УДК 681.51

Модель генерации идентичной последовательности данных с помощью двух синхронизируемых нейронных сетей в целях получения криптографического ключа

Якимов А.Н.
Белорусский национальный технический университет

Проблема обеспечения безопасности информации с каждым днем становится все более острой. Причем, чем глубже информационные технологии внедряются в производственные процессы, тем больше возможные финансовые потери организации от угроз информационной безопасности. Безопасность любой конфиденциальной информации зависит от надежности системы шифрования, ее криптостойкости. Одна из наилучших идей, была идея Диффи-Хеллмана, позволяющий получить общий секретный ключ, используя незащищенный от прослушивания, но защищённый от подмены, канал связи. На сегодняшний день можно взломать такой криптографический ключ любой сложности. Проблема только во временных ресурсах. Задачи дискретного логарифмирования представляют более эффективные решения. Не за горами появление квантового компьютера.

ИНС (искусственные нейронные сети) позволяют взглянуть на проблему обеспечения безопасности иным взглядом. Основное преимущество ИНС в их способности к самообучению. Две ИНС с одинаковым алгоритмом обучения способны дать на выходе идентичные результаты. Это и легло в основу получения общего секретного криптографического ключа. Системы таких ИНС имеют стахостическое поведение и низкую чувствительность к шуму. Такие системы позволяют решить проблемы криптографии с открытым ключом, распределения ключей, хеширования и генерации псевдослучайных чисел. Так как коммуникация необходимых данных для синхронизации сетей передаются по открытому каналу, появляется возможность прослушивания. В идеальных условиях, учитывая факт, что наблюдающая сторона имеет идентичную по строению ИНС, не способна получить те же данные на выходе. Но, как и многие любые криптографические системы, может быть подвержена криптоатакам.

Для улучшения безопасности такой системы является сокращения времени, затраченного на синхронизацию. Опираясь на знания о восстановлении ключевой информации из его имеющейся последовательности, процесс синхронизации системы можно остановить, не дожидаясь ее полной синхронизации. Область относительно нова, и пока не имеет практических применений.