УЯЗВИМОСТЬ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

Минаєва А.В., Рысованый А.Н.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Известно, что при исследовании генераторов случайных чисел, например, пакета GnuPG, выявлена критическая уязвимость, которая сказывается при шифровании информации. Генераторы псевдослучайных чисел являются подклассом генераторов случайных чисел. А такая уязвимость присутствует в функции смешивании энтропии генератора псевдослучайных чисел, используемом в библиотеках Libgcrypt и GnuPG. Как известно, это позволяет предсказать следующие 160 бит последовательности. Эта проблема присутствует во всех версиях библиотек GnuPG и Libgcrypt, выпущенных до 17 августа 2016 года, так как ошибка была допущена на раннем этапе разработки еще в 1998 году.

Разрабатывать и исследовать псевдослучайные последовательности намного проще – для них разработан серьезный математический аппарат. Однако, псевдослучайная последовательность в силу наличия конечного цикла генерирования имеет и недостатки, которые влияют на критичность их использования.

В работе сделана попытка анализа возможных последствий уязвимости. Можно предположить, что такая уязвимость не влияет на надежность созданных в GnuPG ключей RSA. Что касается ключей DSA и Elgamal, то возможность предсказания закрытого ключа по открытой информации оценивается как маловероятная. DSA (Digital Signature Algorithm) – это алгоритм с использованием открытого ключа для создания электронной подписи. Этот алгоритм не подходит для шифрования важной информации.

В работе показано, что и псевдослучайные последовательности могут иметь очень высокую устойчивость. Но в этом случае требования по используемой максимальной степени и распределению промежуточных аргументов полинома усложняются. Это не влияет на сложность математического описания математической модели. Такая сложность возникает уже на этапе проектирования электронных схем таких генераторов. А если применить различные схемы соединения нескольких таких генераторов с различными деградиентами и различными их свойствами, то можно смело утверждать, что обнаружить уязвимость в таких схемах будет почти невозможно.