Ваши данные и Интернет: что происходит за экраном

Для того, чтобы зайти на вебсайт, необходимо открыть браузер и ввести адрес сайта. Это действие запускает цепочку соединений через устройство, в результате чего сайт появляется на нашем экране.

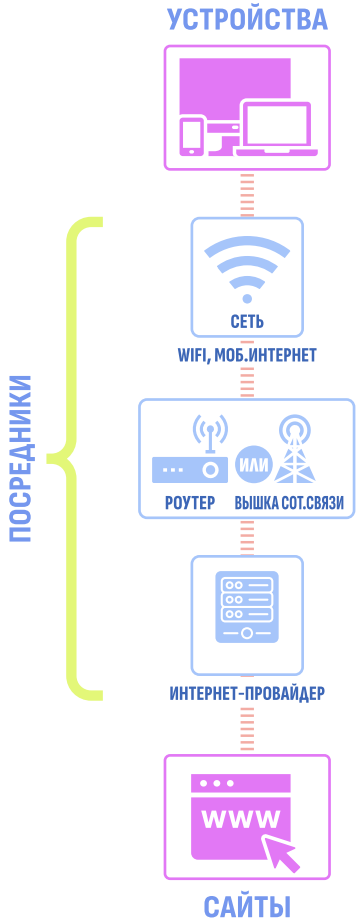
См. СХЕМУ A где показан процесс соединения при использовании Wi-Fi или мобильного Интернета.

При этом возникает вопрос: могут ли посредники, такие как интернет-провайдер или администраторы роутер, получить доступ к нашей информации? Если да, то что именно они могут увидеть? Говоря о безопасности, необходимо понимать, защищены ли наши устройства, каналы связи и посещаемые сайты, и кто может заполучить нашу информацию в случае несанкционированного доступа.

Как защитить наши устройства?

Устройства хранят массу информации, которая может быть интересна третьим лицам, желающим получить

A Соединение с сайтом



к ней физический или удалённый доступ — например, с помощью вредоносного ПО. Взломавший доступ злоумышленник сможет читать и редактировать файлы, видеть чаты и контакты, а также заходить в приложения и аккаунты.

Чтобы защитить устройства от вредоносного ПО, крайне важно использовать лицензионные и своевременно обновляемые операционные системы и программы. Также стоит научиться распознавать фишинг — сообщения и письма от якобы надёжных источников, отправленные с целью нанести вред устройству.

Чтобы уберечь информацию на устройствах от несанкционированного физического доступа (например, в случае конфискации или кражи), важно применять такие меры безопасности, как шифрование данных или полное шифрование диска. Также необходимо использовать длинные, уникальные и случайные пароли. Их можно безопасно хранить в диспетчере паролей и восстанавливать при помощи резервных вариантов доступа, если мы их забудем.

Подчеркнутые слова подробнее описаны в глоссарии на стр. 6

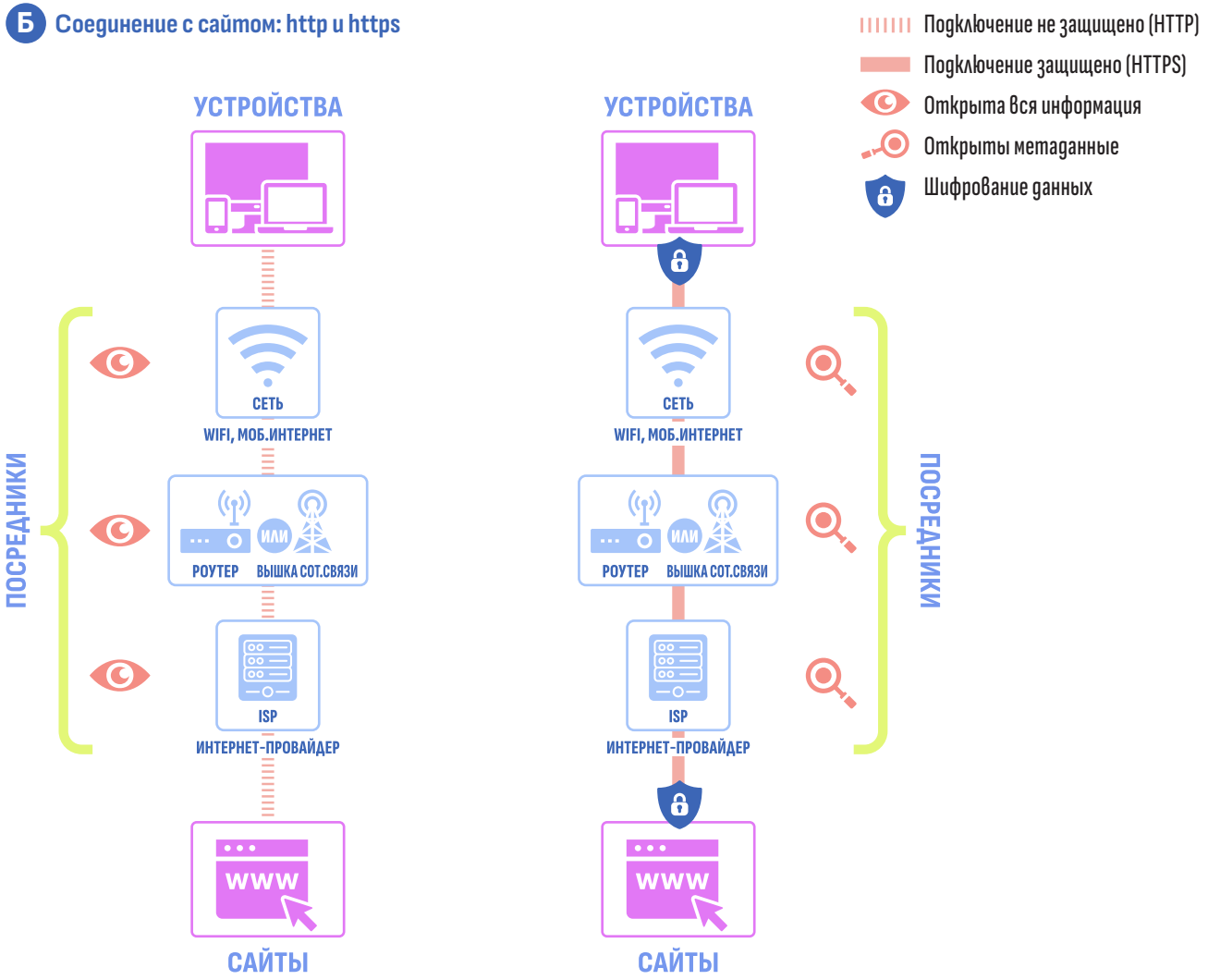
Как защитить свою приватность при посещении сайтов?

Сегодня большинство сайтов и сервисов используют защищённые соединения, что значительно повышает конфиденциальность и безопасность данных пользователей. Раньше, когда соединения не шифровались, все передаваемые данные (пароли, данные кредитных карт, электронные письма, сообщения в чатах и т. д.) были видны администраторам Wi-Fi-сетей, интернет-провайдерам и другим посредникам. Понять, какой протокол используется, открытый HTTP или защищённый HTTPS, можно взглянув на адресную строке браузера.

См. СХЕМУ Б где показана разница в безопасности при использовании http и https.

При использовании HTTPS посредникам, находящимся между нашим устройством и сайтом, видны только метаданные. Например, они видят, что мы зашли на youtube.com, но не могут определить, какие конкретно видео мы смотрим; то же самое касается facebook.com — неизвестно, какие профили просматриваются. Таким же образом они не видят содержимого наших сообщений, электронных писем, паролей или пересылаемых файлов.

Б Соединение с сайтом: http и https

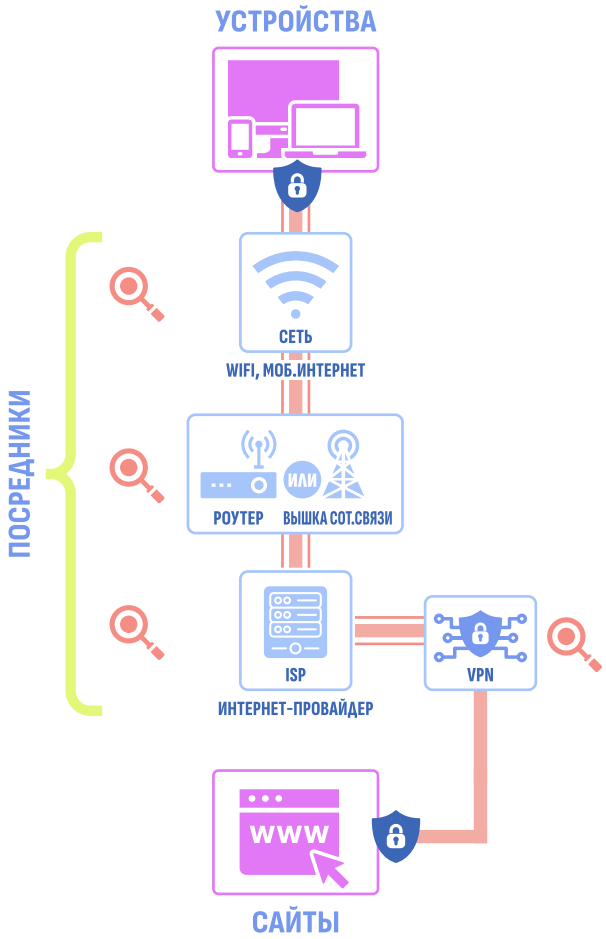


Помимо посредников администраторы самих сайтов также имеют доступ к обширному массиву информации о нашей деятельности в Интернете. Им доступен наш IP-адрес, сведения о браузере и устройстве, информация о нашей активности на сайте и все передаваемые данные. Если вы считаете, что сайт контролируется враждебными лицами или организациями, лучше избегать его посещения или предпринимать дополнительные меры безопасности, например, использовать виртуальную частную сеть (VPN).

См. СХЕМУ B где показано, как работает VPN.

Чтобы защитить наши онлайн-аккаунты и сообщения, рекомендуется использовать такие инструменты как двухфакторная аутентификация (2FA), контроль доступа и сквозное шифрование (E2EE).

B Использование VPN

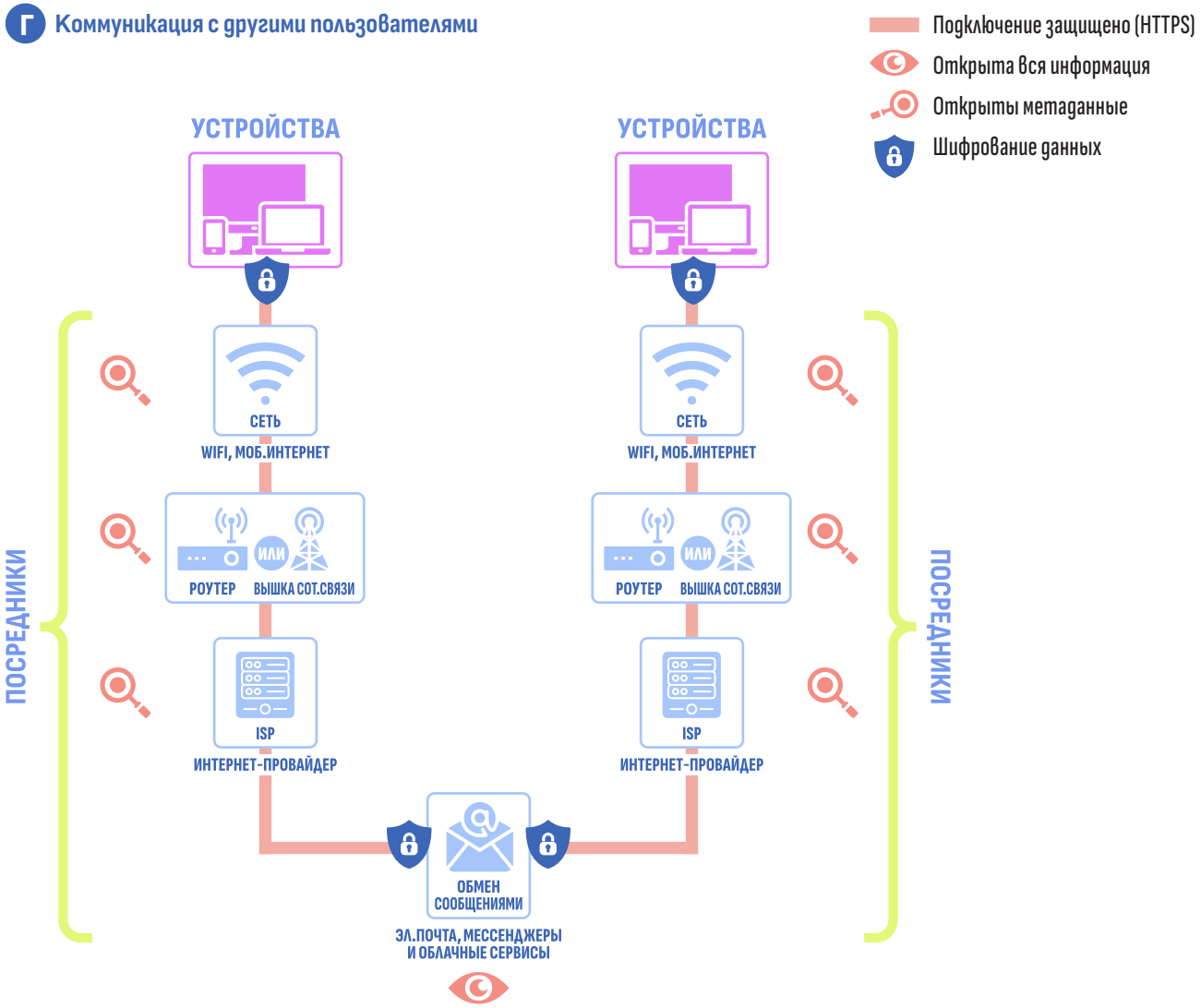


Как защитить свою приватность при использовании онлайн-серверов при коммуникации с другими пользователями?

При использовании HTTPS, когда мы отправляем электронное письмо адресату на общем с нами почтовом сервисе, мы можем быть уверены, что наша коммуникация защищена — администраторы сети Wi-Fi не видят ни содержимого письма, ни факта его отправки. Однако почтовый имеет доступ ко всей информации: содержимому писем, почте адресата, а также частоте и местоположению отправки писем. Тщательно изучите политику конфиденциальности используемых сервисов, чтобы понимать, к каким данным и информации они имеют доступ.

См. СХЕМУ Г где показана структура безопасности при коммуникации с другими пользователями.

Г Коммуникация с другими пользователями



Сквозное шифрование особенно важно в тех случаях, когда мы хотим защитить нашу информацию от самого сервиса коммуникации. Однако следует помнить, что даже при сквозном шифровании, которое скрывает отправляемые и получаемые данные, у сервиса всё равно остается доступ к нашим метаданным.

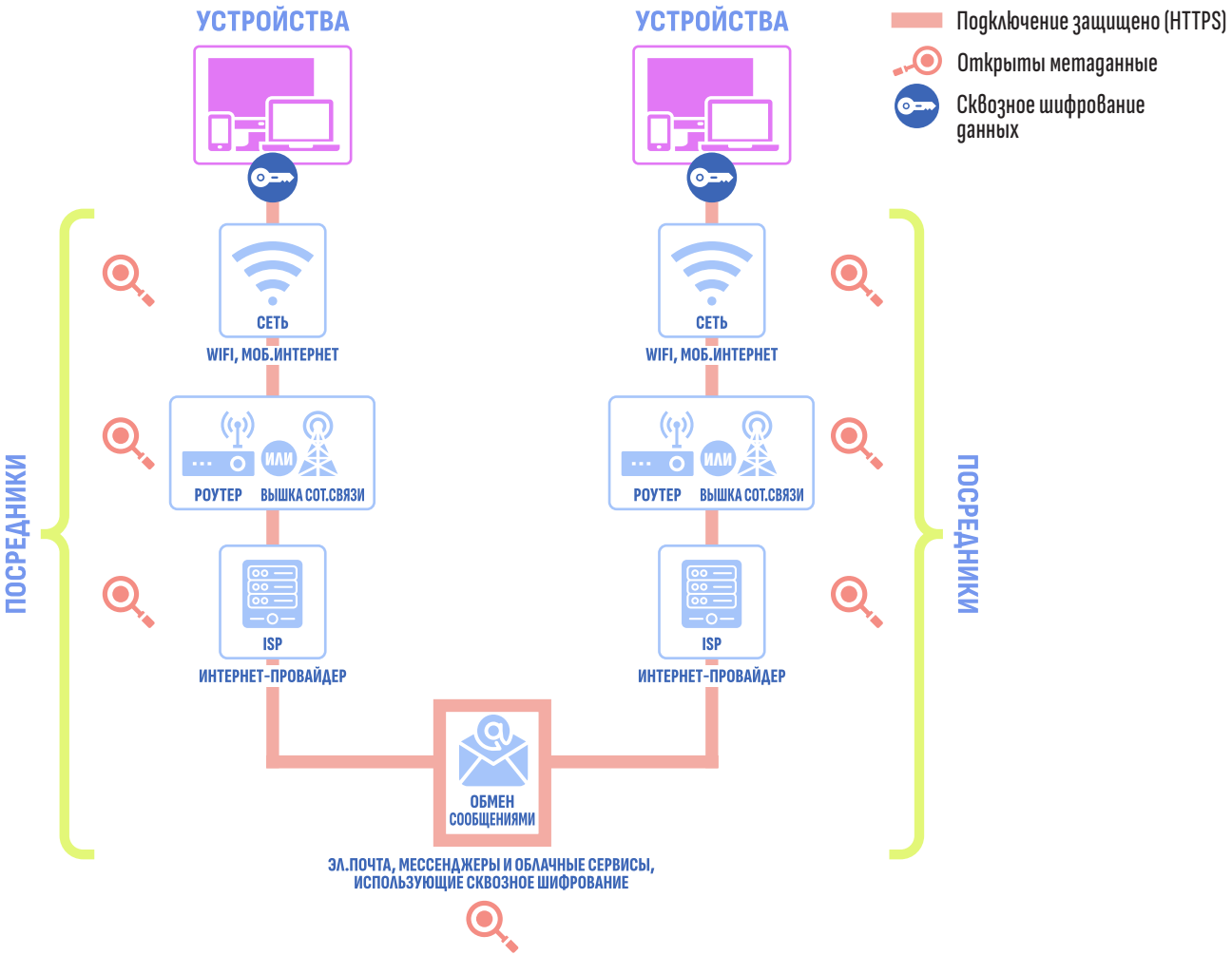
См. СХЕМУ А где наглядно показано, как работает сквозное шифрование.

Чтобы понять, достаточно ли безопасен тот или иной сервис, важно учитывать правовые нормы в стране, где он расположен, и то, как они могут влиять на безопасность наших данных. Например, в некоторых странах закон позволяет государственным органам получать доступ к данным, хранящимся у провайдеров, без согласия пользователей.

Помните о следующем:

- **Не стоит использовать все доступные средства безопасности без разбора — меры защиты должны быть продуманными и соответствовать конкретным рискам.**
- **Сначала определите и расставьте приоритеты среди основных рисков и проблем, а уже затем выбирайте и внедряйте решения.**
- **Не внедряйте решения, не понимая, какие конкретные задачи они решают.**
- **Следуйте всем этапам управления рисками, чтобы сделать безопасность действительно эффективной.**

А Коммуникация с другими пользователями: сквозное шифрование



Глоссарий:

КОНТРОЛЬ ДОСТУПА: метод, который помогает пользователям обезопасить свои облачные или коллективные пространства, устанавливая различные уровни доступа для различных пользователей, что помогает уменьшить риск утечки данных. При контроле доступа лицо или организация получают доступ только к тем данным и инструментам, которые необходимы им для работы.

ШИФРОВАНИЕ ДАННЫХ: метод, блокирующий третьим лицам доступ к файлам путем преобразования исходных данные в нечитабельный формат (шифрование).

СКВОЗНОЕ ШИФРОВАНИЕ (E2EE): система защищенной коммуникации, которая делает невозможным чтение содержимого ваших сообщений и файлов посторонними лицами. Никто, включая провайдеров, операторов, поставщиков коммуникационных программ или злоумышленников, не сможет получить доступ к вашим данным. Шифрование превращает обычное сообщение в нечитаемый зашифрованный текст, расшифровать который может только получатель.

ПОЛНОЕ ШИФРОВАНИЕ ДИСКА: метод, защищающий все данные на устройстве путём их шифрования и предоставления доступа только авторизованным лицам. При включённом полном шифровании, если злоумышленник завладеет устройством в выключенном либо заблокированном состоянии, ваши данные останутся ему недоступны.

ВРЕДОНОСНОЕ ПО: программа, созданная для причинения вреда путём получения доступа к устройству и редактирования информации на нем, например, для кражи данных или паролей и слежки за пользователями.

МЕТАДАННЫЕ: своего рода «цифровой след», включающий информацию о деятельности в сети: IP-адресе, времени подключения, объёме трафика и домене посещаемого сайта.

ДИСПЕТЧЕР ПАРОЛЕЙ: инструмент, упрощающий хранение паролей. С его помощью можно запомнить всего один надёжный пароль для входа в диспетчер, где безопасно хранятся остальные пароли.

ФИШИНГ: практика отправки писем или сообщений от якобы надёжных контактов, в реальности пытающихся заставить пользователя установить вредоносное ПО или раскрыть конфиденциальную информацию.

РЕЗЕРВНЫЕ ВАРИАНТЫ ДОСТУПА: методы, позволяющие восстановить доступ к аккаунту в случае, если пользователь забыл пароль. К ним могут относиться отправка кода восстановления на электронную почту или номер телефона, резервные коды или секретные вопросы.

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ (2FA): метод проверки личности при входе в аккаунты, предполагающий использование двух или более факторов. Эти факторы могут включать (1) информацию, например, пароль или PIN-код, (2) предмет или устройство, например, телефон или токен безопасности, и (3) биометрические данные, например, отпечаток пальца или распознавание лица.

ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ (VPN): инструмент, создающий зашифрованное соединение между вашим устройством и VPN-сервером. При использовании VPN ваш IP-адрес скрывается, и выглядит так, будто вы находитесь в другой локации. При этом ваш интернет-провайдер видит, что вы используете VPN, но не знает, на какие именно сайты вы заходите. Важно убедиться в надёжности разработчика VPN, проверив его политику конфиденциальности, бизнес-модель и местоположение серверов.