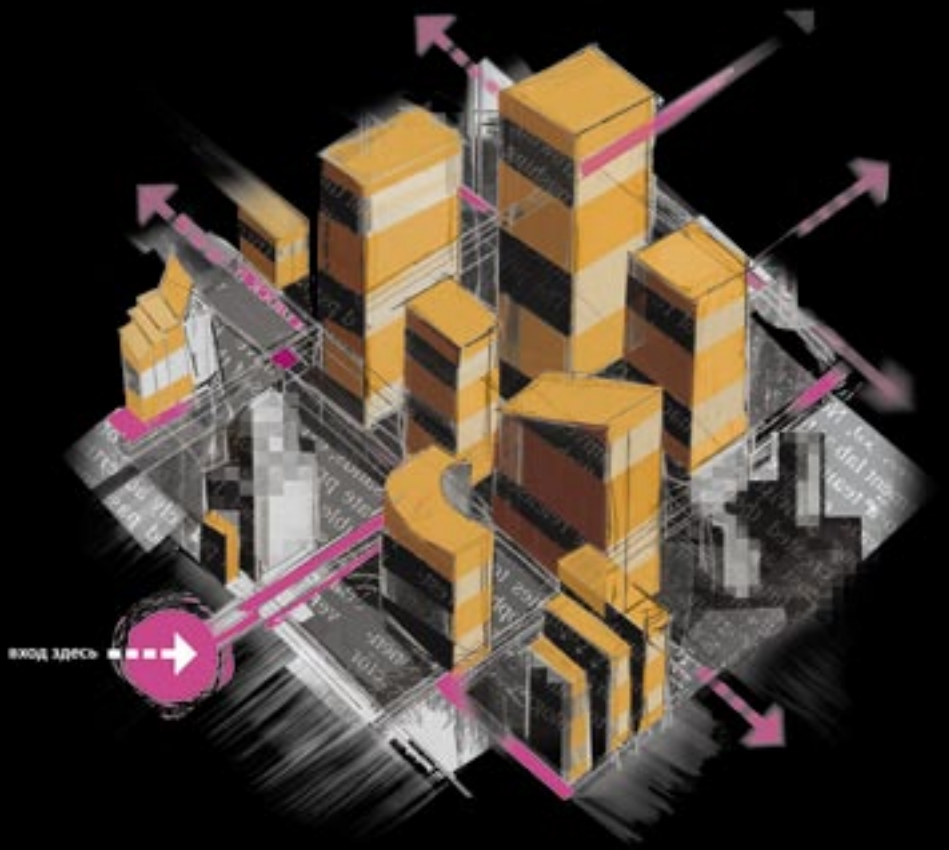


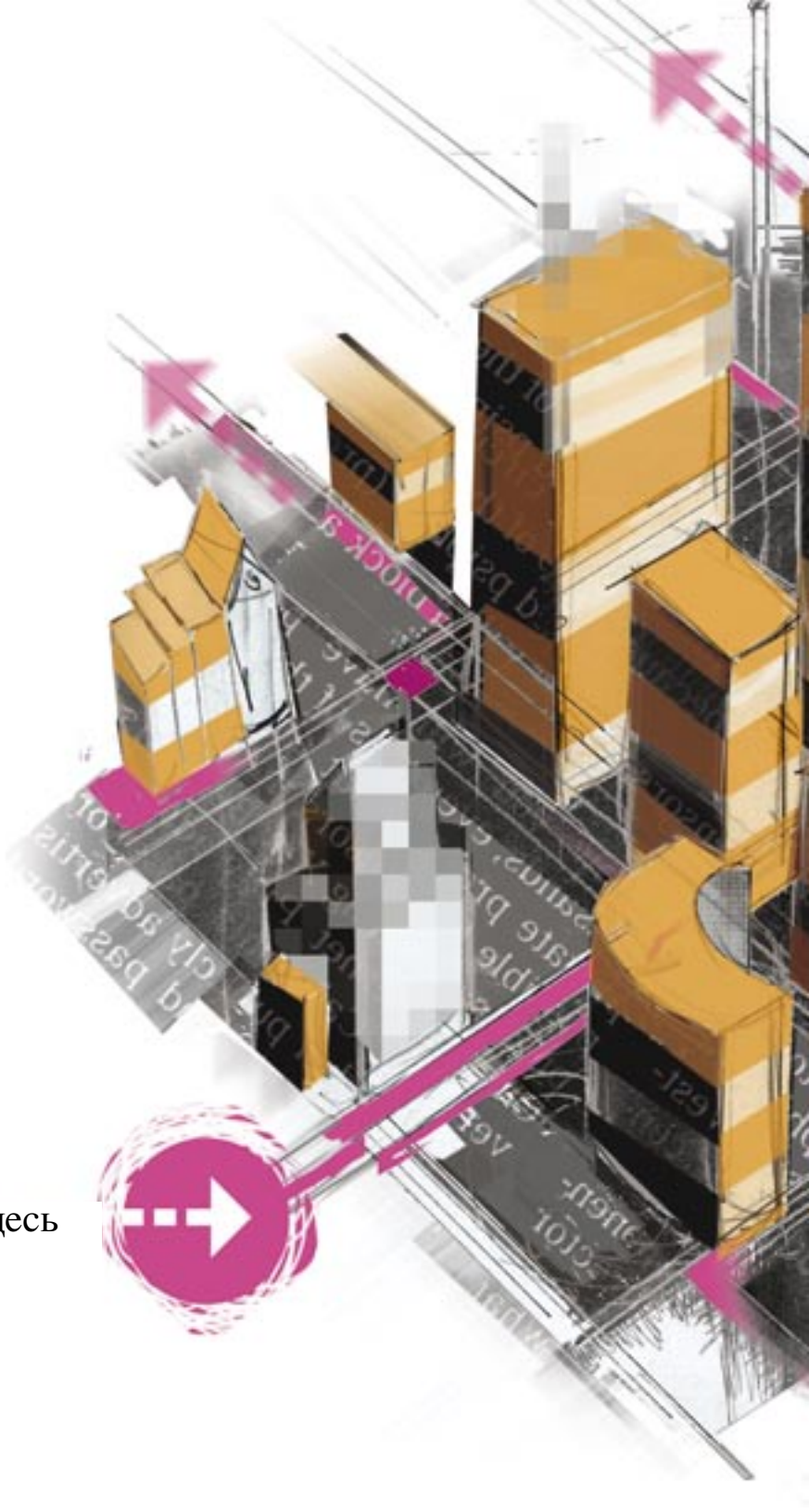

# Справочник по обходу Интернет цензуры

# для всех

**Проект Civisec**

The Citizen Lab
The University of Toronto
September, 2007

Иллюстрации Джейн Гоуан



# Глоссарий

# Глоссарий

## Технологии обхода

Технологии обхода это любые программные средства, программное обеспечение или методы, используемые для обхода Интернет фильтрации. Эти средства разнообразны от сложных компьютерных программ до относительно простых действий вручную, например, организовать доступ к запрещенному веб-сайту, хранящемуся в кэше поискового сервера, вместо того, чтобы пытаться получить прямой доступ.

## Провайдеры обхода

Провайдеры обхода устанавливают программное обеспечение на компьютере в фильтрующемся месте и организуют подключение к этому компьютеру для тех, кто имеет доступ к Интернету с места, подверженного цензуре. Провайдерами обхода могут быть и крупные коммерческие организации, предлагающие платные услуги по обходу, и частные лица, предоставляющие услуги по обходу бесплатно.

## Пользователи обхода

Пользователи обхода – это частные лица, которые используют технологии обхода, чтобы избежать фильтрации Интернет-контента.

# Введение

Интернет-цензура или фильтрация контента стали основной мировой проблемой.

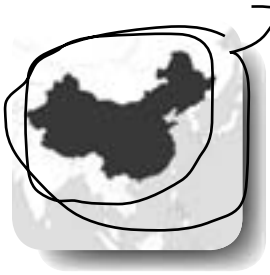
Хотя когда-то согласно исследованию OpenNet Initiative (http://opennet.net) предполагалось, что государства не смогут контролировать Интернет связь, в настоящий момент более 25 стран практикуют Интернет-цензуру. В странах с широко распространенной политикой фильтрации жители сталкиваются с регулярной блокировкой доступа к веб-сайтам организаций по защите прав человека, новостей, блогам и веб-услугам, которые оспаривают статус-кво или считаются угрожающими или нежелательными. Другие блокируют доступ к отдельным категориям Интернет-контента или периодически к определенным веб-сайтам или сетевым службам. Такая блокировка совпадает с политическими событиями выборы или общественные демонстрации.

Хотя некоторые государства принимают законопроекты по Интернет-фильтрации, многие делают это с недостаточной прозрачностью и отчетностью перед обществом, или же при отсутствии их. Большинство государств не показывают, какая информация блокируется, и в редких случаях присутствуют механизмы проверки или выражения претензий со стороны пострадавших граждан или издателей контента. Рост использования коммерческого программного обеспечения фильтрации, которое по причине несовершенной категоризации склонно чрезмерно блокировать контент, усложняет проблему. Коммерческие фильтры блокируют доступ к группированным спискам веб-сайтов, которые согласно праву собственности даже хранятся в секрете для самих клиентов. Как следствие, частные компании без ответственности определяют правила цензуры в политической ситуации, где государство в незначительной степени подотчетно обществу или контролю. Например, коммерческое фильтрующее программное обеспечение используется для Интернет-цензуры в Бирме, Тунисе, Йемене, Саудовской Аравии и Иране.

Данное руководство предназначено для ознакомления простых пользователей, не обладающих специальными техническими навыками обхода Интернет-цензуры и помогает им выбрать те системы, которые лучше всего подходят к их условиям и потребностям.

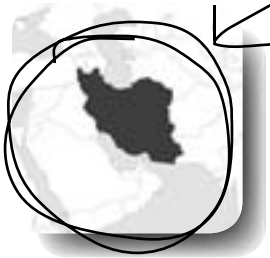
# Примеры из реальной жизни

Фильтрация Интернет-контента различается по странам.



## КИТАЙ

В Китае правительство контролирует доступ к Интернет-контенту и онлайн публикациям при помощи комбинации методов технической фильтрации и исчерпывающих правил и руководств. Техническая фильтрация осуществляется главным образом на национальном магистральном уровне, где запрос информации фильтруется по запрещенным IP (Интернет-протокола) адресам и ключевым словам. Китайская централизованная система фильтрации контента, зачастую непоследовательная, обеспечивает постоянное блокирование доступа всей страны к веб-сайтам по защите прав человека, оппозиционных политических движений, Тайваньской и Тибетской независимости, международным новостям и прочим. Процесс Интернет-фильтрации непрозрачен, а процесс подотчетности общественности отсутствует.



## ИРАН

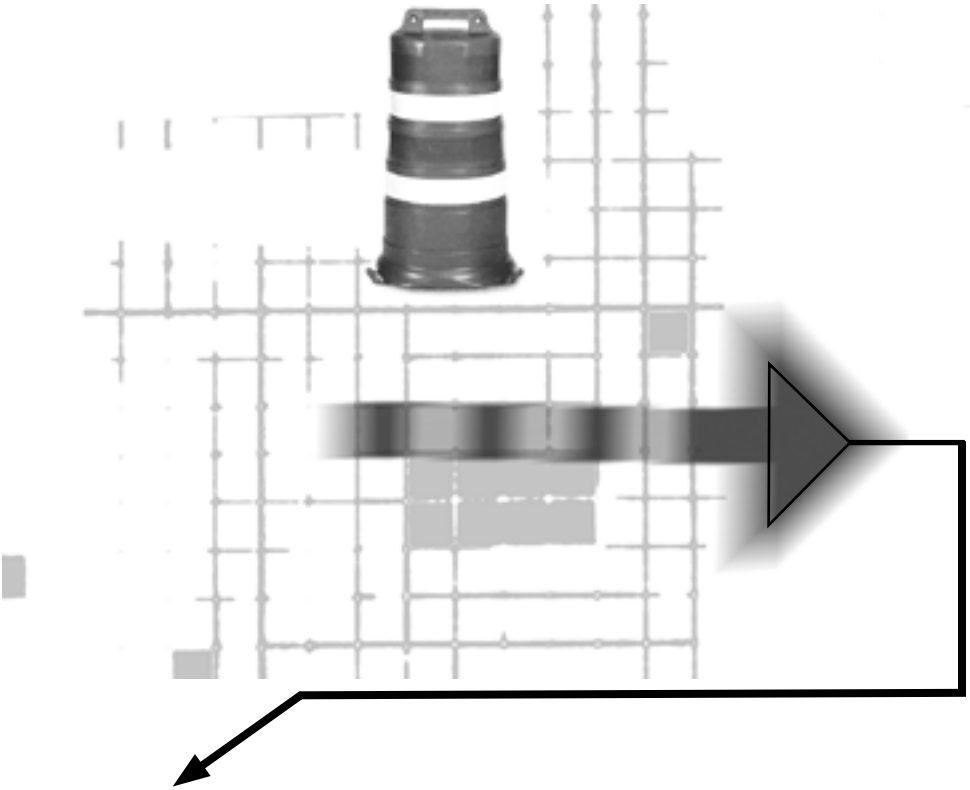
В Иране нет общенациональной системы фильтрации. Вместо этого, провайдеры Интернет-услуг (ISP) несут ответственность за осуществление цензуры согласно подробно разработанным правительственным инструкциям. Отдельные ISP выбирают фильтрацию с помощью американского коммерческого программного обеспечения фильтрации, в то время как другие используют ручные методы. Пользователи, имеющие доступ к Интернету через разных ISP, могут сталкиваться со значительными различиями в доступе к веб-сайтам. Иран использует данную систему для фильтрации контента на иранском и персидском/фарси языках, критикующего режим, включая политические сайты, контент о гомосексуалистах и лесбиянках, сайты по защите прав женщин, потоковые мультимедийные средства и блоги. В то время как в правительстве идут дебаты, открыто признающие и обсуждающие политику фильтрации Интернет-контента, имеется незначительная прозрачность по контенту, который подвергается фильтрации.

## США

В США государственные учреждения (например, школы и библиотеки) по закону (Закон «О защите детей в Интернете» – CIPA) должны использовать программное обеспечение фильтрации, чтобы блокировать доступ к непристойным, порнографическим и другим материалам, связанным с сексуальной эксплуатацией детей. Большинство осуществляет политику фильтрации при помощи коммерческих технологий фильтрации, которые могут содержать неправильную категоризацию и ошибки. Исследователи обнаружили, что коммерческие фильтрующие технологии ошибочно блокируют доступ к контенту, связанному с женским здоровьем, группами по защите прав гомосексуалистов и лесбиянок, а также сексуальным образованием для подростков.

## Введение
(продолжение)

Несмотря на данную растущую глобальную проблему, жители по всему миру ищут пути обхода правительственных фильтров и реализуют фундаментальные права человека на доступ к информации по своему усмотрению.



Используемые средства, методы и стратегии по обходу фильтрации Интернет-контента относятся к так называемым *технологиям обхода*.

Существует множество технологий обхода, которые могут использоваться в различных обстоятельствах разнообразными потенциальными пользователями. Ни одна технология не подходит одинаково разным потенциальным пользователям и обстоятельствам, в которых они находятся. Мы считаем, что лучше думать о технологиях обхода прагматично, как о средствах в инструментарии. Одни инструменты лучше для определенной работы, чем другие, или требуют других уровней квалификации, чтобы эффективнее выполнить задачу. Таким же образом, подход к каждой технологии обхода должен выражаться в том, насколько он соответствует специфическим проблемам пользователя, обстоятельствам и набору навыков.

# Выбор технологии обхода

Технологии обхода часто направлены на разных пользователей с разными ресурсами и уровнями мастерства. То, что может хорошо сработать по одному сценарию, не всегда лучший вариант для другого.

При выборе технологии обхода важно, чтобы потенциальный провайдер обхода и пользователь определили, что будет лучше работать в данной ситуации. Решение об использовании технологии обхода должно приниматься со всей серьезностью, при тщательном анализе специфических потребностей, доступных ресурсов и из соображений безопасности для всех вовлеченных людей. Существует широкий ряд технологий, доступных тем пользователям, которые хотят обойти Интернет фильтрацию. Однако, их использование для успешной и стабильной услуги обхода зависит от ряда факторов, включая уровень технических навыков пользователя, потенциальный риск безопасности и доступная связь за пределами цензурированной территории. Мы опишем некоторые общие размышления о выборе технологий обхода для потенциальных пользователей и затем для их провайдеров.

**Вы пользователь**

**или**

**провайдер обхода?**

# Выбор технологии обхода

(продолжение)

## Вопросы для размышления пользователем обхода: что, где, как?

### Вы хотите иметь доступ к Интернету или размещать информацию?

Несмотря на тесную связь, доступ к запрещенному контенту, в противоположность его размещению, может затрагивать различные риски, стратегии и технологии для пользователя. Мы создали отдельное руководство для тех, кто хочет обойти Интернет цензуру при размещении онлайн информации.

### Вы имеете доступ к Интернету со своего персонального компьютера или компьютера общественного пользования?

Доступ к Интернету с вашего домашнего компьютер или компьютера общественного пользования в Интернет кафе, или же в публичной библиотеке сопряжен рядом различных факторов и представляет ряд возможностей для обхода. Например, у пользователей, подключающихся к Интернету с общественных компьютеров или в Интернет кафе, может отсутствовать возможность установить какое-нибудь программное обеспечение, и они будут ограничены онлайновыми решениями. Другие могут захотеть использовать приложения помимо просмотра веб-страниц (HTTP), такие как электронная почта (SMTP) и передача файлов (FTP), и таким образом они могут пожелать установить программное обеспечение на их компьютерную рабочую станцию и настроить компьютерные установки. На ваш персональный компьютер вы можете установить любое программное обеспечение на ваш выбор, которое вы не сможете установить на общественном Интернет-терминале. Однако это может вызвать дополнительные риски, так как есть доказательство использования технологий обхода на вашем компьютере, что может повлечь ответственность, если на компьютер будет наложен арест правоохранительными органами.

Общественный доступ к Интернету может обеспечить анонимность в отличие от личного компьютера, несмотря на то, что некоторые требуют от посетителей идентификации личности, либо наблюдают за работой посетителя. Пытаетесь ли вы обойти цензуру у себя дома или с общественного терминала, всегда важно понимать условия поставляемой услуги в полной степени.

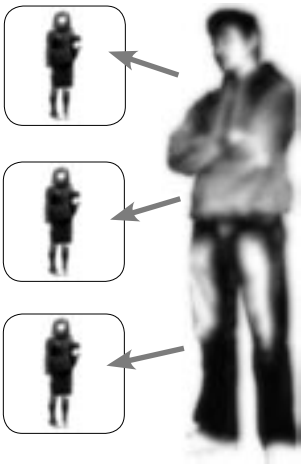
# Выбор технологии обхода

(продолжение)

## Вопросы для размышления пользователем обхода

кого вы знаете?

Есть ли у вас какие-либо связи или надежные контакты (например, друзья, члены семьи, коллеги) за пределами страны?



Так как обход Интернет-цензуры включает в себя подключение к компьютеру, находящемуся за территорией цензуры, важный фактор, который следует учесть, это знаете ли вы и доверяете ли кому-либо или группе, находящейся вне страны, желающей предоставить вам услуги обхода. Многие пользователи, которые обходят цензуру, делают это, подключаясь к открытым общественным прокси-компьютерам, информация о подключении к которым в какой-то мере афишируется. Пользователи должны помнить, что по самому определению, такие компьютеры небезопасны, так как пользователь никогда не может быть уверен, что противник не установил ловушку или «систему-ловушку», чтобы заманить диссидентов.

Самый лучший вариант, если вам установит подключение кто-нибудь, кого вы знаете и кому доверяете, однако это тоже не обойдется без рисков и последствий. Провайдеры могут следить за всем, что вы делаете в режиме он-лайн, включая все сайты, которые вы посещаете. Вот почему необходимо, чтобы вы полностью доверяли лицу или организации, предоставляющей вам услуги обхода. Успешный, долгосрочный и стабильный обход значительно улучшается, если есть надежное контактное лицо, в том районе/местности, где фильтрация отсутствует.

Готовы ли вы платить и доверять третьему лицу/организации, чтобы получить доступ или размещать информацию в Интернете?

Если у вас нет надежных друзей и членов семьи за пределами вашей страны, тогда вы можете довериться третьим лицам. Существует много коммерческих провайдеров, которые предоставляют услуги обхода за определенную плату. Если вы можете позволить себе этот вариант, будьте осторожны с условиями обслуживания и политикой конфиденциальности. Коммерческие службы могут предложить анонимность в Интернете, но не анонимность самого коммерческого провайдера. Коммерческие службы могут передать все записи и вашу личную информацию, если их принудят к этому на основании закона.

# Выбор технологии обхода

(продолжение)

## Вопросы для размышления пользователем обхода

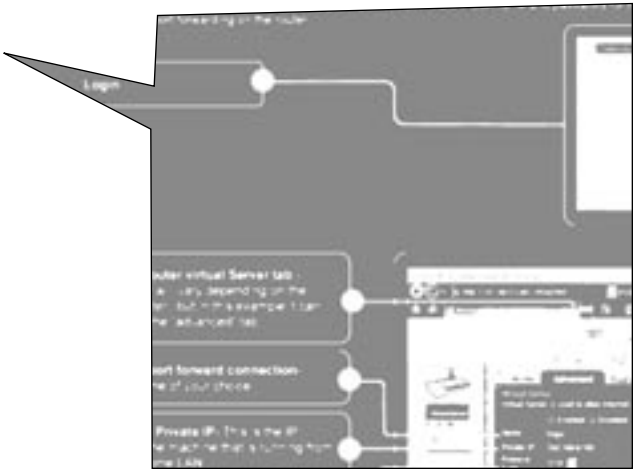
что вы знаете?

Каков уровень вашей технической квалификации? Считаете ли вы себя неопытным пользователем компьютера, средним или опытным пользователем?

Чем выше уровень вашей технической грамотности, тем больше вариантов обхода. Некоторые пользователи могут считать установку, процесс настройки и применения технологий обхода слишком затруднительным, или выше уровня их квалификации. Хотя, всегда можно найти время и научиться пользоваться даже самым сложным программным обеспечением, будьте осторожны – некорректная установка и использование технологий обхода может представлять для вас значительный риск.

Какой язык применим/ предпочтителен для вас? Нужны ли вам технологии не на английском языке?

Большинство технологий обхода разработаны с пользовательским интерфейсом и инструкциями на английском языке, хотя многие могут предложить версии их систем и руководство для пользователя на других языках. Если вы работаете с переведенным руководством для пользователя, убедитесь, что перевод, который, вы используете, совпадает с версией программного обеспечения, на котором вы работаете.

# Выбор технологии обхода

(продолжение)

## Вопросы для размышления пользователем обхода

Безопасность и гарантия

Вы хотите получить доступ к контенту, который считается чрезвычайно важным и рассматривается как угроза безопасности той стране, в которой вы проживаете?

Были ли прецеденты арестов за использование обхода Интернет-цензуры в вашей стране?

Не состоите ли вы в оппозиционных группах/сообществах, за которыми ведется наблюдение?

Доступ к запрещенному контенту может быть серьезным нарушением закона, особенно если информация, которую вы просмотрели, считается угрозой национальной безопасности. Если вы постоянно имеете доступ к данному виду контента, вам следует выбирать те технологии обхода, которые предлагают большую анонимность и безопасность. Однако, обычно есть выбор между простотой в использовании и безопасностью. Поэтому будьте готовы потратить дополнительное время и усилия, чтобы уменьшить риски.

Если вы связаны с оппозиционными или дисседентскими группами/сообществами, тогда вы можете находиться в списке лиц, за которым наблюдает ваше правительство, и вы должны предпринять дополнительные меры предосторожности, тщательно выбирая технологию обхода. Вы можете предположить, что за вами наблюдают, и ваш компьютер может быть конфискован в любое время. Избегайте технологий обхода, требующих установки на ваш компьютер. Если это возможно, подключайтесь к Интернету через ряд различных анонимных общественных терминалов.

# Выбор технологии обхода

(продолжение)

## Вопросы для размышления пользователем обхода
личность/персона

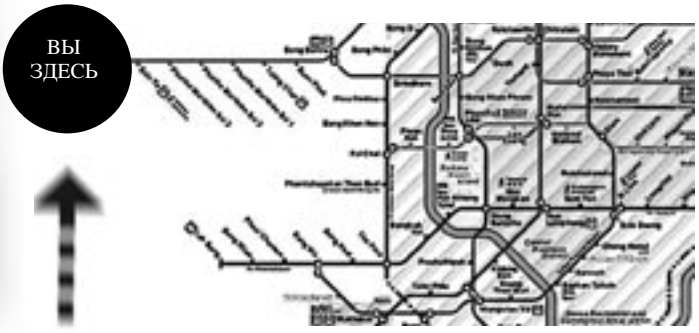
Является ли защита вашей личности в режиме он-лайн задачей первостепенной важности? Хотите ли вы перемещаться по сети и/или размещать информацию анонимно?

Обход и анонимность отличаются друг от друга. Анонимные системы защищают вашу личность от веб-сайта, к которому вы подключаетесь, и от самой анонимной системы. Они могут быть использованы для обхода, но не разработаны специально для этой цели и поэтому могут быть легко заблокированы. Системы обхода разработаны для того, чтобы обойти блокирование, но не защитить вашу личность от провайдера обхода.

Не принимайте открытые общественные прокси-серверы за анонимные системы, они не являются такими. Несмотря на то, что они могут не запрашивать личную информацию, они могут видеть и записывать месторасположение компьютера, с которого вы подключаетесь и все веб-сайты, которые вы посетили через них.

Коммерческие службы, рекламирующие анонимное перемещение, все же могут записывать информацию о подключении и веб-сайты, которые вы посетили. Убедитесь, что вам понятны условия их использования.

Есть несколько стратегий, которым вы можете следовать, если хотите анонимно размещать информацию в режиме он-лайн. Компания «Citizen Lab» разработала специальное руководство по обходу для опубликования он-лайн, которое включает в себя раздел по анонимному опубликованию.



# Выбор технологии обхода

(продолжение)

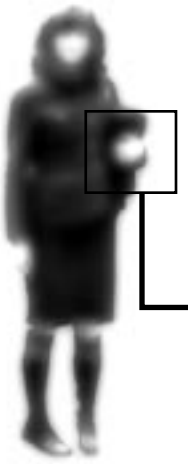
## Вопросы для размышления пользователем обхода

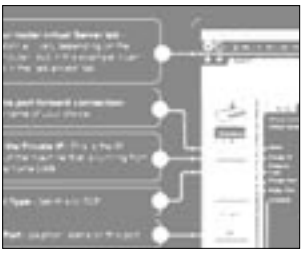
Безопасность прежде всего

**Установка технологий обхода для кого-то - лучший способ помочь другим реализовывать их фундаментальные права на доступ к информации и свободу слова. Однако, этот выбор сопряжен повышенной ответственностью и определенными условиями. Прежде всего, безопасность ваших пользователей должна стать вашей главной заботой.**

Каков ваш уровень технической квалификации? Считаете ли вы себя неопытным компьютерным пользователем, средним или опытным пользователем?

Установка и хостинг сервера с технологией обхода может отнимать много времени и является сложной задачей, в зависимости от системы обхода. Некоторые требуют загрузки и установки нескольких различных частей программного обеспечения. Почти все они потребуют определенной конфигурации, чтобы настроить вашу собственную сетевую среду. Если вы подключаетесь к Интернету через домашний маршрутизатор или брандмауэр, например, возможна некоторая перенастройка вашей системы обхода. Некоторые технологии обхода имеют очень четкую и полезную документацию и руководство пользователю, а у других они отсутствуют. Будьте уверенны, что вы выбираете ту технологию, которая совпадает с вашим уровнем навыков и возможностями, так как неправильная установка системы может нарушить безопасность вашего пользователя. Убедитесь также, что вы спокойно можете работать с вашей системой, так как устаревшая или постоянно прерывающаяся/сбивающаяся технология может мешать/препятсвовать и без нужды подвергать опасности пользователей, находящихся в местностях, на которые распространяется цензура.





# Выбор технологии обхода

(продолжение)

## Вопросы для размышления пользователем обхода

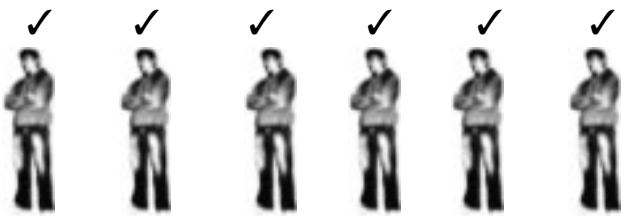
### Ваши пользователи

Какое количество пользователей вы ожидаете или желаете обслуживать, и какая у вас доступная пропускная способность?

Количество пользователей, которым вы даете возможность просматривать веб-сайты через ваш компьютер, повлияет на технологические возможности вашего компьютера и скорость подключения, затрагивая также не только то, что делаете вы, но и то, что могут делать пользователи системы обхода. Чем больше у вас пользователей, тем сложнее наблюдать за процессом пользования (если необходимо) и управлять их экаунтами. **Убедитесь, что вы предлагаете услуги обхода только тому количеству пользователей, с которым можете справиться вы и ваш компьютер.**

Что вы сможете позволить вашим пользователям через ваше подключение? Хотите ли вы знать к какой информации они получают доступ или что размещают? Что вы собираетесь делать с их записями посещения веб-сайтов?

Создание услуги обхода означает, что вы сможете наблюдать за любым процессом использования, которое проходит через систему. Наличие этой возможности означает, что вы можете принимать решение о том, какую информацию вы можете разрешить для получения или размещения вашими пользователями. Некоторые системы обхода легче справляются с этой функцией, но есть и те, которые даже не оставляют признаков активности пользователей на вашем компьютере. Вы должны решить для себя, какую информацию вы выберите для просмотра, архивирования, и (или) удаления. Если вы захотите избавиться от этой информации, убедитесь, что вы делаете это правильно, так как даже удаленная информация может оставить следы. Помимо всего, убедитесь, что вы сообщаете пользователям о вашем стандартном операционном процессе относительно информации, которую они оставляют на вашем компьютере, и о том, что они могут делать через вашу систему обхода. Четко сообщите пользователям о вашей политике.

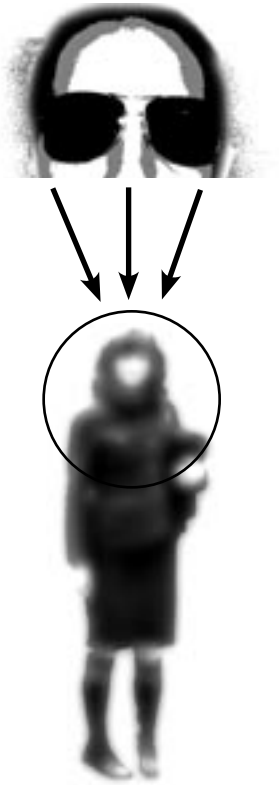


# Выбор технологии обхода

(продолжение)

## Вопросы для размышления провайдеру ОБХОДА: риски

Какие существуют потенциальные риски безопасности и правовые риски при хостинге технологий обхода? Ограничивает ли услуги такого рода ваш провайдер Интернет-услуг или правительство?



Риски хостинга технологий обхода не такие значительные, как для пользователей технологий обхода, но все же они имеются. Вы, скорее всего, несете ответственность за все, что делаете на вашем компьютере с помощью Интернет-подключения. Если кто-либо посещает веб-сайты или размещает незаконную информацию через вашу коммуникационную службу, вы можете понести ответственность. Менее вероятный, но тем не менее значительный риск касается того, что вы возможно станете целью/мишенью иностранных агентов страны, где предлагается ваша услуга. Убедитесь, что вы понимаете потенциальные риски безопасности и правовые риски при хостинге технологии обхода с точки зрения и вашего провайдера Интернет-услуг, и вашего правительства.

**Примеры из реальной жизни**

8 февраля 2006г. в 11:15ч. неизвестные лица насильно вошли в дом Питера Ян Ли в Атланте, США, штат Джорджия, связали его и избили, и ушли с несколькими лэптопами и другими файлами, принадлежащими ему. Питер Ян Ли, специалист по информационной технологии из Университета Принстон и практикующий специалист Falun Gong, поддерживал несколько форумов в США, где пользователи из Китая могли туннелировать национальные системы защиты безопасности (firewalls) для чтения и размещения информации о запрещенном религиозном движении. Хотя отсутствуют неоспоримые доказательства по его делу, г-н Ли считает, что лица, совершившее нападение, были тайными агентами Китайского правительства, попытавшиеся закрыть его службу.



# ОНЛАЙНОВАЯ СИСТЕМА ОБХОДА

Онлайновые системы обхода это специальные веб-страницы, которые дают возможность пользователям подать URL – адрес и заставить онлайновую программу обхода извлечь запрашиваемую веб-страницу. Отсутствует подключение между пользователями и запрашиваемой веб-страницей, так как программа обхода открыто передает через прокси запрос, позволяющий пользователям загружать заблокированные вебсайты без резких переходов. Так как веб-адреса общественных систем обхода широко известны, большинство Интернет фильтрующих приложений уже включают эти услуги в свои списки блоков, как делают многие страны, которые фильтруют на национальном уровне. Онлайновые системы обхода могли бы быть хорошим выбором для пользователей, подключаясь с ненадежным контактным лицом вне страны, предполагая, что страницы еще не заблокированы.

ПРИМЕЧАНИЕ: Хотя некоторые системы рекламируют себя как «анонимные», многие онлайновые системы обхода веб-сайтов не являются таковыми. Некоторые даже могут быть не шифрованными. Важно помнить, что шифрованные вебсайты начинаются с «https» и обозначаются символом открытого ключа в вашем веб-браузере, преобразуясь/переключаясь в позицию закрытого ключа. Если вы отправляете ваши веб-запросы нешифрованными, они могут быть легко перехвачены на любом шаге передачи, от вашего дома или офисного маршрутизатора к вашему провайдеру Интернет-услуг.

## ОНЛАЙНОВАЯ СИСТЕМА ОБХОДА: список

**Proxify**
**https://proxify.com/**

**StupidCensorship**
**https://stupidcensorship.com/**

это шифрованные, общественные, онлайновые системы обхода. Пользователь в цензурированной стране просто посещает один из веб-сайтов и потом вводит их назначение. Так как эти веб-услуги являются общественными, тем не менее они блокируются во многих странах и большинством фильтрующих приложений.



## ОНЛАЙНОВАЯ СИСТЕМА ОБХОДА: продолжение списка

**CGIProxy**
**http://www.jmarshall.com/**

это средство, которое используют большинство онлайновых систем обхода.
Частные онлайновые системы обхода превращают компьютер в персональный, шифрованный сервер, способный доставлять и отображать веб-страницы для пользователей сервера при удаленном доступе. Частные компании по онлайновым системам обхода включают поставщиков, которые устанавливают и применяют программное обеспечение на не цензурированной территории, и пользователей, которые пользуются услугой с территории, где Интернет проверяется. Поставщик систем обхода расширяет его/ее частную сеть, основанную на социальных связях доверия и частных коммуникаций, что осложняет нахождение и блокирование для цензоров.

**psiphon**
**http://psiphon.civisec.org/**

«psiphon» превращает обычный домашний компьютер в личный, шифрованный сервер, способный доставлять и отображать веб-страницы из любого места. Пользователь в не-цензурированной стране загружает программное обеспечение и устанавливает его на его/ее домашнем компьютере. «Psiphon» является бесплатным программным обеспечением с открытым исходным кодом под версии Linux и Windows. Эту программу легко установить и к ней прилагается очень подробное и понятное руководство для пользователя. Если ваш компьютер не включен в домашний маршрутизатор, может потребоваться определенная настройка конфигурации. После установки поставщик «psiphon» отправляет информацию о соединении пользователям на цензурированных территориях посредством наиболее безопасных инструментов. Цензурированный пользователь не должен устанавливать программное обеспечение, а только набирает URL-адрес в «голубом прямоугольнике (blue bar)». Это значит, что система обхода «psiphon» может быть доступна с любого места. Так как расположение компьютеров, включающих «psiphon» частное, для цензоров сложно найти их и заблокировать.

**Peacefire/Circumventor**
**http://peacefire.org/**

«Peacefire/Circumventor» - это система обхода почти схожая по принципу и методу с «psiphon». Однако, иногда ее трудно установить. Три различных пакета программного обеспечения должны быть загружены и установлены, и если ваш компьютер не имеет домашнего маршрутизатора, может потребоваться дополнительная конфигурация. Хотя «Peacefire/Circumventor» предоставляет помощь по установке, отсутствует подробное руководство для пользователя, в отличие от «psiphon». В других моментах «Peacefire/Circumventor» работает по тому же принципу, как и «psiphon».



# ТУННЕЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Туннелирование инкапсулирует одну форму трафика внутри других форм. Обычно, небезопасный, нешифрованный трафик туннелируется в шифрованное подключение. Обычные услуги на компьютере пользователя доступны, но работают через туннель к нефильтрованному компьютеру, который открыто направляет запросы пользователя и ответы. Пользователи с контактами в нефильтруемой стране могут установить частые туннельные услуги, а пользователи без таких контактов могут закупить коммерческие туннельные услуги. Туннельное программное обеспечение «ВЕБ» ограничивает туннелирование веб-трафиком, чтобы могли работать веб-браузеры, но не другие приложения. «Приложения» туннельного программного обеспечения позволяют туннелировать многочисленные Интернет-приложения, такие как электронная почта, клиентские программы и приложения мгновенного обмена сообщениями.

## ОНЛАЙНОВОЕ ТУННЕЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ: бесплатное

**UltraReach**
**http://www.ultrareach.com**

«UltraReach» создал противоцензурное программное обеспечение, известное как «Ultra-Surf». «UltraReach» предоставляет клиентскую программу для Windows, которую загружает пользователь в цензурированной стране (установка не требуется). Это бесплатное программное обеспечение, доступно на английском и китайском языках. После запуска, приложение открывается как приложение «Internet Explorer», которое автоматически конфигурируется, чтобы разрешить пользователю загружать веб-сайты через «UltraSurf». Другие браузеры должны конфигурироваться вручную. По умолчанию, подключение шифровано и применяются различные средства для обнаружения разблокированных IP адресов.

«UltraSurf» это прекрасный выбор для нетехнических пользователей, которые готовы доверять третьей стороне и которым необходим бесплатный веб-просмотр на хорошей скорости.

Так как веб-сайт «UltraReach» часто уже заблокирован в некоторых странах, пользователю на цензурированной территории, возможно, придется приобрести программное обеспечение через третью сторону. Даже если сайт может быть заблокирован, услуга все же доступна, так как предприняты меры, чтобы получать разблокированный IP адрес различными способами. Однако, даже это может блокироваться очень жестким цензором.



## ОНЛАЙНОВОЕ ТУННЕЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ: бесплатное

**FreeGate**
**http://www.dit-inc.us**

«Freegate» это противо-цензорная технология, разработанная DynaWeb, схожая во многом с UltraSurf. В отличие от UltraSurf, «Freegate» не шифрует URL по умолчанию. Если пользователи хотят шифровать URL запрос, им придется загружать другой пакет программного обеспечения и специально конфигурировать «Freegate».

«Freegate» - это хороший выбор для опытных пользователей, которым больше требуется сам обход, чем безопасность, и они доверяют третьей стороне, выполняют вручную конфигурации, и им необходим бесплатный веб-просмотр с хорошей скоростью.

Веб-сайт «Freegate» как и «UltraSurf» блокируется на многих цензурированных территориях, и поэтому пользователи должны получать программное обеспечение через третьи стороны. Также, сама услуга может быть заблокирована, хотя пользователи могут автоматически вставить незаблокированные IP адреса в «Freegate».

## ОНЛАЙНОВОЕ ТУННЕЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ: платное

**Anonymizer**
**http://anonymizer.com**

«Anonymizer» предоставляет клиентскую программу для Windows, которую устанавливает пользователь в цензурированной стране на компьютере. После завершения легкого процесса установки пользователь включает опцию «Anonymous Surfing (tm)» после чего трафик открыто туннелируется через «Anonymizer». Однако, для обеспечения безопасности пользователь должен запустить «Surfing Security (tm) SSL Encryption», чтобы весь поток трафика шифровался HTTPS/SSL. Этот вариант отключен по умолчанию. Программное обеспечение также представляет другие услуги, такие как «Digital Shredder», «Anti-Spyware» и одноразовые адреса электронной почты.

«Anonymizer» - это прекрасный выбор для пользователей, которые технически недостаточно подготовлены и готовы платить и доверять третьей стороне зашифрованный веб-просмотр на высокой скорости. Так как вебсайт «Anonymizer» часто блокируется на многих территориях, пользователю, возможно, придется приобрести программный продукт посредством третьей стороны. Хотя услуга все же доступна, несмотря на фильтрование веб-сайта, услуга сама по себе может быть легко заблокирована жестким цензором. Так как должно устанавливаться приложение, возможно это не подходит для общественных терминалов или пользователей с высоким уровнем риска, чьи компьютеры могут быть захвачены.



## ОНЛАЙНОВОЕ ТУННЕЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

платное

**Ghost Surf**
**http://tenebril.com**

«GhostSurf» предоставляет клиентскую программу для Windows, которую устанавливает пользователь в цензурированной стране на компьютерах. После окончания установки программное обеспечение автоматически проводит настройку конфигурации браузера Internet Explorer. Все другие браузеры должны конфигурироваться вручную. Программное обеспечение установлено по умолчанию на «обычный» режим, означая, что трафик является простым текстом и легко блокируется. Для шифрования трафика пользователь должен изменить этот параметр на «Безопасный», самый высший параметр (параметр «Анонимный» обманчивый, только блокирует кукис, но не делает трафик анонимным). После того, как программное обеспечение конфигурировано на параметр «Безопасный» и пользователь модифицирует установки браузера, в случае не использования Internet Explorer, трафик пользователя шифруется и направляется через серверы «GhostSurf».

«GhostSurf» - хороший выбор для тех, кто технически грамотен и желает заплатить и доверять третьей стороне за быстрое подключение.

Как и в «Anonymzer», так как веб-сайт «GhostSurf» часто блокируется во многих странах, пользователю, возможно, придется приобрести программный продукт через третью сторону. Хотя услуга все же доступна, несмотря на фильтрование веб-сайта, услуга сама по себе может быть легко заблокирована жестким цензором. Так как должно устанавливаться приложение, возможно, это не подходит для общественных терминалов или пользователей с высоким уровнем риска, чьи компьютеры могут быть захвачены.

### WSIS В ТУНИСЕ

### Примеры из реальной жизни

Всемирная встреча на высшем уровне по вопросам информационного общества II (WSIS) прошла в г. Тунисе (Тунис) в 2006г. Тунис сильно фильтрует доступ к контенту, включая веб-сайты, важные для государственных отчетов по правам человека.

Встреча WSIS была проведена в здании, где были две секции, каждая с различными протоколами доступа к Интернет. В секции с официальным процессом, доступ к Интернету не фильтровался. В отдельной секции, предназначенной для НПО и журналистов, доступ к Интернету регулировался тунисским Интернет-провайдером, который значительно фильтровал содержание при помощи американского коммерческого программного продукта Smartfilter

НПО из будки, расположенной на фильтруемой части, установила прокси с туннелем SSH-D к домашнему компьютеру, расположенному в Нидерландах. Затем НПО сообщила членам о номере порта браузера, давая возможность обойти фильтрование Тунисской стороной.



## ТУННЕЛЬНОЕ ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:
бесплатное

**GPass**
**http://gpass1.com/**

«GPass» предоставляет клиентскую программу для Windows, которую загружает (есть альтернативная установка) пользователь на компьютер. Это бесплатное программное обеспечение и доступно на английском и китайском языках. После запуска «GPass» ярлыки приложений, которые должны пройти прокси через «GPass» могут быть перетащены и отпущены (drag and drop) в интерфейс «GPass». Когда это приложение запускается через «GPass», они автоматически конфигурируются под работу через сервис. По умолчанию конфигурируются Internet Explorer, Windows Media Player и клиентская электронная почта. Также по умолчанию подключение шифруется и различные средства используются для нахождения и подключения к разблокированному IP адресу. Приложение представляет подходящую скорость и дает возможность хранить шифрованные закладки и другие файлы.

«GPass» - это прекрасный выбор для пользователей без технических навыков, которые желают доверять третьей стороне и которым необходимо шифрованное, свободное туннелирование для услуг, помимо просмотра (http) на приемлемой скорости.

Как и в «Anonymzer», и других продуктах, поскольку веб-сайт «GPass» часто блокируется на многих территориях и фильтруются приложения, пользователю, возможно, придется приобрести программный продукт через третью сторону. Для противодействия возможной фильтрации услуг предпринимаются меры автоматического нахождения разблокированных IP адресов. Так как приложение должно устанавливаться, возможно, это не подходит для общественных терминалов или пользователей с высоким уровнем риска, чьи компьютеры могут быть захвачены.



## ТУННЕЛЬНОЕ ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ: бесплатное

### HTTP Tunnel

**http://www.http-tunnel.com/**

«HTTP Tunnel» это другая клиентская программа для Windows, которую загружает пользователь и устанавливает на компьютере. Также как и «psiphon», и «Peacefire/Circumventor», «HTTP Tunnel» предоставляет «сервер», который пользователь в нецензурированной стране может загружать для установки частного сервиса для кого-либо в цензурированной стране. «HTTP Tunnel» также можно использовать бесплатно, хотя платная услуга также доступна. Пользователи должны вручную конфигурировать приложения, такие как веб-браузеры, клиенты электронной почты и службу обмена мгновенными сообщениями для использования «HTTP Tunnel».

«HTTP Tunnel» это хороший выбор для технических пользователей, которым более важен обход, чем безопасность и желающим доверять третьей стороне, проводить конфигурации вручную и если им необходимо туннелирование для услуг, помимо просмотра (http) на приемлемой скорости. «HTTP tunnel» трафик не будет шифрован, а просто кодирован. Кодировка это просто другой способ выражения информации, а не для того, чтобы засекречивать информацию, как упомянуто выше.

Поскольку вебсайт «HTTP Tunnel», как и многие другие схожие системы, чаще всего уже заблокирован во многих странах и фильтрующими приложениями, пользователь возможно захочет приобрести программное обеспечение через третью сторону. Жесткий цезор может также заблокировать услугу «HTTP Tunnel», хотя технически опытный пользователь может предпринять меры против такой цензуры. Так как приложение должно устанавливаться, это не подходит для общественных терминалов или пользователей с высоким уровнем риска, чьи компьютеры могут быть захвачены.

# Технология
(продолжение)

## ТУННЕЛЬНОЕ ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ: платное

### Relakks
**https://www.relakks.com/**

«Relakks» представляет собой платную услугу, называемую «Relakks Safe Surf». Это система виртуальной частной сети (VPN), которая использует шифрованный туннель для передачи трафика от пользователя в цензурированной стране через серверы «Relakks». Она использует родные клиенты VPN встроенные в платформы Windows и Mac, чтобы пользователи не устанавливали какое-либо программное обеспечение. Множество различных приложений могут быть туннелированы через VPN, такие как электронная почта, веб-просмотр, и служба обмена мгновенными сообщениями.

«Relakks Safe Surf» это хороший выбор для тех пользователей, которые технически не опытные, готовы платить и доверять третьей стороне зашифрованную VPN. Однако, «Relakks» может быть легко заблокирован.

### Guardster/SSH
**http://www.guardster.com/**

Помимо платной, нешифрованной онлайновой системы обхода, «Guardster» представляет шифрованную онлайновую систему обхода и Безопасный командный процессор (SSH) за плату. Различные приложения, включая веб-браузеры и клиентскую электронную почту, могут быть туннелированы через шифрованный туннель SSH Guardster.

Guardster/SSH это хороший выбор для технически неопытных пользователей, которые готовы платить и доверять третьей стороне за шифрованный туннель.

Как и в других случаях вебсайт «Guardster/SSH» зачастую уже заблокирован во многих странах и фильтрующими приложениями. Поэтому, пользователь, возможно, захочет приобрести программное обеспечение через третью сторону. Жесткий цензор может также заблокировать услугу «Guardster/SSH».



## АНОНИМНЫЕ КОММУНИКАЦИОННЫЕ СИСТЕМЫ

Анонимные технологии скрывают IP адрес пользователя с сервера, где находится веб-сайт, который был посещен пользователем. Некоторые, но не все, анонимные технологии скрывают IP адрес пользователя от самой службы анонимности и шифрует трафик между пользователем и сервисом. Так как пользователи анонимных технологий делают запросы на веб-контент через прокси-сервис, вместо сервера, где находится (хостится) сам контент, анонимные технологии могут стать полезным способом обхода цензуры в Интернете. Однако, определенные анонимные технологии требуют от пользователя загрузки программного обеспечения и могут легко блокироваться властями.

**JAP ANON**
**http://anon.inf.tu-dresden.de/index_en.html**

«JAP ANON» предоставляет клиентскую программу для Windows/Mac/Linux, которую устанавливает пользователь в цензурированной стране на компьютере. Она доступна на английском и некоторых европейских языках. Пользователь должен выбрать «сочетание», через которое маршрутизировать трафик и затем следовать инструкциям, представленным для конфигурации веб-браузера под использование «JAP ANON». «Сочетание (mix)» это набор посредников, через которых запрос маршрутизируется и так как многие запросы перемещаются через комбинацию, ни операторы комбинации, ни запрашиваемый хостинг не знают подлинной личности пользователя. Однако, существуют различные уровни анонимности, так как некоторые применяют «единое сочетание», а другие «каскадное сочетание». Это также платная услуга для доступа на высокой скорости, в сочетании с анонимностью.

«JAP ANON» это хороший выбор для технических пользователей, которым нужна анонимность и услуга обхода для веб-просмотра на приемлемой скорости.

Так как веб-сайт «JAP ANON» зачастую уже заблокирован во многих странах, пользователь в цензурированной стране может приобрести программное обеспечение через третью сторону. Услуга все же доступна, если веб-сайт заблокирован, хотя жесткий цензор может также заблокировать и услугу. Так как приложение должно устанавливаться, это не подходит для общественных терминалов или пользователей с высоким уровнем риска, чьи компьютеры могут быть захвачены



## АНОНИМНЫЕ КОММУНИКАЦИОННЫЕ СИСТЕМЫ

### Tor

**http://tor.eff.org**

«Tor» это бесплатная анонимная коммуникационная система, которая работает через маршрутизацию веб-запросов в серии маршрутизаторов, каждый из которых снимает слой шифрования, чтобы ни один отдельный маршрутизатор в сети не мог определить источник или назначение запроса. Это прекрасный выбор для тех, кому необходима анонимность, так как правительству очень сложно наблюдать за передачей информации через сеть «Tor». «Tor» также позволяет пользователям туннелировать ряд других протоколов через сеть, такие как трафик службы обмена мгновенными сообщениями и электронной почты. Эта функция также известна как «скрытый сервис», который дает возможность пользователям анонимно публиковать свои веб-страницы, которые доступны только через «Tor».

В настоящее время требуется клиентская программа, поэтому скорее всего она не подходит для общественных терминалов и несет в себе существенный риск для тех, чьи компьютеры могут быть захвачены. Программа доступна на нескольких языках и с открытым исходным кодом, имеет достаточно специфическую, бурно развивающуюся сеть и документацию. После установки начинается обслуживание «Tor» и пользователь может пользоваться предпочитаемым браузером Firefox, который идет вместе с «Torbutton», чтобы «Tor» легко запускалась и отключалась. Другие браузеры требуют ручной конфигурации.

«Tor» это прекрасный выбор для технических пользователей, которым необходима высокая анонимность и услуги обхода для многочисленных приложений на медленной скорости.

Даже если веб-сайт «Tor» блокируется в некоторых странах, услуга все же доступна. Однако, непримиримое правительство может легко заблокировать «Tor», если пожелает. Тем не менее, разработчики работают над решениями вопроса блокировки. Из-за многочисленных маршрутизаторов, через которые проходит трафик «Tor», просмотр Интернета с помощью «Tor» может быть медленным. «Tor» требует значительных компьютерных навыков. Эта программа не для новичка.



## АНОНИМНЫЕ КОММУНИКАЦИОННЫЕ СИСТЕМЫ

### I2P

**http://www.i2p.net**

«I2P» это сеть анонимизации, которая в основном предназначена пользователям для анонимного размещения материала и анонимного доступа к контенту через «I2P». Однако, «I2P» может также применяться для просмотра Интернета анонимно. «I2P» представляет клиентскую программу для Windows/Mac/Linux, которую пользователь в цензурированной стране загружает и устанавливает на компьютере. Браузер пользователя должен вручную конфигурироваться для сети «I2P».

«I2P» это хороший выбор для технических пользователей, которым необходима анонимность, в первую очередь для обнародования, но также и для фильтров обхода на небольшой скорости.

Так как вебсайт «I2P» часто блокируется во многих странах, пользователь в цензурированной стране может приобрести программное обеспечение через третью сторону. Услуга все же может быть доступна, хотя также может заблокироваться жестким цезором. Так как приложение должно устанавливаться,  это не подходит для общественных терминалов или пользователей с высоким уровнем риска, чьи компьютеры могут быть захвачены

«I2P» это сеть анонимизации, которая в основном предназначена пользователям для анонимного размещения материала и анонимного доступа к контенту через «I2P». Однако, «I2P» может также применяться для просмотра Интернета анонимно. «I2P» представляет клиентскую программу для Windows/Mac/Linux, которую пользователь в цензурированной стране загружает и устанавливает на компьютере. Браузер пользователя должен вручную конфигурироваться для сети «I2P».

# Специфические приемы

## «Кэшированные» страницы

Многие поисковые серверы предоставляют копии веб-страниц оригинальных страниц, которые они индексируют, известные как кэшированные страницы. При поиске веб-сайта, смотрите на небольшую ссылку с названием «кэшировано» около результатов поиска. Так как вы извлекаете копию блокированной страницы с поискового сервера, а не с самого блокированного веб-сайта, вы сможете иметь доступ к цензурированному контенту. Однако, некоторые страны имеют целевые кэшированные службы для блокирования.

Пример: Кэш «Google»

## Услуги перевода

Существует много переводческих услуг в Интернет, часто предоставляемых поисковыми серверами. Если вы получаете доступ к веб-сайту через переводческую службу, именно она получает доступ к заблокированному сайту. Это позволит вам читать цензурированное содержание без прямого подключения к заблокированному веб-сайту.

Пример: babel.altavista.com

## RSS агрегаторы

RSS (стандарт для обмена контентом, основанный на XML) агрегаторы – это веб-сайты, которые позволяют вам делать закладки и читать любимую информацию в RSS-формате. Сайты RSS агрегаторов подключат вас к заблокированным веб-сайтам и загрузят информацию в формате RSS и сделают доступной. Так как не вы, а агрегатор связывается с сайтом, вы сможете получить доступ к цензурированному контенту.

Пример: www.bloglines.com

## Альтернативные доменные имена

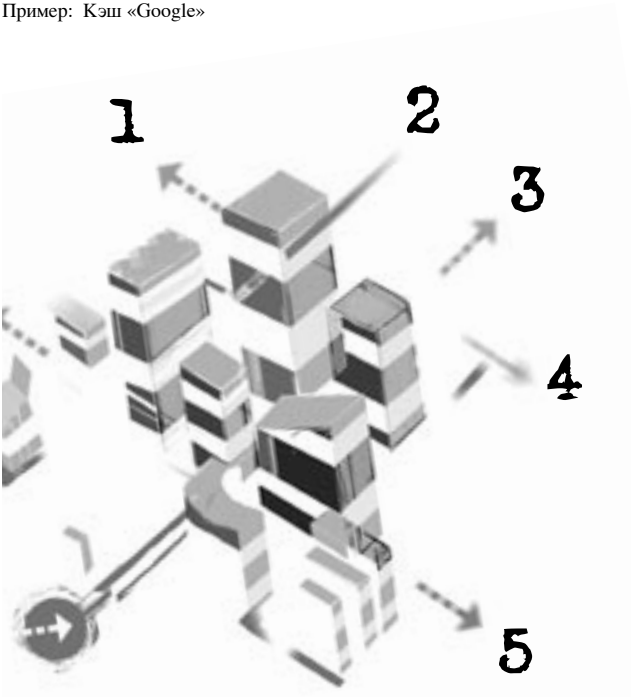
Одним из наиболее простых способов цензурировать веб-сайт – это блокировать доступ к его доменному имени, например, news.bbc.co.uk. Однако, сайты часто доступны под другими доменными именам, такими как newsrss.bbc.co.uk. Поэтому, если одно доменное имя блокируется, попытайтесь найти возможный доступ к другому домену.

Пример:
news.bbc.co.uk ->
newsrss.bbc.co.uk

## Веб-ускорители

Web-ускорители кэшируют веб-страницы и они показываются вам, как если бы ваше подключение к Интернет было быстрее. Так как вы извлекаете веб-сайт из кэша, а не с самого заблокированного веб-сайта, вы можете получить доступ к цензурированному содержанию.

Пример:
webaccelerator.google.com



# На заметку

Существует много способов получить доступ к заблокированному сайту. Большинство методов не позволяют вам сделать это безопасно. Найдите метод, который предоставит вам и доступ, и безопасность.

Лучше, если система обхода является решением частного лица. Независимо от выбора технологии, частные решения представляют лучшую возможность не быть обнаруженным и заблокированным.

Вы увеличите ваш уровень стабильного и безопасного обхода, если сможете использовать надежный контакт вне страны.

Никогда не используйте контакт вне страны, если вы его не знаете и не доверяете! Ваш контакт может быть вашим ключом к безопасности и вашим наиболее важным источником уязвимости.

Помните, что ваш поставщик может потенциально увидеть все, что вы делаете через систему обхода.

Нарушение государственного закона о цензуре в Интернет может быть большим риском. Не применяйте технологию, которую вы не до конца понимаете или не знаете, как применять. Тщательно оцените угрозу, основанную на ситуации в стране, своем уровне навыков и социальной сети.

Убедитесь, что вы полностью понимаете технологию, которую используете. Некоторые службы рекламируют безопасность и анонимность, но фактически не предоставляют их, или требуют дополнительной конфигурации или оплаты, для того чтобы активировать эти функции.

---

# Дополнительная информация

**NGO-in-A-Box** **http://security.ngoinabox.org/**
Многоязычная и рецензированная подборка программного обеспечения и руководств к повышению компьютерной безопасности и секретности в Интернет для защитников прав человека и независимых СМИ.

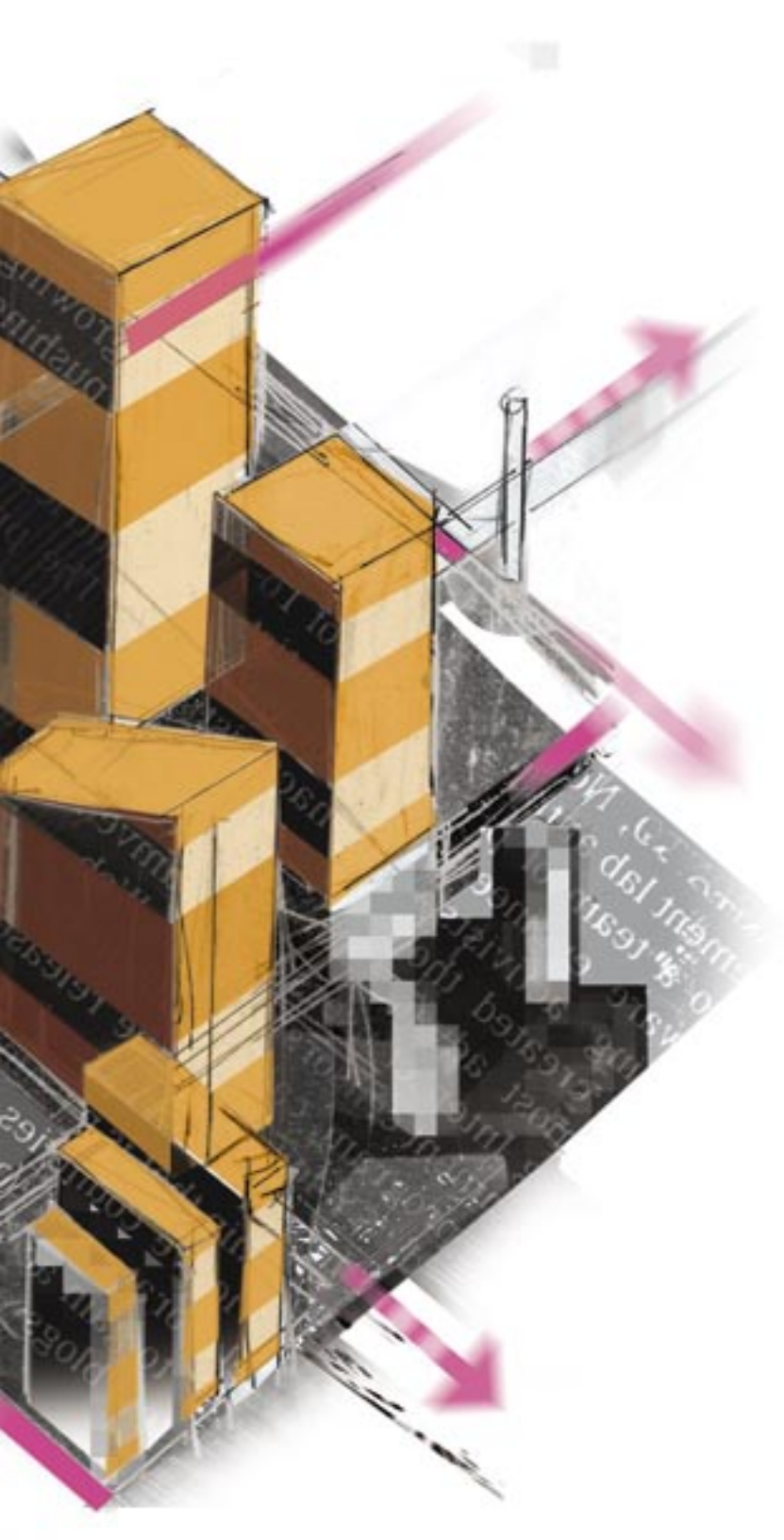
**Коллектив тактической технологии** **http://www.tacticaltech.org/**
Некоммерческий фонд, продвигающий использование бесплатного программного обеспечения и с открытым исходным кодом для неправительственных организаций и производителей Security NGO-in-A-Box.

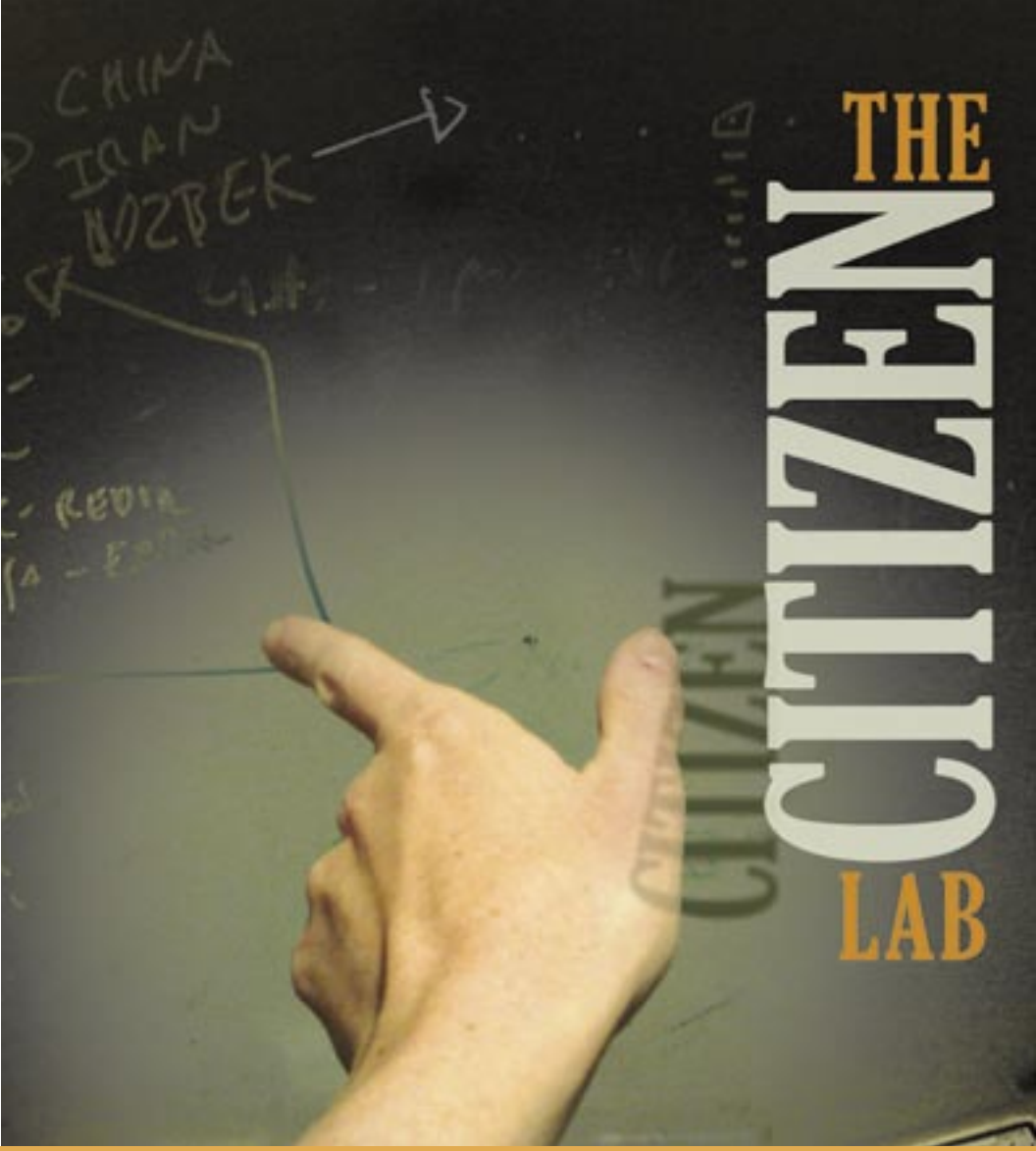
**Репортеры без границ, Руководство для кибер-диссидентов и блоггеров**
**http://www.rsf.org/rubrique.php3?id_rubrique=542**

**OpenNet Initiative** **http://opennet.net/**
Совместный проект Университетов Торонто, Кэмбриджа, Оксфорда и Гарварда. Их цель – документировать Интернет цензуру и наблюдение по всему миру.

**Цифровая безопасность и секретность для защитников прав человека**
**http://www.frontlinedefenders.org/manual/en/esecman/**
Дмитрия Витальева, опубликовано Front Line – Международным фондом защиты защитников прав человека.

**ICE** **www.nartv.org/blog/**
Блог Программы технических исследований Citizen Lab, Нарт Вилленев (Nart Villeneuve).






www.citizenlab.org

MUNK CENTRE
FOR INTERNATIONAL STUDIES

Ситизен Лаб - междисциплинарная лаборатория работает при Мунк Центре по международным исследованиям, Университета Торонто в Канаде, занимается исследованиями и разработками на пересечении сфер цифровых технологий и общемировых проблем гражданского общества.

Своеобразная “оранжерея”, в которой совместно работают социологи, ученые-компьютерщики, активисты, и художники. В проектах Ситизен Лаб проводятся исследования политических и социальных аспектов новых информационных и коммуникационных технологий, уделяя особое внимание правам человека, гуманизму и демократическим реформам во всем мире.

Проект Сивисек работает при общей поддержке Института Открытого Общества