Библиотека Анархизма
Антикопирайт и инфоанархизм

Брюс Шнайер
Почему мы шифруем

Скопировано 03.06.2025 с
https://habr.com/ru/articles/262103/ (оригинал на английском: https://www.schneier.com/blog/archives/2015/06/why_we_encrypt.html)

ru.anarchistlibraries.net

Почему мы шифруем

Брюс Шнайер

Шифрование защищает наши данные. Оно защищает наши данные на компьютерах и в дата-центрах, защищает их во время передачи через интернет. Защищает наши видео-, аудио- и текстовые разговоры. Защищает нашу частную информацию. Защищает нашу анонимность. Иногда защищает наши жизни.

Эта защита важна для каждого. Легко увидеть, как шифрование защищает журналистов, правозащитников и политических деятелей в авторитарных странах. Но шифрование также защищает и всех остальных. Защищает наши данные от преступников. Защищает от конкурентов, соседей и членов семьи. Защищает от злонамеренных атак и случайных инцидентов.

Шифрование лучше всего работает, когда оно вездесуще и работает без вмешательства пользователя. Вы чаще всего используете шифрование в двух случаях: HTTPS и шифрование связи мобильного телефона с базовой станцией, и они так хорошо работают именно потому, что вы о них даже не задумываетесь.

Шифрование должно быть включено по умолчанию, а не как дополнительная возможность, которую вы включаете, когда собираетесь сделать что-то, что стоит защитить.

Это важно. Если мы используем шифрование только, когда работаем с важными данными, то сам факт шифрования говорит о важности данных. Если в стране шифрование используют только диссиденты, то власти имеют простой способ определять диссидентов. Но если шифрование используют все и всегда, оно перестаёт выдавать важность информации. Никто не сможет отличить повседневную болтовню от конфиденциальной беседы. Правительство не сможет отличить диссидентов от остальных людей. Каждый раз, когда вы используете шифрование, вы защищаете кого-то, кому приходится использовать шифрование, чтобы выжить.

Важно помнить, что шифрование не обеспечивает безопасность магическим образом. При шифровании есть множество способов сделать что-то не так, и мы часто читаем про такие случаи в СМИ. Шифрование не защищает ваш компьютер или телефон от взлома, оно не может защитить метаданные (например: адрес e-mail должен оставаться незашифрованным, чтобы ваше письмо могло быть доставлено адресату).

Но шифрование — самая важная технология сохранения конфиденциальности, которая у нас есть; технология, лучше всего подходящая для защиты от массовой слежки вроде той, которую правительства используют для контроля населения и которую преступники используют для поиска уязвимых жертв. Заставляя правительства и преступников точно нацеливать свои атаки, мы защищаем общество.

Сегодня мы видим, что правительства сопротивляются внедрению сильного шифрования. Многие государства, от Китая и России до более демократических правительств

вроде США и Великобритании, говорят об ограничении сильного шифрования. Это опасно, технически невозможно и такая попытка нанесёт серьёзнейший вред безопасности Интернета.

Из сказанного вот что следует. Первое, мы должны влиять на компании, чтобы они предлагали шифрование всем, по умолчанию. И второе, мы должны сопротивляться требованиям правительств ослабить шифрование. Любое ослабление, даже с целью обеспечения правопорядка, ставит нас всех под угрозу. Несмотря на то, что преступники извлекают выгоду из сильного шифрования, мы все находимся в гораздо большей безопасности, если у нас есть сильное шифрование.