План статьи журнала «Хакер»

1. Защищенный сообщения
2. Социальные сети
3. Голосовой и видеочат

Тезисы статьи журнала «Хакер»

Автор: Илья Русанен

Безопасные способы общения в сети

Для пересылки защищенных сообщений разработан крипто- графический протокол OTR (Off-the-Record). Для создания сильного шифрования протокол использует комбинацию алго- ритмов AES, симметричного ключа, алгоритма Диффи — Хел- лмана и хеш-функции SHA-1. Основное преимущество OTR перед другими средствами шифрования — это его применение на лету, а не после под- готовки и оправления сообщения.

Вообще, соцсети слабо вяжутся с концепцией анонимности и приватности переписки. Эти сервисы стали источником информации о ли- цах всех возрастов: люди пишут в соцсети все о себе, своих близких и друзьях, выкладывают жизненные фото и видео. Можно ограничить доступ к этим сведениям, но это не преграда для спецслужб

С мгновенными текстовыми сообщениями мы анонимны, а что насчет голосового и видеообщения? Skype принадлежит Microsoft, а она (по документам Сноудена) была уличена в пере- даче сведений спецслужбам.