УДК 621.391.25

Об одной модели формирования ключевой информации для перспективных информационных технологий

Голиков В.Ф., Абдольванд Ф.
Белорусский национальный технический университет

Одной из главных проблем, которую необходимо решать для достижения правильного функционирования симметричной криптосистемы, это проблема обеспечения абонентов системы общим секретным ключом. Эта проблема в настоящее время решается с использованием алгоритма открытого распределения ключей Диффи- Хеллмана Однако в последние годы бурное развитие физики, электроники, математики и информатики сделало вполне реальным появление квантового компьютера одним из возможных применений которого является «взлом» традиционных односторонних функций с последующим вычислением общего ключа, формируемого по схеме Диффи- Хеллмана. Представляет интерес обобщение формулировки задачи формирования общего ключа с учетом известных фундаментальных закономерностей теории информации. Пусть два абонента А и В хотят иметь одинаковую случайную равновероятную бинарную последовательность (СРБП) известную только им, не используя при этом защищенного канала связи. В качестве меры секретности СРБП можно использовать ее энтропию H(K)=n, где n-длина последовательности K. На первом этапе каждый абонент независимо друг от друга формирует секретное число: ХА, ХВ. . На втором этапе абоненты обмениваются некоторой информацией, прямо или косвенно связанной с их секретными числами. Задача этого этапа на основании полученной информации сформировать каждым абонентом одинаковую СРБП. В ходе процесса обмена согласующей информацией третий абонент С, подключившись к открытому каналу связи, может получить некоторую информацию о сформированном общем ключе. Количество этой информации зависит от связности согласующей информации с секретными числами. Исходя из такой постановки задачи, в докладе рассматриваются альтернативные способы распределения ключевой информации: использование квантового канала, использование нейронных сетей, использование аномальных статистических эффектов. Последний способ включает многократное генерирование пар начальных случайных последовательностей, обор из них пар, отличающихся не более чем на 30%, эффективную процедуру устранения несовпадений, повышение конфиденциальности сформированного ключа.