных сообщений позволяют запросто копировать сообщения, проходящие по обычным телефонным каналам. Несколько сложнее, но все же возможно, перехватить сообщение таким образом, чтобы оно не дошло до адресата, но у отправителя сложилось впечатление, что оно было отправлено. Очевидно, что значимая для вероятного противника информация заключается как в тексте сообщения, так и в данных об отправителе и получателе.

Решать проблему конфиденциальности этой информации можно различными путями. Наилучший из них - отказаться от телефаксной связи вовсе. Интернет технологии позволяют передавать те же документы более качественно, конфиденциально и намного дешевле. Однако, на практике нередки случаи, когда воспользоваться факсом совершенно необходимо, например, если ваш корреспондент не использует Интернет. И снова на помощь приходят Интернет технологии и криптография.

Основой всех систем отправки и получения факсовых сообщений, которые используют технологии Интернет, являются факсовые шлюзы. Факсовый шлюз, это компьютер, который с одной стороны подключен к Интернету, а с другой стороны, через факс-модем подключен к телефонной сети.

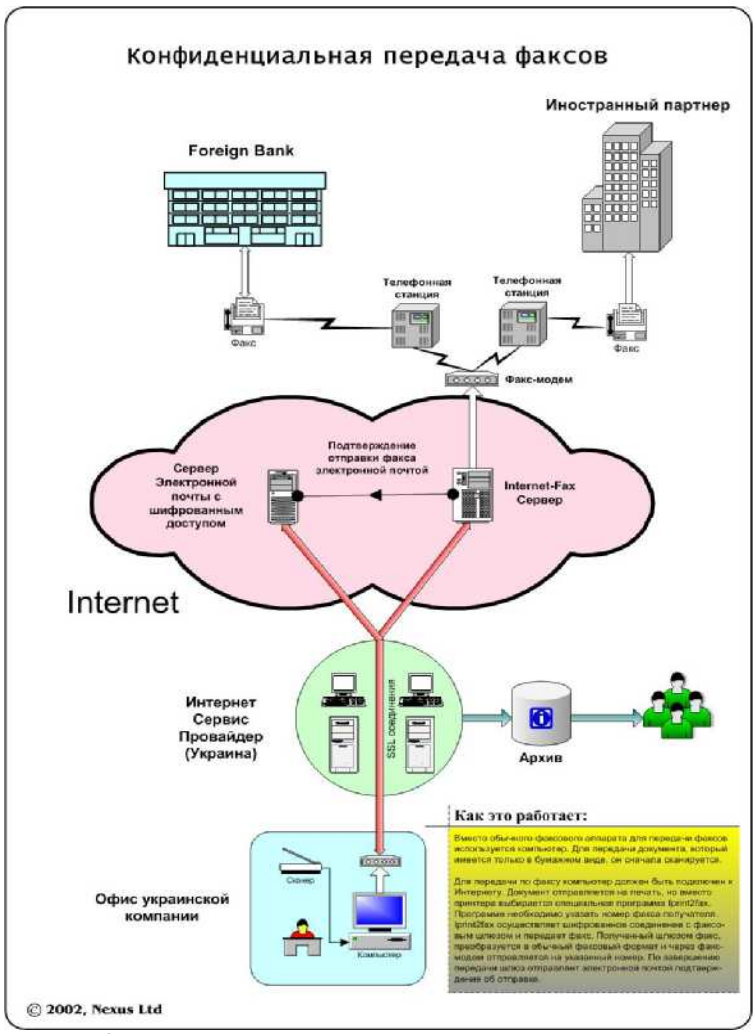
Рассмотрим практические схемы конфиденциальной и анонимной доставки телефаксных сообщений.

Передача телефаксных сообщений

В мире насчитывается около десятка компаний, обеспечивающих доставка факсовых сообщений с использованием Интернет технологий. По сведениям автора,

лишь три из них обеспечивают шифрованный обмен между компьютером клиента и факсовым шлюзом Faxsav, Telus Internet Fax и Quicknet.

Рис.2 иллюстрирует работу системы доставки факсов с шифрованным каналом



связи между клиентом и факсовым шлюзом.

Вместо обычного факсового аппарата для передачи факсов используется компьютер, подключенный к Интернету. На компьютере устанавливается специальная программа, которую бесплатно предоставляет компания, обеспечивающая доставку факсов. Для передачи документа, который имеется только в бумажном виде, он сначала сканируется. Для отправки документа по факсу он отправляется на печать, но вместо принтера выбирается программа доставки факсов. Программе необходимо указать номер факса получателя. Программа автоматически осуществляет шифрованное соединение с факсовым шлюзом и передает факс. Полученный шлюзом факс, преобразуется в обычный факсовый формат и через факс-модем отправляется на указанный факсовый номер.

Помимо конфиденциальности такой способ доставки факсов имеет и другие преимущества:

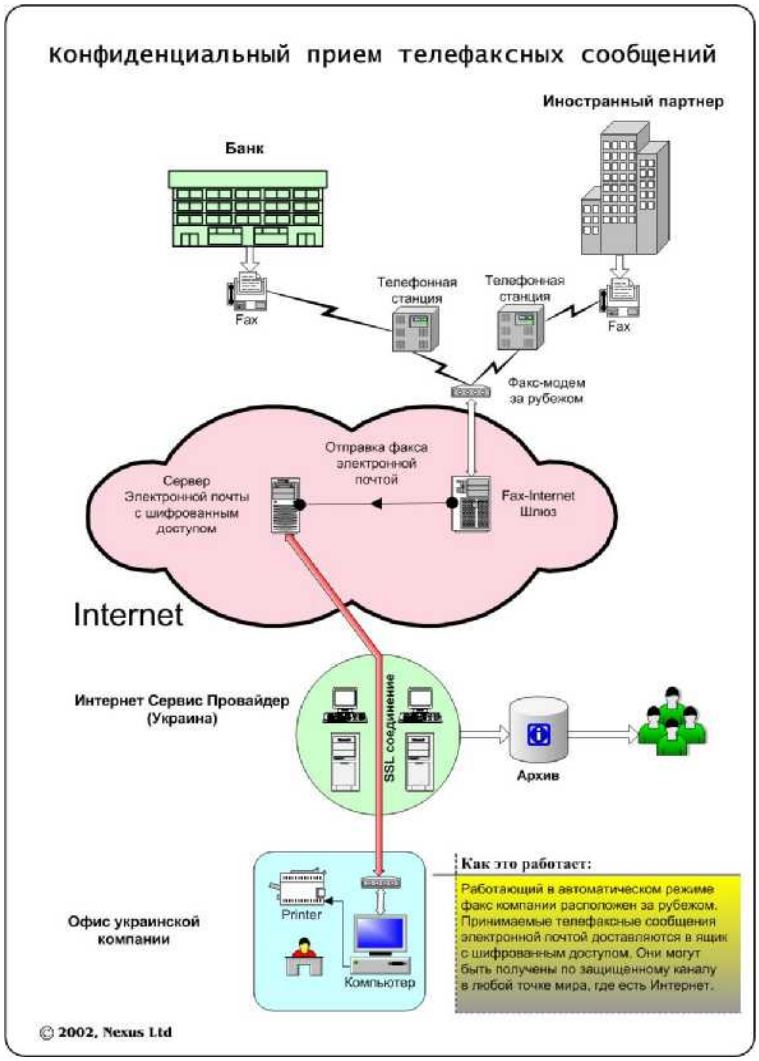
а) Высокое качество, поскольку по обычным телефонным линиям сообщения, как правило, передаются в пределах страны получателя.

б) Низкая стоимость. В десятки раз дешевле прямой отправки и зачастую намного дешевле IP-телефонии.

в) Экономия времени и бумаги, т.к. созданные на компьютере документы для отправки факсом печатать не нужно.

Прием телефаксных сообщений

Для конфиденциального приема факсов и голосовых сообщений используются услуги компаний, предоставляющих номера телефона в различных городах мира. Таких компаний в настоящее время работает несколько. Наиболее известная из них - J2.com. Общий принцип их услуг проиллюстрирован на Рис.3.



В различных городах мира компания приобретает телефонные номера. К этим номерам подключаются факс-модемы/автоответчики, соединенные с факсовым шлюзом. Только теперь шлюз работает в другом направлении. Принимаемые факсы и голосовые сообщения отправляются электронной почтой в виде присоединенных файлов на адрес электронной почты, который указывает клиент, арендующий данный номер телефона. Стоимость аренды номера составляет от $5 до $20 в месяц и, как правило, не зависит от количества принимаемых сообщений. Если в качестве адреса электронной почты указать адрес, предоставленный провайдером или бесплатный адрес с нешифрованным доступом, то это позволит провайдеру (и не только) получить доступ к содержимому факсовых и голосовых сообщений. Если же сообщения направить в ящик с доступом по шифрованному каналу, то ваши сообщения в безопасности. Время доставки факса до конечного получателя обычно не превышает нескольких минут.

Безопасность и анонимность Web-броузинга

Путешествуя по Интернету, вы оставляете очень много различной информации о себе и своих действиях. Вот далеко неполный перечень опасностей, которые вас могут подстерегать: Сайты, которые вы посещаете очень часто, собирают определенную информацию о вас. Они также могут загружать на ваш компьютер некоторые программы, которые там могут находиться и выполнять определенные действия. Злоумышленники

создают страницы со специальным кодом, который может заражать ваш компьютер вирусами и открывать доступ к файлам на вашем компьютере. Кроме того, ваш Интернет-провайдер может легко наблюдать за всеми вашими действиями и иметь о них полную информацию.

Защиту от возможного проникновения злоумышленников в ваш компьютер обеспечивают: своевременное обновление программного обеспечения, применение брандмауэров и антивирусных программ. В данной статье они не рассматриваются.

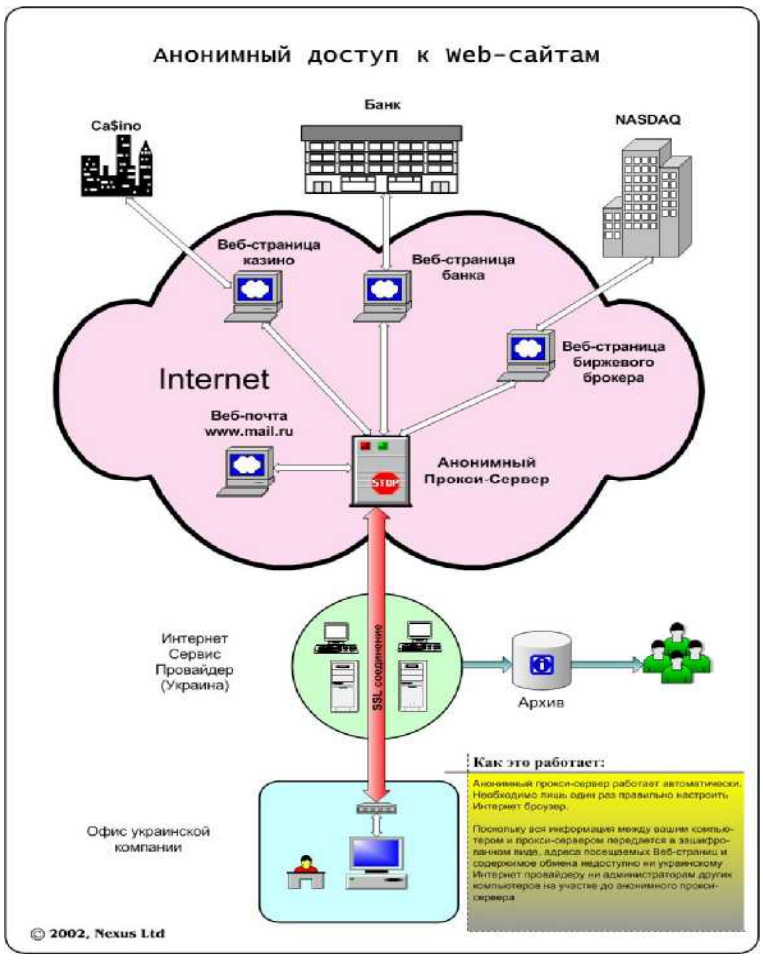
Довольно часто пользователей не беспокоит то, что владельцы посещаемых сайтов собирают о них информацию и то, что провайдер может наблюдать за их действиями. Однако, в ряде случаев это совсем нежелательно.

Одно из решений проблемы анонимности и конфиденциальности заключается в использовании прокси-серверов. Это специальным образом настроенные компьютеры в сети Интернет, которые пропускают через себя весь поток данных между вашим компьютером и другими Интернет сайтами, подменяя при этом ваш IP-адрес своим. Регулярно обновляемые списки анонимных прокси-серверов можно получить, например, на сайте http://des.tora.ru/service/proxy.htm или http://www.samair.ru/proxy/. Убедиться в реальной анонимности выбранного прокси-сервера можно с помощью бесплатных инструментов доступных на сайте http://tools-on.net/. Существуют также специальные программы, которые автоматически ищут, проверяют и используют бесплатные анонимные прокси-серверы. Одна из них – Internet Anonym (www.steganos.com)

Однако даже анонимный прокси-сервер не защищает вас от контроля со стороны вашего Интернет-провайдера. Защиту обеспечивают шифрующие анонимные прокси-серверы. Это серверы, соединение с которыми осуществляется по каналу, защищенному криптографическим протоколом SSL. Если прокси-сервер использует этот протокол ваш Интернет браузер перейдет в защищенный режим автоматически. Убедиться в этом можно посмотрев на правый нижний край окна Интернет Эксплорера[1]. В защищенном режиме там появится изображение замка желтого цвета.

Из многих тысяч бесплатных прокси-серверов в Интернете всегда можно найти такой, который удовлетворяет вышеуказанным требованиям, т.е. подмена IP-адреса клиента своим и шифрование входящего трафика. Однако в некоторых случаях более оправдано использование платных прокси-серверов, например, когда нужна высокая скорость соединения. Надежность платных серверов, обычно, выше, поскольку их бесперебойная работа залог стабильного дохода владельца. Наиболее известный из них Anonymizer.com (www.anonymizer.com). Рис.4 иллюстрирует работу анонимного шифрующего прокси сервера.

[1] Крипографический протокол SSL поддерживают и другие популярные Интернет броузеры, Opera и Netscape Communicator.



Заключение

В целом проблема безопасности и конфиденциальности весьма сложна и многогранна. Автор не претендует на полное изложение даже тех ее аспектов, которые вынесены в оглавление этой статьи. Тем не менее, все описанные здесь технологии испытаны и используются в реальных условиях.

Некоторые полезные ссылки:

Общая информация по компьютерной безопасности
kiev-security.bigmir.net
www.epic.org
www.bezpeka.com/library
www.ssl.stu.neva.ru/psw/
Общая информация по сетевой безопасности на русском языке
securitylab.ru
Международный сайт программы PGP
www.pgpi.com
Российский сайт программы PGP
www.pgpru.com/
Анонимные прокси-серверы
www.samair.ru/xwww/proxy.htm
Анонимные Web-ремейлеры
https://riot.eu.org/anon/remailer.html.en
Проверка анонимности прокси-сервера и много других полезных услуг.
tools-on.net