Библиотека Анархизма
Антикопирайт и инфоанархизм

Эрик Хьюз
Манифест шифропанка
1993

https://www.activism.net/cypherpunk/manifesto.html
Перевод О. Турухиной, A Cypherpunk's Manifesto

ru.anarchistlibraries.net

Манифест шифропанка

Эрик Хьюз

1993

Приватность необходима открытому обществу цифрового века. Приватность и секретность не одно и то же. Частное дело – это то, о чем, по мнению человека, всему миру знать не нужно, о секретном же деле не должен знать вообще никто. Приватность – это возможность выбирать, какую информацию о себе открыть миру.

Если две стороны заключают сделку, у каждой из них остаются воспоминания, о которых она впоследствии может рассказать. Разве кто-то способен этому помешать? Можно было бы принять запрещающий это закон, однако свобода слова ещё более важна для открытого общества, чем приватность. Мы не пытаемся добиться ограничения свободы слова. Если на одном форуме в дискуссии участвует множество людей, каждый из них может обращаться к остальным и обобщать сведения о некоторых лицах или других участниках. Электронные коммуникации сделали такие дискуссии возможными, и они никуда не исчезнут только потому, что нам этого хочется.

Если нам необходима приватность, мы должны позаботиться о том, чтобы все участники транзакции располагали

только той информацией, которая требуется для совершения сделки.

Поскольку любая информация может быть передана, мы должны постараться рассказать о себе настолько мало, насколько это возможно. В большинстве случаев личность человека не очевидна. Когда я, покупая в магазине журнал, отдаю деньги продавцу, ему нет необходимости знать, кто я. Когда я договариваюсь с провайдером об отсылке и получении электронной почты, ему не нужно знать, кому я посылаю сообщения, что я пишу и что мне отвечают; ему нужно знать только, как их доставить и сколько я должен за это платить. Если механизмы транзакции таковы, что моя личность непременно раскрывается, значит, приватности у меня нет. У меня нет возможности выбирать, раскрывать свою личность или нет; я всегда должен это делать.

Приватность в открытом обществе, таким образом, подразумевает наличие системы анонимных транзакций. До настоящего времени наличные деньги оставались основой такой системой. Система анонимных транзакций – это не система секретных транзакций, но система, дающая человеку возможность раскрывать свою личность только тогда, когда он сам этого захочет. Вот в чем суть приватности.

Приватность в открытом обществе требует использования криптографии. Если я что-то говорю, то хочу, чтобы это слышали только те люди, к которым я обращаюсь. Если мои слова доступны всему миру, приватности у меня нет. Использование шифрования указывает на стремление к приватности, использование для шифрования слабой криптографии говорит о том, что это стремление не слишком велико. Кроме того, если сообщение послано анонимно и вы хотите иметь гарантию, что ваша личность будет раскрыта только получателю, необходимо использовать криптографическую подпись.

Не приходится рассчитывать на то, что государство, корпорации или другие крупные безликие организации добровольно предоставят нам приватность. Им выгодно разглашать информацию о нас, и мы должны быть к этому готовы. Пытаться заставить их молчать – значит бороться с существующей информационной реальностью. Информация не просто хочет быть свободной – ей это необходимо. Информация занимает весь предоставленный ей объем. Информация – это младшая, но более сильная сестра Молвы: она быстрее, у неё больше глаз, она больше знает, но понимает меньше, чем Молва.

Если мы рассчитываем на приватность, то должны сами её защищать. Мы должны объединиться и создать системы, которые позволят осуществление анонимных транзакций. Люди веками пытались добиться приватности, используя шёпот, темноту, конверты, закрытые двери и курьеров. Однако эти методы не могли обеспечить полной приватности, а вот электронные технологии могут.

Мы, шифропанки, призваны создать анонимные системы. Мы защищаем свою приватность с помощью криптографии, анонимных систем переадресации электронной почты, цифровых подписей и электронных денег.

Шифропанки пишут программы. Мы знаем, что кто-то должен писать программы для защиты приватности, а поскольку мы не сможем добиться приватности, пока её не получат все, мы напишем такие программы. Мы публикуем код программ, чтобы наши единомышленники могли попрактиковаться и поработать над ним. Он доступен любому в любой точке планеты. И нам нет дела, что кто-то не одобряет наши программы. Мы уверены, что их невозможно уничтожить и что работу над распространившейся по всему миру системой нельзя остановить.

Шифропанки протестуют против ограничения использования криптографии, поскольку шифрование –

основной способ защиты приватности. Шифрование, в сущности, делает информацию недоступной широкой общественности. Законы, запрещающие использование криптографии, бессильны за пределами границ конкретного государства. Криптография неизбежно распространится по всему миру, а вместе с ней и системы анонимных транзакций, существование которых она делает возможным.

Широкое распространение приватности требует, чтобы она стала частью общественного договора. Люди должны объединиться и использовать эти системы ради общего блага. Приватность будет поддерживаться только в том случае, если все члены общества объединятся для этого. Мы, шифропанки, готовы выслушать ваши вопросы и предложения и надеемся, что вы присоединитесь к нам и поможете осуществить наши планы. Однако мы не отклонимся от нашего курса только потому, что кому-то не по душе цели, которые мы преследуем.

Мы, шифропанки, активно работаем, чтобы достичь приватности в сетях.
Давайте же продолжим наше дело вместе.